МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТУСА

Л. В. Загоруйко, А. В. Дудатьєв

КОНСПЕКТ ЛЕКЦІЙ
з дисципліни
«УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ»

Вінниця
2023

УДК 004.056:005](075.4)
М 545

Рекомендовано до друку вченою радою
факультету інформаційних та прикладних технологій
Донецького національного університету імені Василя Стуса
(протокол № 4 від 21.11.2023 р.)

Укладачі:

Загоруйко Л. В., канд. техн. наук, доцент, доцент кафедри прикладної математики та кібербезпеки ДонНУ імені Василя Стуса;

Дудатьєв А. В., канд. техн. наук, доцент, доцент кафедри захисту інформації Вінницького національного технічного університету;

Рецензенти:

Крижановський В. Г., д-р техн. наук, професор кафедри прикладної математики та кібербезпеки Донецького національного університету імені Василя Стуса;

Кондратенко Н. Р., канд. техн. наук, професор кафедри захисту інформації Вінницького національного технічного університету.

М 545 Конспект лекцій з дисципліни «Управління інформаційною безпекою» / укл. Л. В. Загоруйко, А. В. Дудатьєв. Вінниця: ДонНУ імені Василя Стуса, 2023. 280 с.

У конспекті лекцій з дисципліни «Управління інформаційною безпекою» подано теоретичний і методичний матеріал для вивчення і самостійного опрацювання матеріалу із сучасних проблем управління інформаційною безпекою, основ політики і засобів управління, упередження ризиків на підприємствах та для підвищення рівня знань здобувачів у сфері управління інформаційною безпекою.

Конспект лекцій рекомендовано для здобувачів вищої освіти спеціальності 125 Кібербезпека, а також для фахівців із систем інформаційної безпеки, які спеціалізуються в області використання й упровадження інформаційних технологій у різних сферах діяльності.

УДК 004.056:005](075.4)

© Загоруйко Л. В., 2023
© Дудатьєв А. В., 2023
© ДонНУ імені Василя Стуса, 2023

ЗМІСТ

ВСТУП 5

Тема 1. Загрози інформаційній безпеці 10
Контрольні питання.....29

Тема 2. Інформаційна система персональних даних.....30
Контрольні питання.....53

Тема 3. Захист інформації в мобільних пристроях.....54
Контрольні питання.....58

Тема 4. Управління інформаційною безпекою 59
Контрольні питання.....84

Тема 5. Кіберзлочинність.....85
Контрольні питання.....94

Тема 6. Інформаційна безпека держави.....95
Контрольні питання.....104

Тема 7. Передумови та основні напрямки розвитку менеджменту
у сфері інформаційної безпеки 105
Контрольні питання.....118

Тема 8. Діяльність міжнародних організацій
у сфері інформаційної безпеки 119
Контрольні питання.....129

Тема 9. Стандартизація в сфері менеджменту інформаційної безпеки.....130
Контрольні питання.....136

Тема 10. Роботи спеціалізованих міжнародних організацій
та об’єднань у галузі інформаційної безпеки.....137
Контрольні питання.....144

Тема 11. Управління інформаційною безпекою на рівні великих
постачальників інформаційних систем.....145
Контрольні питання.....153

Тема 12. Організаційне забезпечення інформаційної безпеки
на Державному рівні: практика США 154
Контрольні питання.....165

Тема 13. Забезпечення інформаційної безпеки на державному рівні:
практика України 166
Контрольні питання.....179

Тема 14. Забезпечення інформаційної безпеки на державному рівні:
практика України (криптографічні методи захисту).....180
Контрольні питання.....189

Тема 15. Забезпечення інформаційної безпеки на державному рівні:
практика України (технічні методи захисту) 190
Контрольні питання.....199

Тема 16. Менеджмент інформаційної безпеки на рівні підприємства:
основні напрями і структура політики безпеки 200
Контрольні питання.....211

Тема 17. Зміст деталізованої політики безпеки 212
Контрольні питання.....218

Тема 18. Департамент інформаційної безпеки і робота з персоналом 219
Контрольні питання.....228

Тема 19. Організація реагування на надзвичайні ситуації (інциденти) 229
Контрольні питання.....237

Тема 20. Аудит стану інформаційної безпеки на підприємстві 238
Контрольні питання.....246

Тема 21. Надання послуг у сфері інформаційної безпеки 247
Контрольні питання.....255

Тема 22. Надання послуг у сфері інформаційної безпеки (страхування) 256
Контрольні питання.....262

Тема 23. Міжнародний стандарт ISO/IEC 27001 263
Контрольні питання.....272

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....273

ВСТУП

Кожен технологічний бізнес-процес піддається загрозам безпеки і конфіденційності. Сучасні засоби захисту здатні боротися з атаками кіберзлочинців. Але цього недостатньо, тому фірма або підприємство повинні забезпечити такі умови внутрішньої політики і поведінки співробітників, щоби мінімізувати або значно зменшити ці ризики.

Оскільки цей процес складний і потребує висококваліфікованих фахівців, компанії впроваджують структурні підрозділи, що застосовують систему управління інформаційною безпекою. Система управління інформаційною безпекою (СУІБ) – основа політики і засобів управління, що систематично керують інформаційною безпекою та упередженням ризиків на підприємстві.

Ці заходи безпеки можуть відповідати загальним стандартам безпеки або бути більш сфокусованими на певній галузі. Наприклад, ISO 27001 являє набір специфікацій з детальним описом створення, управління та реалізації політики і засобів управління СУІБ. ISO містить керівництво з розробки відповідних стратегій системи управління інформаційною безпекою.

Основа системи управління інформаційною безпекою орієнтована на оцінку ризиків і управління ними. Процес управління ризиками безпеки дає змогу організаціям досягти поєднання максимальної економічної ефективності з відомим та прийнятним рівнем ризику й надає керівникам різних рівнів зрозумілий метод організації та ресурсів з обмеженим доступом для реалізації управління ризиками. Реалізація управління ризиками інформаційної безпеки дає змогу організаціям з розподіленими корпоративними мережами використовувати економічно ефективний контроль, що знижує ризик до прийнятного рівня.

Управління інформаційною безпекою можливе за підтримки безпеки в інформаційно-комунікаційних системах та мережах певного діапазону засобів і заходів управління.

Розвиток нових інформаційних технологій і загальна комп’ютеризація призвели до того, що інформаційна безпека не тільки стає обов’язковою, вона ще й одна з характеристик інформаційних систем. Існує великий клас систем обробки інформації, під час розробки яких фактор безпеки відіграє першорядну роль.

Практично за всіма визначеними світовою практикою пороговими значеннями показників інформаційної безпеки Україна подолала небезпечну межу. Показник зниження валового внутрішнього продукту (ВВП) щодо базового періоду (2020 р.) перевищує максимальне порогове значення у 2021 р. і становить 12,9 %. Зниження обсягів виробництва має постійну тенденцію коливання біля критичної межі, низьке його фізичне зростання до базового періоду.

Деформація галузевої структури виробництва характеризується зменшенням обсягу продукції галузей, які визначають ступінь науково-технічного та соціально-економічного розвитку країни.

Низький рівень інформаційної безпеки обумовлений неефективністю державного управління, його недостатньою зорієнтованістю на захист національних інтересів в усіх сферах, а також непослідовністю та безсистемністю у здійсненні економічних реформ, недосконалістю національного законодавства щодо забезпечення інформаційної безпеки та ефективного управління економікою; недостатнім рівнем кваліфікації держслужбовців із питань забезпечення національної безпеки; корупцією в управлінських структурах.

Негативні тенденції в інформаційній сфері національної безпеки та потреби їх подолання визначили актуальність і пріоритетність цього напряму наукових досліджень. Вітчизняні фахівці працюють над розв'язанням цих проблем. Серед них – В. Н. Амітан, О. І. Амоша, О. І. Барановський, І. Ф. Бінько, З. С. Варналій, О. С. Власюк, В. М. Геєць, Б. В. Губський, О. Є. Ємельянов, М. М. Єрмошенко, Я. А. Жаліло, Б. Є. Кваснюк, Т. Т. Ковальчук, Д. Г. Лук'яненко, В. О. Мандибура, В. І. Мунтіян, І. В. Недін, О. Ф. Новікова, М. А. Павловський, Г. А. Пастернак-Таранушенко, С. І. Пірожков, А. Ю. Сменковський, А. І. Соляник, А. І. Сухоруков, М. Г. Чумаченко, В. Т. Шлемко.

Активізація наукових досліджень із проблем інформаційної та економічної безпеки обумовила формування самостійного наукового напряму, який передбачає сполучення та взаємозв'язок двох підсистем державного управління – національної безпеки та економічної політики.

Економічну та інформаційну безпеку підприємства можна розглядати як практичне використання таких принципів сучасного менеджменту: своєчасна реакція на зміни в зовнішньому середовищі, бачення підприємства, тобто чітке подання про те, що воно повинно собою являти, а також одного з основних положень сучасної теорії управління – ситуаційного підходу до керування, який означає важливість швидкості й адекватності реакції, що забезпечують адаптацію підприємства до умов його існування. Звідси, економічну та інформаційну безпеку підприємства треба розглядати як еволюційний розвиток ситуаційного підходу до керування. Економічна та інформаційна безпека викликають усе більшу зацікавленість підприємств, які стикаються із труднощами під час реалізації принципово нових підходів до керування підприємствами, організації керування підприємством у ринкових умовах.

У централізованій економіці інформаційна безпека підприємства забезпечувалася вертикально побудованими методами керування, які стали неприйнятними в умовах ринкової економіки, оскільки в ринковому середовищі з урахуванням його специфіки механізми безпеки розосереджуються за багатьма

суб'єктами і напрямами економічної, фінансової, законодавчої, правоохоронної діяльності, коли організаційно починає зростати горизонтальний складник системи захисту. Наявні недопрацювання з економічної та інформаційної безпеки підприємства як у теорії, так і на практиці необхідно переборювати.

Навчальна дисципліна «Управління інформаційною безпекою» передбачає ознайомлення здобувачів вищої освіти з загальними принципами управління інформаційною безпекою, основними поняттями управління інформаційною безпекою підприємства на базі міжнародних стандартів серії ISO/IEC серії 27000, вивчення організаційних методів захисту, організаційно-технічних та організаційно-правових заходів, наукового підходу до організації захисту інформації; планування захисту; керування системою захисту; безперервності процесу захисту інформації; мінімальної достатності організації захисту; системного підходу до організації та проєктування систем і методів захисту інформації; комплексного підходу до організації захисту інформації; відповідності рівня захисту цінності інформації; гнучкість захисту; багатозональності захисту, що передбачає розміщення джерел інформації в зонах з контрольованим рівнем її безпеки; обмеження кількості осіб, які допускаються до захищеної інформації; особиста відповідальність персоналу за збереження довіреної інформації.

Дисципліна спрямована на розгляд широкого кола питань щодо принципів створення комплексних систем захисту інформації (КСЗІ) в інформаційно-телекомунікаційних системах (ІТС), здійснення комплексу заходів, спрямованих на розроблення і впровадження інформаційних технологій, які забезпечують обробку інформації в ІТС згідно з вимогами, встановленими нормативно-правовими документами у сфері захисту інформації.

Дисципліна «Управління інформаційною безпекою» є дисципліною професійної та практичної підготовки для бакалаврів спеціальностей 125 Кібербезпека освітніх програм «Кібербезпека» та «Кібербезпека та захист інформації», що формує загальні і фахові компетентності та програмні результати навчання, якими оволодіють здобувачі вищої освіти.

Мета вивчення навчальної дисципліни полягає у: формуванні у здобувачів вищої освіти здатності діяти на основі законодавчої та нормативно-правової бази України й вимог відповідних стандартів, зокрема міжнародних у галузі інформаційної та/або кібербезпеки; здатність розв'язувати складні спеціалізовані задачі та практичні проблеми у галузі забезпечення інформаційної безпеки і/або кібербезпеки, що характеризується комплексністю та неповною визначеністю умов; забезпеченні теоретичної підготовки для дослідження стану інформаційної безпеки комп'ютерних систем і мереж, надання знань про сучасні технології створення комплексних систем захисту інформації, отримання знань

і навичок практичного застосування прийомів та методів захисту інформації в інформаційно-телекомунікаційних системах різного призначення; засвоєнню принципів, завдань системи управління інформаційною безпекою, вивченню нормативної та правової бази з питань організації та проведення аудиту інформаційної безпеки, методики оцінки інформаційних ризиків, здійсненню комплексу заходів, спрямованих на розроблення і впровадження інформаційних технологій, які забезпечують обробку інформації в інформаційно-телекомунікаційних системах згідно з вимогами, встановленими нормативно-правовими актами та нормативними документами у сфері захисту інформації.

Вивчення навчальної дисципліни передбачає формування та розвиток у здобувачів вищої освіти таких компетентностей та програмних результатів навчання відповідно до освітніх програм «Кібербезпека» та «Кібербезпека та захист інформації».

Спеціальні компетентності:

1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки (СК-1).

2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної та/або кібербезпеки (СК-2).

3. Здатність до використання програмних та програмно-апаратних комплексів засобів захисту інформації в інформаційно-телекомунікаційних (автоматизованих) системах (СК-3).

4. Здатність забезпечувати неперервність бізнесу згідно зі встановленою політикою інформаційної та/або кібербезпеки (СК-4).

5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки (СК-5).

6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.) (СК-7).

7. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку (СК-8).

8. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпекою (СК-9).

9. Здатність виконувати моніторинг ресурсів і процесів функціонування, інформаційно-телекомунікаційних (автоматизованих) систем згідно зі встановленою політикою інформаційної та/або кібербезпеки (СК-11).

10. Здатність аналізувати, виявляти та оцінювати можливі загрози, вразливості та дестабілізуючі чинники інформаційному простору та інформаційним

ресурсам згідно зі встановленою політикою інформаційної та/або кібербезпеки (СК-12).

Програмні результати навчання (ПРН):

1. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки (ПРН 9).

2. Аналізувати проекти інформаційно-телекомунікаційних систем, базуючись на стандартизованих технологіях та протоколах передачі даних (ПРН 13).

3. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів (ПРН 29).

4. Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків (ПРН 33).

5. Брати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації (ПРН 34).

6. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно зі встановленою політикою інформаційної і/або кібербезпеки (ПРН 35).

7. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки (ПРН 42).

8. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/або кібербезпеки для розслідування інцидентів (ПРН 43).

9. Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами (ПРН 44).

10. Застосовувати ріні класи політик інформаційної безпеки та/або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів (ПРН 45).

11. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах (ПРН 46).

ТЕМА 1
ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

У темі наведена характеристика інформаційної безпеки, основні її складники. Описано, чим обумовлені інформаційні загрози, подана класифікація загроз; їх розташування, розміри завдання шкоди, ступені впливу на інформаційну систему, природа їх виникнення; ступінь впливу на інформаційну систему. Описана класифікація вразливостей систем безпеки. Наведені сучасні загрози. Описані причини витоку інформації та способи їх захисту.

Ключові слова: *інформаційна безпека, захист інформації, інформаційна загроза, внутрішні загрози, зовнішні загрози, цілісність, конфіденційність, доступність, загроза розкриття, загроза цілісності, загроза відмови в обслуговуванні, Ping-of-Death, SYN Flood, Land / Latierra, WinNuke, Ping sweeps, TCP-сканування, UDP-сканування, Ідентифікація ОС, сучасні загрози, стихійні джерела, загроза безпеці комп'ютерної системи, вразливість комп'ютерної системи, атака на комп'ютерну систему, хакерські атаки, хакери, технологія інфраструктури відкритих ключів, системи одноразових паролів, структура системи, біометричні системи, криптографічний захист даних, криптографія, електронний підпис, цифровий підпис, інформаційні ризики, витік інформації, комерційна таємниця, помилки в роботі ПЗ, збої в роботі серверного обладнання, поломка технічних засобів захисту, канал витоку даних, шифрування.*

План

1.1. Характеристика інформаційної безпеки.
1.2. Класифікація загроз.
1.3. Сучасні загрози.
1.4. Інформаційні ризики.
1.5. Витік інформації.

1.1. Характеристика інформаційної безпеки

Під *інформаційною безпекою* розуміють захищеність інформації і підтримуючої інфраструктури від випадкових або навмисних впливів природного або штучного характеру, що можуть завдати неприйнятного збитку суб'єктам інформаційних відносин, зокрема власникам та користувачам інформації і підтримуючої інфраструктури.

Захист інформації – комплекс заходів, спрямованих на забезпечення інформаційної безпеки. Аналізуючи підходи до проблем інформаційної безпеки, необхідно починати з виявлення суб'єктів інформаційних відносин та інтересів цих суб'єктів, пов'язаних з використанням інформаційних систем (ІС). Загрози інформаційній безпеці пов'язані з використанням інформаційних технологій.

Інформаційна безпека залежить від комплексу заходів та сучасних технологій, керування якими відбувається із застосуванням різноманітних інформаційних систем.

Інформаційна безпека – багатогранна, багатовимірна діяльність, у якій успіх може принести тільки системний, комплексний підхід. Безпека використання інформаційних систем полягає у забезпеченні доступності, цілісності, конфіденційності та підтримки інформаційних ресурсів її інфраструктури.

До основних складників інформаційної безпеки належить конфіденційність, тобто захист від несанкціонованого доступу до інформації.

Під час аналізу проблематики, пов'язаної з інформаційною безпекою, необхідно враховувати специфіку цього аспекту безпеки: інформаційна безпека є складником інформаційних технологій – системи, що розвивається безпрецедентно високими темпами. Тут важливі не стільки окремі рішення (закони, навчальні курси, програмно-технічні вироби), наявні на сучасному рівні, скільки механізми генерації нових рішень, що дають змогу жити в темпі технічного прогресу.

Складність механізмів прийняття сучасних управлінських рішень щодо захисту інформації в новому інформаційному середовищі пов'язана із застосуванням інформаційних систем, призначених для великого обсягу обробки, обміну та використання їх у сучасному житті особи, підприємства, держави, світу, а також зі швидкими темпами розвитку технічних засобів.

Загрозу можна розглядати як атаку та можливість порушення інформаційної безпеки і посягання на заволодіння інформацією, а той, хто посягає на інформацію, є зловмисником. Загроза проявляється через низький захист або знаходження вразливих місць у системі захисту інформаційних систем.

Основними завданнями системи інформаційної безпеки є:

– виявлення та усунення загроз безпеці нанесенням економічного, фінансового, матеріального та морального збитку;

– створення механізмів реагування на загрози розвитку і функціонуванню підприємства та національній безпеці;

– вжиття заходів щодо забезпечення безпеки персоналу підприємства та ін.

Поняття інформаційної безпеки включає:

– надійність роботи комп'ютера;

– збереження цілісності даних;

– захист інформації від несанкціонованого доступу;

– таємниця електронного листування.

Інформаційні загрози можуть бути обумовлені:

– природними факторами;

– людськими факторами.

До природних факторів належать такі джерел загроз, які об'єднують, обставини, що становлять непереборну силу, тобто такі обставини, що мають об'єктивний і абсолютний характер, поширюється на всіх. До непереборної сили в законодавстві і договірній практиці належать стихійні лиха або інші обставини, які неможливо передбачити або запобігти, або можливо передбачити, але неможливо запобігти із сучасним рівнем людського знання і можливостей. Такі джерела загроз абсолютно не піддаються прогнозуванню, тому заходи захисту від них повинні застосовуватися завжди.

Стихійні джерела потенційних загроз інформаційній безпеці зазвичай є зовнішніми відносно тих, що захищаються, і під ними розуміються насамперед природні катаклізми (пожежі, землетруси, повені, урагани, різні непередбачені обставини, незрозумілі явища та інші форс-мажорні обставини).

До людських факторів належать:

– загрози випадкового характеру (помилки обробки, передачі, обміну інформації);

– загрози навмисного характеру (несанкціонований доступ до інформації).

Навмисні загрози призводять до шкідливих наслідків для користувачів автоматизованих інформаційних систем і можуть бути *активними та пасивними.*

Пасивні загрози спрямовані на несанкціоноване використання інформаційних ресурсів і не впливають на функціонування системи (прослуховування).

Активні загрози спрямовані на порушення нормального процесу функціонування системи через вплив на апаратні, програмні та інформаційні ресурси. Джерелами активних загроз можуть бути безпосередні дії зловмисників, програмні віруси і т. ін.

1.2. Класифікація загроз

Загрози інформаційній безпеці класифіковані за різними ознаками.

1. За аспектом інформаційної безпеки, на який спрямована загроза:

– *загрози конфіденційності* (неправомірний доступ до інформації – інформація стає відомою тому, хто не має повноважень доступу до неї) – наявні тоді, коли отримано доступ до деякої інформації обмеженого доступу, що зберігається в обчислювальній системі, чи передано інформацію від однієї системи до іншої. Через загрозу порушення конфіденційності використовується термін «витік». Подібні загрози виникають внаслідок «людського фактора» (наприклад, випадкове делегування тому чи іншому користувачеві привілеїв іншого користувача), збоїв в роботі програмних і апаратних засобів. *До інформації обмеженого доступу належить державна таємниця і конфіденційна інформація* (комерційна таємниця; персональні дані; професійні види таємниць: лікарська, адвокатська, банківська, службова, нотаріальна, таємниця страхування, слідства і

судочинства, листування, телефонних переговорів, поштових відправлень, телеграфних або інших повідомлень (таємниця зв'язку); відомості про сутність винаходу, корисної моделі чи промислового зразка до офіційної публікації (ноу-хау) та ін.);

– *загрози цілісності* (неправомірна зміна даних). Загрози порушення цілісності – загрози, пов'язані з імовірністю модифікації тієї чи іншої інформації, що зберігається в інформаційній системі. Порушення цілісності може бути викликано різними факторами – від навмисних дій персоналу до виходу з ладу обладнання;

– *загрози доступності* (здійснення дій, що унеможливлюють чи утруднюють доступ до ресурсів інформаційної системи). Порушення доступності – це створення таких умов, за яких доступ до послуги або інформації буде або заблокований, або можливий за час, який не забезпечить виконання тих чи інших бізнес-цілей.

2. За розташуванням джерела загроз:

– *внутрішні* (джерела загроз розташовуються всередині системи);

– *зовнішні* (джерела загроз знаходяться поза системою).

Внутрішні загрози:

– виток інформації;

– неавторизований доступ.

Зовнішні загрози:

– шкідливі програми (віруси, трояни, черв'яки і под.);

– атаки хакерів;

– DDos-атаки;

– таргетингові атаки;

– спам;

– фішинг;

– промислові загрози (stuxnet, flame, duqu);

– шпигунське програмне забезпечення (spyware, adware);

– botnets (ботнети, або зомбі-мережі).

3. За розмірами завдання шкоди:

– *загальні* (нанесення збитку об'єкту безпеки загалом, заподіяння значної шкоди);

– *локальні* (заподіяння шкоди окремим частинам об'єкта безпеки);

– *приватні* (заподіяння шкоди окремим властивостям елементів об'єкта безпеки).

4. За ступенем впливу на інформаційну систему:

– *пасивні* (структура і зміст системи не змінюються);

– *активні* (структура і зміст системи піддаються змінам).

5. За природою виникнення:

– *природні* (об'єктивні) – викликані впливом на інформаційне середовище об'єктивних фізичних процесів або стихійних природних явищ, що не залежать від волі людини;

– *штучні* (суб'єктивні) – викликані впливом на інформаційну сферу людини. Серед штучних загроз виділяють:

– ненавмисні (випадкові) загрози – помилки програмного забезпечення, персоналу, збої в роботі систем, відмови обчислювальної і комунікаційної техніки;

– навмисні (умисні) загрози – неправомірний доступ до інформації, розробка спеціального програмного забезпечення, що використовується для здійснення незаконного втручання, розробка та поширення вірусних програм і т. ін. Навмисні загрози обумовлені діями людей.

Основні проблеми інформаційної безпеки пов'язані насамперед із навмисними загрозами, оскільки вони є головною причиною злочинів і правопорушень.

Цілісність інформаційних даних означає здатність інформації зберігати початковий вигляд і структуру як у процесі зберігання, так і після неодноразової передачі. Вносити зміни, видаляти або доповнювати інформацію має право тільки власник або користувач із легальним доступом до даних.

Конфіденційність – характеристика, що вказує на необхідність обмеження доступу до інформаційних ресурсів для певного кола осіб. У процесі дій і операцій інформація стає доступною тільки користувачам, які включені в інформаційні системи і успішно пройшли ідентифікацію.

Доступність інформаційних ресурсів означає, що інформація, яка знаходиться у вільному доступі, надається повноправним користувачам ресурсів своєчасно і безперешкодно.

Достовірність вказує на приналежність інформації довіреній особі або власнику, який одночасно виступає в ролі джерела інформації.

Забезпечення і підтримка інформаційної безпеки включають комплекс різнопланових заходів, що запобігають, відстежують і усувають несанкціонований доступ третіх осіб. Заходи забезпечення інформаційної безпеки спрямовані також на захист від пошкоджень, спотворень, блокування або копіювання інформації. Принципово, щоби всі завдання вирішувалися одночасно – тільки тоді забезпечується повноцінний, надійний захист.

Класифікація вразливостей систем безпеки

Загрози інформаційній безпеці проявляються не самостійно, а через можливу взаємодію з найбільш слабкими ланками системи захисту, тобто через фактори вразливості. Загроза призводить до порушення діяльності систем на конкретному об'єкті-носієві.

Основні вразливості виникають внаслідок дії таких факторів:

– недосконаліть програмного забезпечення, апаратної платформи;

– різні характеристики будови автоматизованих систем в інформаційному потоці;

– частина процесів функціонування систем є неповноцінною;

– неточність протоколів обміну інформацією та інтерфейсу;

– складні умови експлуатації і розташування інформації.

Найчастіше джерела загрози запускаються з метою отримання незаконної вигоди внаслідок заподіяння шкоди інформації. Але можливі і випадкові загрози через недостатні заходи забезпечення захисту і дії масового загрозливого фактору.

Існує поділ вразливостей за класами:

– об'єктивні;

– випадкові;

– суб'єктивні.

Якщо усунути або, як мінімум, послабити вплив вразливостей, можна уникнути повноцінної загрози, спрямованої на систему зберігання інформації.

Отже, класифікація погроз ІБ розподіляється за характером загрози, видом впливу, джерелом та об'єктом загрози.

Дослідники виділяють три основні види загроз безпеці:

– *загрози розкриття;*

– *загрози цілісності;*

– *загрози відмови в обслуговуванні.*

Загроза розкриття полягає в тому, що інформація стає відомою тому, кому не варто її знати. Серед термінів комп'ютерної безпеки загроза розкриття наявна щоразу, коли отриманий доступ до певної конфіденційної інформації, що зберігається в ІС або передається від однієї системи до іншої.

Загроза цілісності включає будь-яку навмисну зміну (модифікацію або навіть видалення) даних, що зберігаються в ІС, або передаються з однієї системи до іншої. Зазвичай вважається, що загрозі розкриття піддаються більшою мірою державні структури, а загрозі цілісності – ділові або комерційні структури.

Загроза відмови в обслуговуванні виникає щоразу, коли внаслідок деяких дій блокується доступ до певного ресурсу ІС. Реальне блокування може бути постійним, щоб запитуваний ресурс ніколи не був отриманий, або блокування може викликати тільки затримку запитуваного ресурсу, досить тривалу для того, щоб він став непридатним. У таких випадках кажуть, що ресурс вичерпаний.

Пропонується ще одна класифікація загроз ІБ [25], хоча єдиної й загальноприйнятої класифікації погроз ІБ не існує, і напевно, не буде взагалі, тому що постійно з'являються нові загрози, які все складніше ідентифікувати.

Найпоширеніші DoS-атаки – відмова в обслуговуванні

1. Ping-of-Death посилає ICMP-пакет розміром більше 64 Кб, що може призвести до переповнення буфера операційної системи і виведення системи, що атакується, з ладу.

2. SYN Flood дуже швидко посилає велику кількість TCP SYN-пакетів (які ініціюють з'єднання), залишаючи жертву чекати величезної кількості з'єднань і викликаючи цим посилене завантаження ресурсів та відмову від санкціонованих з'єднань.

3. Land / Latierra посилає підроблений SYN-пакет з ідентичними вихідною адресою та кінцевим портом так, що система рухається нескінченною петлею, намагаючись виконати TCP-з'єднання.

4. WinNuke посилає OOB/URG-дані для TCP-з'єднання із портом 139 (NetBIOS Session/SMB), що призводить до зависання ОС Windows. Найбільшому впливу піддається ОС Windows 95, пізніші версії ОС Windows мають проти цієї атаки відповідний захист.

Найпоширеніші процеси сканування

1. Ping sweeps. Протягом цього простого процесу сканування діапазон IP-адрес аналізується утилітою **ping** (так зване пінгування) з метою визначення активних комп'ютерів. Варто зауважити, що більшість складних сканерів буде використовувати інші протоколи (як-от SNMP sweep), щоб виконувати ту саму дію.

2. TCP-сканування. Зондування відкритих TCP-портів у пошуках сервісів, які може використовувати порушник. Сеанси сканування можуть використовувати звичайні TCP-з'єднання або приховані (stealth) сеанси сканування, що використовують наполовину відкриті з'єднання (для того, щоб захистити їх від реєстрації в журналах) або FIN-сеанси сканування (ніколи не відкривають порт, але тестують, якщо щось прослуховується). Сеанси сканування можуть бути послідовними, випадковими, або сконфігурованими за переліком портів.

3. UDP-сканування. Ці сеанси сканування є складнішими, тому що User Datagram Protocol (UDP) працює без встановлення віртуального з'єднання. Метод полягає в тому, щоб послати «сміттєвий» UDP-пакет до наміченого порту. Більшість машин будуть реагувати за допомогою ICMP-повідомлення «destination port unreachable», яке вказує, що на цьому порту немає сервісу, який прослуховується. Однак багато комп'ютерів «поглинають» ICMP-повідомлення, тому ви не зможете здійснювати швидке UDP-сканування.

4. Ідентифікація ОС. Шляхом посилання неприпустимих (або дивних) ICMP чи TCP-пакетів порушник може ідентифікувати ОС. Стандарти зазвичай встановлюють, у який спосіб комп'ютери повинні реагувати на легальні пакети, тому машини мають тенденцію бути однаковими у своїй реакції на припустимі вхідні дані. Однак стандарти упускають (зазвичай навмисно) реакцію на непри-

пустимі вхідні дані. Отже, унікальні реакції кожної ОС на неприпустимі вхідні дані формують сигнатуру, яку хакери можуть використовувати для того, щоби зрозуміти, під чиїм управлінням функціонує обраний комп'ютер. Цей тип діяльності навний на нижньому рівні (начебто прихованих сеансів TCP-сканування), на якому аналізовані системи не реєструють події.

1.3. Сучасні загрози

Носіями загроз інформаційній безпеці є джерела загроз, якими виступають як суб'єктивні (особистості), так і об'єктивні обставини (конкуренти, злочинці, корупціонери, адміністративно-управлінські органи, інше). Джерела загроз мають таку мету: ознайомлення з відомостями, які охороняють, їх модифікація в корисливих цілях і знищення для нанесення прямих матеріальних збитків. Усі джерела загроз інформаційній безпеці можна розділити на три основні групи.

Обумовлені діями суб'єкта (антропогенні джерела) – суб'єкти, дії яких призводять до порушення безпеки інформації, кваліфікуються як умисні або випадкові злочини. Джерела, дії яких можуть призвести до порушення безпеки інформації, можуть бути зовнішніми і внутрішніми. Ці джерела можна спрогнозувати і вжити адекватних заходів.

Обумовлені технічними засобами (техногенні джерела) – ці джерела загроз менш прогнозовані, безпосередньо залежать від властивостей техніки і тому вимагають особливої уваги. Ці джерела загроз інформаційній безпеці також можуть бути зовнішніми і внутрішніми.

Стихійні джерела (обставини, що становлять непереборну силу) – стихійні лиха або інші обставини, що неможливо передбачити або запобігти, або можливо передбачити, але неможливо запобігти. Ці обставини об'єктивного й абсолютного характеру поширюються на всіх. Такі джерела загроз абсолютно не піддаються прогнозуванню, тому заходи проти них повинні застосовуватися завжди. Стихійні джерела зазвичай є зовнішніми відносно інформаційних джерел, що захищаються, і під ними розуміються природні катаклізми.

Загроза безпеці комп'ютерної системи – це потенційно можлива подія, незалежно від того, навмисна чи ні, що може здійснити небажаний вплив на саму систему, а також на інформацію, що зберігається в ній.

Вразливість комп'ютерної системи – це її невдала характеристика, що уможливлює виникнення загрози. Інакше кажучи, саме через наявність вразливостей у системі відбуваються небажані події.

Атака на комп'ютерну систему – це дія, що вчиняється зловмисником і полягає в пошуку й використанні загрози або іншої вразливості. Отже, атака – це реалізація загрози. Варто зауважити, що таке тлумачення атаки (за участю людини, яка має злий намір) виключає наявний у визначенні загрози елемент

випадковості. Але, як показує досвід, часто буває неможливо розрізнити навмисні й випадкові дії, і надійна система захисту повинна адекватно реагувати на кожне з них.

Більш детально розглянемо особливості зовнішніх загроз.

1. Хакерські атаки. Отримавши доступ до системи, вони направлені на крадіжку конфіденційних даних або встановлюють шкідливі програми та використовують «зламані» комп'ютери для розсилки спаму. У програми закрадаються помилки, що робить їх вразливими для атаки. Хакерам ці «лазівки» дають змогу проникнути в систему, а ті, хто пише віруси, використовують помилки в коді додатків, щоб забезпечити автоматичний запуск на комп'ютері шкідливих програм.

Хакери – це електронні «зламники», які проникають у комп'ютерну систему, використовуючи особливі вразливі «лазівки» у програмному забезпеченні. Захиститися від них можна за допомогою особливого додатка – мережевого екрана з пакетною фільтрацією, що входить до складу антивірусних програм і робить комп'ютер невидимим для хакерів.

Для захисту від шкідливого коду і хакерських атак:

– встановлюється антивірусна програма;

– встановлюється оновлення ОС Windows (Update), що відповідає за безпеку;

– увага під час роботи зі спамом в електронній пошті і системах миттєвих повідомлень;

– збереження резервної копії (BackUp) даних.

2. Технологія інфраструктури відкритих ключів. Технологія інфраструктури відкритих ключів дає змогу перевіряти і засвідчувати справжність користувача. Інфраструктура відкритих ключів (англ. *Public key infrastructure, PKI*) забезпечує єдину ідентифікацію, аутентифікацію й авторизацію користувачів системи, додатків і процесів, і водночас гарантує доступність, цілісність і конфіденційність інформації. Інфраструктура PKI являє собою систему цифрових сертифікатів, носіями яких є USB-ключі або смарт-карти.

Під час використання індивідуального секретного пароля і засобів криптографічного захисту цифрові сертифікати відіграють роль електронних паспортів. Використання в корпоративній мережі технології інфраструктури відкритих ключів значно підвищує безпеку всієї мережі загалом, оскільки дає змогу відмовитися від використання парольної аутентифікації користувачів всередині, а також забезпечує безпечний доступ віддалених користувачів до системи. Основними носіями інформації є USB-ключі та смарт-карти. Користувачам не треба запам'ятовувати складні паролі і періодично їх міняти – досить підключити електронний ключ або смарт-карту і ввести PIN-код.

3. Системи одноразових паролів. Системи багатофакторної аутентифікації засновані на технології одноразових паролів (англ. *one time password,*

OTP). Вони призначені для автентифікації мобільних користувачів, які відрізняється простотою у використанні, установці й адмініструванні.

Ця технологія заснована на тому, що пароль користувача не постійний і змінюється з плином часу токеном (спеціальним апаратно-програмним пристроєм). Це рішення широко використовується в системах віддаленого доступу, зокрема системах клієнт-банк, для автентифікації користувачів під час доступу з недовірених середовищ (інтернет-кафе, бізнес-центри тощо).

OTP-токен – мобільний персональний пристрій, що належить певному користувачеві і генерує одноразові паролі, які використовуються для аутентифікації цього користувача. *OTP*-токени мають невеликий розмір і випускаються у вигляді: кишенькового калькулятора; брелока; смарт-карти; пристрою, комбінованого з USB-ключем; спеціального програмного забезпечення для кишенькових комп'ютерів. Як приклад рішень OTP можна навести лінійку RSA SecurID, ActivCard Token, комбінований USB-ключ Aladdin eToken NG-OTP.

Структура системи:

– сервер автентифікації (баз даних акаунтів, прив'язаних до пристроїв, синхронізація за часом);

– канал передачі;

– форма для введення автентифікаційних даних (зазвичай три поля (Login, OTP, PIN));

– клієнтська частина (OTP брелок та ін.).

4. Біометричні системи – це вимірні фізіологічні або поведінкові дані людини. Біометричні дані унікальні для кожної людини і їх можна використовувати для встановлення особи або перевірки декларованих особистих даних:

– для ідентифікації користувача (замість введення імені користувача);

– для однофакторної автентифікації користувача;

– спільно з паролем або аутентифікації токеном (як-от смарт-карта) для забезпечення двофакторної автентифікації.

Біометричні дані діляться на групи:

1. Фізіологічні біометричні характеристики – засновані на даних, отриманих шляхом вимірювання анатомічних характеристик людини, як-от відбиток пальця, форма обличчя або кисті, сітківка ока.

2. Поведінкові біометричні характеристики (динамічні) – засновані на даних, отриманих шляхом вимірювання дій людини. Характерною рисою для поведінкових характеристик є їх протяжність у часі – вимірюється дією, що має початок, середину і кінець, як-от голос, підпис.

1. Криптографічний захист даних. Криптографія – область знань, що вивчає тайнопис (криптографія) і методи його розкриття (криптоаналіз). Криптографія вважається розділом математики.

Мета криптографічної системи полягає в тому, щоб зашифрувати вихідний текст (шифртекст, криптограма). Одержувач, якому він призначений, повинен бути здатний розшифрувати («дешифрувати») цей шифртекст, відновивши відповідний йому відкритий текст. Водночас зловмисник повинен бути нездатний розкрити вихідний текст.

Існує відмінність між розшифрування (дешифруванням) і розкриттям шифртексту. Широко відомим історичним прикладом криптосистеми є так званий шифр Цезаря, що є простою заміною кожної букви відкритого тексту третьої наступної за нею буквою алфавіту (з циклічним перенесенням, коли це необхідно). Наприклад, «A» замінювалося на «D», «B» на «E», «Z» на «C».

Всі методи шифрування поділяються на дві групи:

– шифри з секретним ключем (симетрична схема);

– шифри з відкритим ключем (асиметрична схема).

Перший тип шифрів передбачає наявність інформації (ключа), володіння якою дає змогу як зашифрувати, так і розшифрувати повідомлення. Шифри з відкритим ключем – відкритого і закритого типу; один використовується для шифрування, інший для розшифровки повідомлень.

Основні напрями шифрування:

– шифрування даних на локальних дискових системах (клієнтське шифрування);

– криптографічний алгоритм (шифр) – математичний спосіб обробки інформації для приховування її змісту.

Основні тенденції застосування шифрування:

– шифрування окремих файлів;

– шифрування окремих розділів на жорсткому диску, віртуальних дисків;

– шифрування жорстких дисків повністю.

Електронний підпис (ЕП) – послідовність символів, отримана внаслідок криптографічного перетворення вихідної інформації з використанням закритого ключа ЕЦП, яка дає змогу підтверджувати цілісність і незмінність цієї інформації, а також її авторство за умови використання відкритого ключа ЕП і його сертифіката.

Цифровий підпис забезпечує:

– вихідні джерела документа. Залежно від деталей визначення «документа» можуть бути підписані поля автор, внесені зміни, мітка часу та ін.;

– захист від змін документа. У разі будь-якої випадкової або навмисної зміни документа (або підпису) зміниться хеш (хеш-функція, або геш-функція – функція, що перетворює вхідні дані будь-якого розміру в дані фіксованого розміру), отже, підпис стане недійсним;

– неможливість відмови від авторства. Оскільки створити коректний підпис можна лише знаючи закритий ключ, а він відомий тільки власнику, то власник не може відмовитися від свого підпису під документом.

Для підпису документа спочатку обчислюється значення хеш-функції для документа, а потім це значення за спеціальним криптоалгоритмом підписується секретним ключем автора документа.

Для перевірки документа на справжність необхідно за допомогою відкритого ключа перевірити підпис, потім обчислити його хеш-значення і порівняти з підписаним контрольним підписом. Якщо обидва значення збігаються, то підпис правильний, в іншому випадку документ недійсний.

1.4. Інформаційні ризики

Сучасні системи спеціального призначення характеризуються наявністю в своєму складі інформаційних систем (ІС). Реалії часу диктують необхідність в умовах обмеженої можливості фінансування розробки ІС отримати оцінку розумної достатності захищеності таких ІС від ризиків. Класичне визначення ризику визначає його як комбінацію ймовірності події та її наслідків [ISO Guide 73:2002]. Серед різновидів ризиків українські та зарубіжні автори виділяють операційний ризик відповідно до Базель ІІІ (Базель ІІІ – документ Базельського комітету з банківського нагляду, що містить методичні рекомендації в області банківського регулювання), що визначається ризиком прямих або непрямих втрат, джерелами яких можуть бути невідповідні або неправильно організовані внутрішні процеси, людські ресурси і системи або зовнішні події. Наслідком виникнення таких подій є зниження ймовірності, повноти та актуальності створюваної і інформації, що обробляється.

Отже, інформаційний ризик може бути визначений як різновид операційного ризику, що відбувається внаслідок неадекватних і помилкових внутрішніх процесів, дій працівників або зовнішніх подій. Стандарт ISO 27000:2018 вказує: інформаційний ризик – це потенційна можливість того, що загроза буде використовувати вразливість активу або групи активів, завдаючи шкоди організації.

Ризик викликає інцидент інформаційної безпеки – одна або серія небажаних чи несподіваних подій інформаційної безпеки, що мають значну ймовірність порушення бізнес-операцій або становлять загрозу для інформаційної безпеки [ISO/IEC TR 15446:2017]. Отже, приступаючи до аналізу інформаційних ризиків, необхідно визначити перелік об’єктів і їх вразливостей, на які спрямовані атаки, реалізуючи загрози. Інформаційні ризики спрямовані на такі види активів: інформація, мережеве, системне і прикладне програмне забезпечення, персональні комп’ютери, накопичувальні і друкувальні пристрої, мережеві сервери, шлюзи, інтерфейси, сервіси.

Витік інформації

Сьогодні більшість підприємств використовують багаторівневі системи обробки інформації – комп'ютери, хмарні сховища, корпоративні мережі та ін. Усі ці системи не тільки передають дані, але і є середовищем їх можливого витоку. Витік секретної інформації – процес неконтрольованого розголошення ключових даних.

Комерційна таємниця – інформація про організацію діяльності підприємства, технології розробки продукції, дані про грошові потоки, інтелектуальну власність та інші відомості, завдяки володінню яким отримуються фінансові вигоди.

Причина 1 – Персонал

Кожен співробітник підприємства є потенційною загрозою для безпеки інформації. Часто люди забирають роботу додому – переміщують робочі файли на свої флеш-носії, передають їх незахищеними каналами з'єднання, обговорюють інформацію зі співробітниками конкуруючих компаній.

Дії персоналу бувають навмисними і ненавмисними. Ненавмисні дії – це наслідок незнання регламенту роботи з комерційною інформацією. Ризик витоку інформації від персоналу є завжди, і його не можна виключити повністю. Служба безпеки може вжити заходів щодо обмежень взаємодії працівників з конфіденційною інформацією та впровадити правила розмежування доступу.

Правила – перелік чітких прав і обмежень, що повинні дотримуватися кожним співробітником. Їх основний принцип – кожен працівник взаємодіє тільки з тими даними, які потрібні для його роботи. Отже, простий менеджер не зможе дізнатися технологію розробки продукції та інші важливі дані, які бажає знати зловмисник.

Питаннями контролю роботи персоналу з секретними матеріалами повинен займатися уповноважений співробітник або відділ безпеки. Їх завдання – стежити за діяльністю працівників протягом усього робочого дня й оперативно виявляти всі випадки витоку інформації.

На практиці виявити людину, що зливає комерційну таємницю, можна за такими ознаками:

– *Співробітник без попередження затримується після роботи на своєму робочому місці.* В такому випадку є ймовірність того, що він намагається отримати доступ до секретної інформації в момент, коли поруч нікого немає. На такого працівника потрібно звернути увагу і простежити, чи не є його метою дізнатися таємні відомості. Контролювати час перебування персоналу на робочому місці допомагають спеціальні системи обліку доступу. Починати розслідування потрібно лише в тому випадку, якщо стали відомі конкретні факти витоку інформації, що захищається.

– *Співробітник зберігає на свій персональний комп'ютер або смартфон занадто багато електронних документів компанії.* Такий варіант витоку можна відстежити в компаніях, що використовують системи захисту файлової системи. Суть їх роботи полягає у створенні загального сервера, що діє в межах однієї корпоративної або Wi-Fi-мережі. Під час кожного відкриття, копіювання та переміщення даних на службовому комп'ютері вся інформація про процеси надходить на сервер. Отже, адміністратор безпеки може виявити, з якого комп'ютера і в якій кількості була переміщена секретна інформація.

– *Співробітник без необхідності копіює паперовий документообіг електронним (сканує документи або фотографує).* Згідно з нормами документування, всі фізичні папки і файли з комерційною таємницею повинні зберігатися в захищеній частині архіву. Доступ до документів можливий тільки для уповноважених працівників. Усі дані про отримання документа з таємницею для користування повинні документуватися (із зазначенням імені працівника і точного часу видачі документа). Якщо ж секретний документ потрапив у руки недобросовісного співробітника, відстежити його несанкціоноване копіювання можна на сканері або ксероксі, що зберігає звіт щодо діяльності за останній час. Також існують факсимільні апарати, доступ до яких можливий тільки після правильного введення пари «ідентифікатор користувача – пароль».

– *Працівник регулярно порушує загальні вимоги безпеки під час роботи з комерційною таємницею.* Якщо персонал регулярно намагається обійти систему заборони, переглядаючи заборонені ресурси, або використовує особисту техніку для обробки секретних даних, необхідно впровадити додаткові системи контролю користувачів. Наприклад, DLP-системи. Їх завдання полягає в моніторингу всіх листувань користувачів з комерційної пошти та інших електронних скриньок, які зареєстровані в системі. Також модуль захисту забороняє установку стороннього ПЗ, а всі дії співробітника за комп'ютером видно адміністратору безпеки.

– *Співробітник був викритий в контактах із службовцями конкуруючих компаній.* У великих компаніях працівники часто спілкуються поза робочим часом. Отже, вони отримують більше інформації один про одного і можуть дізнатися про зв'язки колеги і працівника конкуруючої організації. Ймовірність звичайних дружніх відносин між людьми теж можлива, але краще оповістити керівництво компанії про це, щоб уникнути непотрібних підозр.

Причина 2 – Проблеми підбору кадрів

Часта зміна персоналу, масштабні зміни в організації роботи компанії, зниження заробітних плат, скорочення співробітників – усе це є частиною «плинності» кадрів. Таке явище часто стає причиною витоку секретної інформації.

Криза, нестача коштів для видачі зарплат змушують керівництво погіршувати умови роботи персоналу. Внаслідок цього підвищується невдоволення

працівників, які можуть звільнитися або просто почати поширювати секретні дані конкурентам. Проблема зміни персоналу особливо важлива для керівних посад, адже всі керівники повинні мати доступ до секретної документації. Загрозу поширення таємниці можуть нести не тільки ті співробітники, які звільнилися, але і поточні працівники, рівень мотивації яких знижений.

Для запобігання проблеми потрібно створити для працівників максимально комфортні умови роботи. У разі серйозної кризи рекомендується зібрати персонал для обговорення можливих шляхів виходу зі складної ситуації. Важливо повідомляти співробітників про всі зміни в нарахуванні заробітних плат заздалегідь, а не за фактом виплати окладу.

Часом несприятливу атмосферу в колективі створює один співробітник. Тоді буде актуальним установлення систем автоматизованого профайлінгу, які аналізують листування працівників в електронній пошті і месенджерах та створюють їх психологічні портрети. Система визначає позитивні і негативні риси характеру людини, що дає змогу приймати правильні управлінські рішення.

Для усунення «плинності» працівників важливо виконувати такі рекомендації:

– *Налагодження системи найму кадрів.* Усі передові організації мають спеціальний відділ, що займається питаннями найму, звільнення і підтримки співробітників. Не варто шукати працівника на вакансію, що звільнилася або з'явилася, якомога швидше. Хороший HR (фахівець із підбору кадрів – Human resources) зобов'язаний прослухати кілька претендентів на посаду, поширити інформацію про вакансію на популярних інтернет-майданчиках, провести підсумковий конкурс, результати якого визначать кандидатуру, яка найбільше підходить.

– *Впровадження системи винагород.* За успіхи в роботі, перевиконання планів і укладення вигідних контрактів співробітників потрібно заохочувати. Прикладами заохочення можуть бути підвищення заробітної плати, покращення умов роботи, просування кар'єрними сходами.

– *Надання всім співробітникам можливості професійного зростання, підвищення кваліфікації.* Хороші компанії завжди відправляють своїх співробітників на курси підвищення кваліфікації або закуповують онлайн-тренінги для більш зручного проходження навчання. Також рекомендується організовувати тренінги від провідних професіоналів галузі.

Причина 3 – Відрядження

Робочий процес фірми включає ділові зустрічі, поїздки в інші філії компанії, країни. Співробітники, які часто виїжджають у відрядження, можуть ненавмисно стати основною причиною витоку секретної інформації підприємства.

У поїздці такий працівник завжди має при собі особистий або корпоративний ноутбук / смартфон, що обробляє захищені документи. Техніка може бути залишена в громадському місці, зламана або викрадена. Якщо за співробітником ведеться стеження або він зустрічається з керівниками конкуруючої компанії, загублений ноутбук може стати головним джерелом розголошення службової інформації.

Для запобігання подібним випадкам важливо використовувати системи шифрування жорсткого диска тих ПК, що видаються співробітникам на час ділових зустрічей. Навіть внаслідок крадіжки і несанкціонованого доступу інформація буде надійно захищена, і зламати її без знання ключа буде неможливо.

Причина 4 – Співпраця з іншими компаніями

Більшість автоматизованих систем захисту здатні обмежити доступ до службової інформації тільки в межах однієї будівлі або одного підприємства (якщо кілька філій використовують загальний сервер зберігання даних). У процесі спільного виконання проєкту декількома фірмами служби безпеки не можуть повною мірою простежити за тим, як реалізується доступ до службової таємниці кожного з підприємств. Як і в попередньому випадку, використання криптоконтейнера (систем шифрування жорсткого диска) дасть змогу захистити таємну інформацію від злому.

Причина 5 – Використання складних IT-інфраструктур

Великі корпорації використовують комплексні системи захисту службових відомостей. Автоматизовані системи передбачають наявність декількох відділів безпеки і роботу понад п’яти системних адміністраторів, завдання яких полягає в підтримці збереження комерційної таємниці.

Складність системи теж є ризиком витоку, адже одночасна робота кількох людей може бути незлагодженою. Наприклад, один адміністратор може впровадити або видалити правила розмежування доступу, а інший – забути внести дані прав доступу до серверів. Під час використання складних систем захисту інформації важливо грамотно розподіляти всі обов’язки і контролювати їх своєчасне виконання. В іншому випадку – створена система може нашкодити компанії. Наприклад, можна розмежувати доступ співробітників служби безпеки до певних звітів і операцій у системі. Максимальну кількість повноважень надійніше довірити керівнику ІБ-служби.

Причина 6 – Поломки техніки

Помилки в роботі ПЗ

Всілякі збої в роботі програмного забезпечення виникають постійно. В момент появи вразливості захищені файли ризикують стати перехопленими хакером. Важливо вчасно виявляти всі неполадки в роботі встановлених програмних і апаратних компонентів. За працездатність і взаємодію всіх модулів захисту

відповідальний адміністратор безпеки. Внаслідок збою в базі даних втрачається значна кількість важливої документації. Відновлення жорстких дисків – це складне завдання, що не дає гарантії повернення втрачених відомостей.

Збої в роботі серверного обладнання

Безпечніше зберігати всю інформацію з використанням хмарних сховищ. Cloud-платформи підвищують швидкість обробки інформації. З їх допомогою кожен співробітник зможе отримати доступ до потрібних файлів з будь-якого пристрою. Система шифрування використовується віддаленим сервером, тому немає необхідності захищати канали передачі.

Збої на серверах постачальника послуг можуть траплятися через природні катаклізми або через масивні хакерські атаки. Зазвичай власники хмарних платформ завжди зберігають архівовані резервні копії вмісту акаунтів користувачів, тому збої швидко ліквідуються без втрати важливих документів.

Поломки технічних засобів захисту

Для збереження комерційної таємниці рекомендується захищати не тільки операційні системи і гаджети, але і весь периметр офісного приміщення, а також зону контролю вуличних комунікацій. Для цих цілей використовуються заглушки на вікна, ущільнювачі архітектурних конструкцій (для запобігання прослуховувань), пристрої для екранування і зашумлення (для неможливості перехоплення радіохвиль), інші гаджети. Через поломку одного з таких пристроїв виникає канал витоку інформації, що стає доступним зловмисникові для перехоплення секретних даних.

У разі поломки комп’ютерів та інших засобів обробки даних їх необхідно відремонтувати в сервісному центрі. Винос гаджета за межі приміщення і передача його сторонній людині (навіть якщо він не зацікавлений в отриманні службової таємниці) є можливою причиною витоку. Департамент безпеки компанії не може контролювати гаджети, поки вони знаходяться за межами фірми.

Причина 7 – Витік з технічних каналів передачі даних

Канал витоку даних – це фізичне середовище, всередині якого не контролюється поширення таємної інформації. На будь-якому підприємстві, що використовує комп’ютери, серверні стійки, мережі, є канали витоку. З їх допомогою зловмисник може отримати доступ до комерційної таємниці.

Мовний канал витоку

Конкуренти часто використовують прослуховувачі та інші закладки, за допомогою яких відбувається крадіжка таємниці.

Віброакустичний канал витоку

Цей канал витоку виникає в процесі зіткнення звуку з архітектурними конструкціями (стінами, підлогою, вікнами). Вібраційні хвилі можна зчитати і перевести в мовний текст. За допомогою спрямованих мікрофонів на відстані

до 200 метрів від приміщення зловмисник може зчитати розмову, в якій фігурує службова інформація.

Електромагнітний канал витоку

Внаслідок роботи всіх технічних засобів виникає магнітне поле. Між апаратними елементами передаються сигнали, що можна зчитати спеціальним обладнанням на великих відстанях і отримати секретні дані.

Візуальний канал витоку

Приклад появи візуального каналу крадіжки – це проведення нарад і конференцій з неприкритими вікнами. З сусіднього будинку зловмисник може легко переглянути всю інформацію. Також можливі варіанти використання відеозакладок, які передають картинку того, що відбувається, конкурентам.

Для захисту технічних каналів витоку рекомендується використовувати:

– *Тепловізор.* За допомогою такого девайса можна просканувати всі стіни і частини інтер'єру на наявність закладних пристроїв (жучків, відеокамер).

– *Пристрої, що заглушають подачу сигналу радіочастот*.

– *Засоби захисту архітектурних конструкцій* – ущільнювачі для вікон, дверей, підлоги і стелі. Вони ізолюють звук і унеможливлюють зчитування вібраційних хвиль з поверхні будівлі.

– *Пристрої для екранування і зашумлення.* Вони використовуються для захисту електромагнітного каналу витоку.

Також варто заземлити всі комунікації, що виходять за межі приміщення і контрольованої зони (труби, кабелі, лінії зв'язку).

Існує кілька дієвих способів, що допоможуть знизити ризик витоку і розголошення інформації. Підприємство може використовувати всі методи захисту або тільки кілька з них, адже система безпеки повинна бути економічно вигідною. Збитки від втрати секретної інформації не можуть бути менше вартості впровадження та підтримки системи безпеки.

Шифрування

Це простий і дієвий метод захисту комерційної таємниці. Сучасні алгоритми шифрування використовують світові стандарти в області криптографії (шифри AES, ГОСТ), двосторонній обмін ключами (з його допомогою хакер не зможе зламати шифр навіть після отримання доступу до каналу передачі), еліптичні криві для генерації захисту. Такий підхід робить злом шифрованого повідомлення неможливим для стандартних комп'ютерів.

Переваги використання шифрування з метою запобігання витоку комерційної інформації:

Простота застосування. Реалізація шифрування проводиться спеціальним ПЗ. Програма повинна бути встановлена на всі комп'ютери і мобільні пристрої,

в яких циркулює секретна інформація. Роботу додатка налаштовує системний адміністратор або адміністратор безпеки. Отже, звичайному користувачеві автоматизованих систем не потрібно вчитися використовувати систему захисту. Всі файли шифруються і дешифруються автоматично в межах корпоративної мережі.

У разі необхідності передачі важливих електронних документів за межі комерційної мережі вони будуть зберігатися на флеш-носії, хмарному носії або в клієнтській пошті виключно в зашифрованому вигляді. Недолік – без спеціального ПЗ працівник не зможе переглянути вміст файла.

Високий ступінь надійності. З використанням потужних обчислювальних алгоритмів криптографії зловмисникові складно перехопити секретні повідомлення або трафік фірми, а розшифровка без знання відкритого і закритого ключа неможлива.

Зазначимо, що шифрування є не єдиним варіантом захисту таємниці від усіх можливих атак. Працівники здатні без проблем прочитати вміст електронних документів у межах комерційної мережі, тому ризик несанкціонованого розголошення третім особам залишається. Використання криптографії є невід'ємною частиною функціоналу кожної комплексної системи безпеки.

Контроль персоналу

Якщо технічні засоби легко контролювати, то персонал є одним з найнебезпечніших джерел витоку. Людський фактор наявний завжди, і навіть співробітники відділу безпеки не завжди можуть встановити, від якого працівника може виходити загроза.

Зазвичай пошук зловмисника серед персоналу виконується вже тоді, коли стали відомі перші випадки передачі даних конкурентам. Адміністратори безпеки перевіряють можливість перехоплення інформації технічними каналами витоку, і якщо всі канали надійно захищені, підозра падає на працівників.

Діяльність співробітників організації контролюється за допомогою систем обліку робочого часу. Це комплексне апаратне і програмне забезпечення, що документує точний час прибуття на роботу, час догляду, діяльність персоналу за комп'ютером, записує листування корпоративної пошти, проводить відеоспостереження і передає всі ці дані керівництву фірми або керівнику відділу безпеки. Далі вся отримана інформації аналізується і виявляється кількість працівників, які могли поширювати комерційну таємницю.

Норми документування та передачі комерційної таємниці

Захищати треба не тільки електронні документи, а й усю друковану документацію, що містить секретні відомості. Відповідно до Закону «Про зберігання і обробку відомостей, що містять комерційну таємницю», треба виконувати такі вимоги:

– Зберігати всі документи з комерційною таємницею виключно в окремих закритих приміщеннях, що охороняються цілодобово системами відеоспостереження або охоронцями.

– Доступ до службової таємниці можуть мати тільки співробітники, яким вона потрібна в процесі роботи.

– Запис про вилучення документа з архіву вноситься до реєстраційного журналу. Вказується точна дата, гриф документа та ініціали особи, яка здобула копію файла. Аналогічні дії проводяться під час повернення об'єкта.

– Документ, що містить комерційну таємницю, не можна виносити за межі офісу без повідомлення про це керівника департаменту безпеки.

Для передачі таємних документів між філіями підприємства використовується фельд'єгерська пошта – захищена кур'єрська передача документів особливої важливості.

Контрольні питання:

1. Поняття інформаційної безпеки.
2. Основні завдання інформаційної безпеки.
3. Фактори обумовлення інформаційних загроз.
4. Приклади внутрішніх загроз безпеці інформації.
5. Приклади зовнішніх загроз безпеці інформації.
6. Що таке хакерські атаки? Приклади.
7. Методи захисту від хакерських атак.
8. Що таке технологія інфраструктури відкритих ключів?
9. Особливість системи багатофакторної автентифікації.
10. Особливість біометричних систем. Приклади.
11. Суть біометричного захисту даних.
12. Методи криптографічного захисту даних.
13. Призначення електронного підпису.
14. Автентифікація та ідентифікація.

ТЕМА 2
ІНФОРМАЦІЙНА СИСТЕМА ПЕРСОНАЛЬНИХ ДАНИХ

У темі наведені нормативні документи, прийняті для захисту даних. Детально описані закони України: «Про захист інформації в інформаційно-телекомунікаційних системах», «Про криптографічний та технічний захист інформації». Приділено багато уваги термінам «конфіденційність персональних даних», «захист персональної інформації» та детально описана європейська система захисту персональних даних.

Ключові слова: *Закон України «Про інформацію», документ, захист інформації, інформація, суб'єкт владних повноважень, основні принципи інформаційних відносин, основні напрями державної інформаційної політики, інформація про фізичну особу, інформація довідково-енциклопедичного характеру, інформація про стан довкілля, інформація про товар, науково-технічна інформація, податкова інформація, правова інформація, статистична інформація, соціологічна інформація, доступ до інформації, інформація з обмеженим доступом, Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», блокування інформації в системі, витік інформації, власник інформації, власник системи, доступ до інформації в системі, захист інформації в системі, знищення інформації в системі, інформаційна (автоматизована) система, інформаційно-телекомунікаційна система, комплексна система захисту інформації, користувач інформації в системі, криптографічний захист інформації, несанкціоновані дії щодо інформації в системі, обробка інформації в системі, порушення цілісності інформації в системі, порядок доступу до інформації в системі, телекомунікаційна система, технічний захист інформації, відповідальність за забезпечення захисту інформації в системі, Закон України Про криптографічний та технічний захист інформації, обробка персональних даних, інформаційна система персональних даних, правові засади захисту персональних даних.*

План

2.1. Нормативні документи захисту даних.
2.2. Конфіденційність персональних даних.
2.3. Захист персональної інформації.
2.4. Європейська система захисту персональних даних.

2.1. Нормативні документи захисту даних

В Україні розроблено і впроваджено такі законодавчі та нормативні документи щодо захисту інформації, технічного захисту інформації, захисту персональних даних, електронного цифрового підпису, технічного захисту інформації:

– Закон України «Про захист персональних даних»;

– Закон України «Про інформацію»;

– Закон України «Про доступ до публічної інформації»;

– Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»;

– Закон України «Про телекомунікації»;

– Закон України «Про ліцензування видів господарської діяльності»;

– Концепція технічного захисту інформації в Україні. Затверджено постановою Кабінету Міністрів України від 08.10.1997 № 1126;

– Постанова Кабінету Міністрів України від 25.05.2011 № 616 «Про затвердження Положення про Державний реєстр баз персональних даних та порядок його ведення»;

– Постанова Кабінету Міністрів України від 29.10.2000 № 1755 «Про термін дії ліцензії на провадження певних видів господарської діяльності, розміри і порядок зарахування плати за її видачу»;

– Постанова Кабінету Міністрів України від 16.11.2016 № 821 «Деякі питання ліцензування господарської діяльності з надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації за переліком, що визначається Кабінетом Міністрів України»;

– Постанова Кабінету Міністрів України від 21.06.2017 № 437 «Про затвердження критеріїв, за якими оцінюється ступінь ризику від провадження господарської діяльності, що підлягає ліцензуванню, у сфері надання послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та технічного захисту інформації за переліком, що визначається Кабінетом Міністрів України, і встановлюється періодичність проведення планових заходів державного нагляду (контролю) Адміністрацією Державної служби спеціального зв'язку та захисту інформації»;

– Положення про технічний захист інформації в Україні. Затверджено Указом Президента України від 27.09.1999 № 1229;

– Постанова Кабінету Міністрів України від 13.03.2002 № 281 «Про деякі питання захисту інформації, охорона якої забезпечується державою»;

– Постанова Кабінету Міністрів України від 29.03.2006 № 373 «Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах»;

– Постанова Кабінету Міністрів України від 12.04.2002 № 522 «Порядок підключення до глобальних мереж передачі даних»;

– Положення про порядок надання відомостей з Єдиного державного реєстру юридичних осіб та фізичних осіб-підприємців, затверджено Наказом

Державного комітету України з питань регуляторної політики та підприємництва 20.10.2005 № 97, Зареєстровано в Міністерстві юстиції України 28 жовтня 2005 р. за № 1294/11574;

– Положення про державну експертизу в сфері технічного захисту інформації, затверджене наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України 16.05.2007 № 93, зареєстровано в Міністерстві юстиції України 16.07.2007 за № 820/14087;

– Положення про державний контроль за станом технічного захисту інформації, затверджене наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України 16.05.2007 № 87, зареєстровано в Міністерстві юстиції України 10.07.2007 за № 785/14052;

– Правила проведення робіт із сертифікації засобів захисту інформації, затверджені наказом Держспоживстандарту та Адміністрації Держспецзв'язку від 25.04.2007 № 75/91 та зареєстровані у Мін'юсті 14.05.2007 № 498/13765;

– Порядок формування реєстру організаторів державної експертизи у сфері технічного захисту інформації та реєстру експертів з питань технічного захисту інформації, затверджений наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України 16.04.2008 № 64;

– Порядок оновлення антивірусних програмних засобів, що мають позитивний експертний висновок за результатами державної експертизи в сфері ТЗІ, затверджений наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України 26.03.2007 № 45;

– Тимчасове положення про категоріювання об'єктів від 10.07.1995 № 35;

– ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення;

– ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт;

– ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення;

– НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу;

– НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу;

– НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі;

– НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації захисту інформації в комп'ютерних системах від несанкціонованого доступу;

– НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу;

– НД ТЗІ 2.5-008-2002. Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2;

– НД ТЗІ 2.5-010-2003. Вимоги із захисту інформації WEB-сторінки від несанкціонованого доступу;

– НД ТЗІ 3.6-001-2000. Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу;

– НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі (зі зміною № 1, затвердженою наказом ДСТСЗІ СБ України 18.06.2002 № 37);

– НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі;

– НД ТЗІ 1.1-005-07. Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення;

– НД ТЗІ 2.1-002-07. Захист інформації на об'єктах інформаційної діяльності. Випробування комплексу технічного захисту інформації. Основні положення;

– НД ТЗІ 3.1-001-07. Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації;

– НД ТЗІ 3.3-001-07. Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації.

У **Законі України «Про інформацію»** від 02.10.1992 р. № 2657-XII (остання редакція від 21.12.2019) [34], який регулює відносини щодо створення, збирання, отримання, зберігання, використання, поширення, охорони, захисту інформації, визначаються основні терміни та положення про інформацію. Розглянемо такі основні терміни:

– **документ** – матеріальний носій, що містить інформацію, основними функціями якого є її збереження та передавання у часі та просторі;

– **захист інформації** – сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї;

– **інформація** – будь-які відомості та/або дані, що можуть бути збережені на матеріальних носіях або відображені в електронному вигляді;

– **суб'єкт владних повноважень** – орган державної влади, орган місцевого самоврядування, інший суб'єкт, що здійснює владні управлінські функції відповідно до законодавства, зокрема на виконання делегованих повноважень.

Основними принципами інформаційних відношень є:

– гарантованість права на інформацію;

– відкритість, доступність інформації, свобода обміну інформацією;

– достовірність і повнота інформації;

– свобода вираження поглядів і переконань;

– правомірність отримання, використання, поширення, зберігання та захисту інформації;

– захищеність особи від втручання в її особисте та сімейне життя.

Основними напрямами державної інформаційної політики є:

– забезпечення доступу кожного громадянина до інформації;

– забезпечення рівних можливостей щодо створення, збирання, отримання, зберігання, використання, поширення, охорони, захисту інформації;

– створення умов для формування в Україні інформаційного суспільства;

– забезпечення відкритості та прозорості діяльності суб'єктів владних повноважень;

– створення інформаційних систем і мереж інформації, розвиток електронного урядування;

– постійне оновлення, збагачення та зберігання національних інформаційних ресурсів;

– забезпечення інформаційної безпеки України;

– сприяння міжнародній співпраці в інформаційній сфері та входженню України до світового інформаційного простору.

Кожен громадянин має право на інформацію, що передбачає можливість вільного отримання, використання, поширення, зберігання та захисту інформації, необхідної для реалізації своїх прав, свобод і законних інтересів.

Реалізація права на інформацію не повинна порушувати громадські, політичні, економічні, соціальні, духовні, екологічні та інші права, свободи і законні інтереси інших громадян, права та інтереси юридичних осіб.

Право на інформацію може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку, з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя.

Право на інформацію охороняється законом. Держава гарантує всім суб'єктам інформаційних відносин рівні права і можливості доступу до інформації.

За змістом інформація поділяється на такі види:

Інформація про фізичну особу (персональні дані) – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

Інформація довідково-енциклопедичного характеру – систематизовані, документовані, публічно оголошені або в інший спосіб поширені відомості про суспільне, державне життя та навколишнє природне середовище.

Інформація про стан довкілля (екологічна інформація) – відомості та/або дані про: стан складників довкілля та його компоненти, фактори, що впливають або можуть впливати на складники довкілля, стан здоров'я та безпеки людей, умови життя людей, стан об'єктів культури і споруд тією мірою, якою на них впливає або може вплинути стан складових довкілля.

Інформація про товар (роботу, послугу) – відомості та/або дані, що розкривають кількісні, якісні та інші характеристики товару про вплив товару (роботи, послуги) на життя та здоров'я людини. Правовий режим інформації про товар (роботу, послугу) визначається законами України про захист прав споживачів, про рекламу, іншими законами та міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України.

Науково-технічна інформація – будь-які відомості та/або дані про вітчизняні та зарубіжні досягнення науки, техніки і виробництва, отримані внаслідок науково-дослідної, дослідно-конструкторської, проєктно-технологічної, виробничої та громадської діяльності, що можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

Правовий режим науково-технічної інформації визначається Законом України «Про науково-технічну інформацію», іншими законами та міжнародними договорами України, згода надана Верховною Радою України.

Податкова інформація – сукупність відомостей і даних, що створені або отримані суб'єктами інформаційних відносин у процесі поточної діяльності і необхідні для реалізації покладених на контролюючі органи завдань і функцій у порядку, встановленому Податковим кодексом України.

Правова інформація – будь-які відомості про право, його систему, джерела, реалізацію, юридичні факти, правовідносини, правопорядок, правопорушення і боротьбу з ними та їх профілактику тощо. Джерелами правової інформації є Конституція України, інші законодавчі і підзаконні нормативно-правові акти, міжнародні договори та угоди, норми і принципи міжнародного права, а також ненормативні правові акти, повідомлення засобів масової інформації, публічні виступи, інші джерела інформації з правових питань.

Статистична інформація – документована інформація, що дає кількісну характеристику масових явищ та процесів, які відбуваються в економічній, соціальній, культурній та інших сферах життя суспільства. Правовий режим державної статистичної інформації визначається Законом України «Про державну статистику», іншими законами та міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України.

Соціологічна інформація – будь-які документовані відомості про ставлення до окремих осіб, подій, явищ, процесів, фактів тощо. Правовий режим соціологічної інформації визначається законами та міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України.

За доступом до інформації виділяють відкриту інформацію та інформацію з обмеженим доступом.

Інформацією з обмеженим доступом є конфіденційна, таємна та службова інформація. Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом. Відносини, пов'язані з правовим режимом конфіденційної інформації, регулюються законом.

Згідно з визначенням інформаційної безпеки, вона залежить не тільки від комп'ютерів, але і від підтримуючої інфраструктури, до якої належать системи електро-, водо- і теплопостачання, кондиціонери, засоби комунікацій і, звичайно, обслуговуючий персонал. Ця інфраструктура має самостійну цінність, але нас цікавитиме лише те, як вона впливає на виконання інформаційною системою запропонованих їй функцій.

Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» № 80/94-ВР від 05.07.1994 р., чинний (остання редакція від 19.04.2014) [35].

У цьому Законі наведені нижче терміни вживаються в такому значенні:

– **блокування інформації в системі –** дії, внаслідок яких унеможливлюється доступ до інформації в системі;

– **виток інформації** – результат дій, внаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї;

– **власник інформації** – фізична або юридична особа, якій належать права на інформацію;

– **власник системи** – фізична або юридична особа, якій належить право власності на систему;

– **доступ до інформації в системі** – отримання користувачем можливості обробляти інформацію в системі;

– **захист інформації в системі** – діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі;

– **знищення інформації в системі** – дії, внаслідок яких інформація в системі зникає;

– **інформаційна** (автоматизована) **система** – організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів;

– **інформаційно-телекомунікаційна система** – сукупність інформаційних та телекомунікаційних систем, які в процесі обробки інформації діють як єдине ціле;

– **комплексна система захисту інформації** – взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації;

– **користувач інформації в системі** (далі – користувач) – фізична або юридична особа, яка в установленому законодавством порядку отримала право доступу до інформації в системі;

– **криптографічний захист інформації** – вид захисту інформації, що реалізується шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховування / відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо;

– **несанкціоновані дії щодо інформації в системі** – дії, що провадяться з порушенням порядку доступу до цієї інформації, установленого відповідно до законодавства;

– **обробка інформації в системі** – виконання однієї або кількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів;

– **порушення цілісності інформації в системі** – несанкціоновані дії щодо інформації в системі, внаслідок яких змінюється її вміст;

– **порядок доступу до інформації в системі** – умови отримання користувачем можливості обробляти інформацію в системі та правила обробки цієї інформації;

– **телекомунікаційна система** – сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб;

– **технічний захист інформації** – вид захисту інформації, спрямований на забезпечення за допомогою інженерно-технічних заходів та/або програмних і технічних засобів унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації.

Відповідальність за забезпечення захисту інформації в системі покладається на власника системи. Власник системи, в якій обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо

захисту якої встановлена законом, утворює службу захисту інформації або призначає осіб, на яких покладається забезпечення захисту інформації та контролю за ним.

Вимоги до забезпечення захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, встановлюються Кабінетом Міністрів України.

Спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації:

– розробляє пропозиції щодо державної політики у сфері захисту інформації та забезпечує її реалізацію в межах своєї компетенції;

– визначає вимоги та порядок створення комплексної системи захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;

– організовує проведення державної експертизи комплексних систем захисту інформації, експертизи та підтвердження відповідності засобів технічного і криптографічного захисту інформації;

– здійснює контроль за забезпеченням захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;

– здійснює заходи щодо виявлення загрози державним інформаційним ресурсам від несанкціонованих дій в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах та дає рекомендації з питань запобігання такій загрозі.

Державні органи в межах своїх повноважень за погодженням відповідно зі спеціально уповноваженим центральним органом виконавчої влади з питань організації спеціального зв'язку та захисту інформації або підпорядкованим йому регіональним органом, встановлюють особливості захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом.

За законом особливості захисту інформації в системах, що забезпечують банківську діяльність, встановлюються Національним банком України.

Особи, винні в порушенні законодавства про захист інформації в системах, несуть відповідальність згідно із законом.

Державний стандарт України ДСТУ 3396.0-96, чинний від 01.01.1997 р., включає захист інформації, технічний захист інформації, основні положення.

Цей стандарт встановлює об'єкт, мету, основні організаційно-технічні положення забезпечення технічного захисту інформації (ТЗІ), неправомірний доступ до якої може завдати шкоди громадянам, організаціям (юридичним особам) та державі, а також категорії нормативних документів системи ТЗІ.

Вимоги стандарту обов'язкові для підприємств та установ усіх форм власності і підпорядкування, громадян-суб'єктів підприємницької діяльності, органів державної влади, органів місцевого самоврядування, військових частин усіх військових формувань, представництв України за кордоном, які володіють, користуються та розпоряджаються інформацією, що підлягає технічному захисту.

Закон України Про криптографічний та технічний захист інформації (проєкт, неофіційний текст від 12.03.2016 р., не набрав чинності). Цей Закон визначає правові та організаційні засади криптографічного та технічного захисту важливої для держави, суспільства і особи інформації, що обробляється або озвучується на об'єктах інформаційної діяльності та в інформаційно-телекомунікаційних системах, охорона якої забезпечується державою відповідно до законодавства, регулює відносини між суб'єктами у цій сфері.

2.2. Конфіденційність персональних даних

Необхідність забезпечення безпеки персональних даних у наш час – об'єктивна реальність. Сучасна людина не може самостійно протидіяти посяганню на її приватне життя. Підвищені технічні можливості щодо збору та обробки персональної інформації, розвиток засобів електронної комерції і соціальних мереж роблять необхідним вжиття заходів щодо захисту персональних даних.

Розглянемо декілька прикладів із повсякденного життя, коли порушуються права людини на конфіденційність персональних даних. Буває так, що під час оформлення дисконтної картки в магазині покупець вказує такі відомості: прізвище, номер телефону, електронну адресу, а потім отримує повідомлення і листи абсолютно з інших магазинів, в яких ніколи не бував, тобто магазин без згоди покупця передав його дані третім особам. Якщо газета друкує ПІБ і суми виграшу переможців лотереї без їх відома, чи об'єднання співвласників багатоквартирного будинку вивішує на під'їзді списки боржників і суму їх боргу – це приклади «нешкідливих» витоків. Крадіжка персональних даних може завдати правовласнику відчутної матеріальної шкоди, якщо йдеться про кредитні картки або інформацію про банківські заощадження. Зловмисники, які володіють достатніми технічними знаннями, викрадають реквізити банківських карт (скімінг) або імітують сайти фінансових установ, щоби змусити користувача показати свою особисту інформацію (фішинг). Насправді важко встановити джерело витоку персональних даних через високу інформатизацію сучасного суспільства.

Держава на законодавчому рівні вимагає від організацій та фізичних осіб, які обробляють персональні дані, забезпечити їх захист. Законодавство України в області захисту персональних даних ґрунтується на Конституції України, міжнародних договорах України, Законі України «Про захист персональних даних»,

Законі України «Про захист інформації в інформаційно-телекомунікаційних системах» та інших нормативних документах.

Метою українського законодавства у сфері захисту персональних даних є забезпечення захисту прав і свобод громадянина під час обробки його персональних даних, зокрема захисту прав на недоторканність приватного життя, особисту і сімейну таємницю. Законодавством регулюються відносини, пов'язані з обробкою персональних даних, що здійснюється державними органами влади, органами місцевого самоврядування, юридичними особами та фізичними особами.

Відповідно до Закону, персональні дані – будь-яка інформація, за допомогою якої можна однозначно ідентифікувати фізичну особу. До персональних даних належать: прізвище, ім'я, по батькові; рік, місяць, дата і місце народження; адреса; сімейний, соціальний, майновий стан; освіта, професія, доходи, інша інформація, що належить суб'єкту.

Операторами персональних даних є державний орган, юридична або фізична особа, які організують і (або) здійснюють обробку персональних даних, а також визначають цілі і зміст обробки персональних даних.

Обробка персональних даних – дії (операції) з персональними даними, зокрема збір, систематизація, накопичення, зберігання, уточнення (оновлення, зміна), використання, поширення (також передача), знеособлення, блокування, знищення персональних даних.

Інформаційна система персональних даних (далі ІСПД) – інформаційна система, що являє собою сукупність персональних даних, які містяться в базі даних, а також інформаційних технологіях і технічних засобах, що дають змогу здійснювати обробку таких персональних даних з використанням засобів автоматизації або без використання таких засобів [7].

Регуляторами називаються органи державної влади, уповноважені здійснювати заходи щодо контролю і нагляду щодо дотримання вимог Закону України «Про захист персональних даних».

Україна в питанні захисту персональних даних спирається на міжнародний досвід. Але в державі поки немає достатньої законодавчої бази і системи, здатної ефективно працювати в сучасних умовах.

2.3. Захист персональної інформації

1. Правові засади захисту персональних даних.

У 2005 р. Україна ратифікувала Конвенцію 1981 р. Ради Європи № 108 «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних». Серед основних зобов'язань держави за зазначеним документом є також прийняття нормативно-правових актів, що повинні сприяти захисту персональних

даних. Через це Верховною Радою України 01.06.2010 р. прийнято Закон України «Про захист персональних даних», що визначив:

– поняття персональних даних – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути ідентифікована (наприклад: інформація про працівника є базою персональних даних, оскільки особисті справи, трудові книжки, копії паспорта, документів про освіту зберігаються та обробляються роботодавцем);

– власник персональних даних – фізична або юридична особа, якій законом або за згодою суб'єкта персональних даних надано право на обробку цих даних, яка затверджує мету обробки персональних даних у цій базі даних, встановлює склад цих даних та процедури їх обробки, якщо інше не визначено законом;

– розпорядник персональних даних – фізична чи юридична особа, який є власником персональних даних або законом надано право обробляти ці дані;

– необхідність реєстрації персональних даних в Державному реєстрі баз персональних даних;

– вимоги до обробки персональних даних власника та розпорядника баз персональних даних як загальні вимоги до організаційних та технічних заходів захисту персональних даних під час їх обробки у базі персональних даних (згода суб'єкта персональних даних, порядок використання і поширення персональних даних та порядок доступу до персональних даних третіх осіб та ін.);

– необхідність контролю за дотриманням законодавства про захист персональних даних,

– відповідальність за порушення законодавства про захист персональних даних.

З метою забезпечення виконання громадянами, органами державної влади та місцевого самоврядування, підприємствами, установами, організаціями, незалежно від форм їх власності, вимог Закону України «Про захист персональних даних» Верховною Радою України:

– прийнято Закон України «Про внесення змін до деяких законодавчих актів в Україні щодо посилення відповідальності за порушення законодавства про захист персональних даних» № 3454-VI від 2 червня 2011 р.;

– внесено зміни до Кодексу України про адміністративні правопорушення.

2. Реєстрація баз персональних даних.

2.1. База персональних даних підлягає державній реєстрації шляхом внесення відповідного запису уповноваженим державним органом з питань захисту персональних даних до Державного реєстру баз персональних даних.

2.2. Реєстрація баз персональних даних здійснюється за заявочним принципом шляхом повідомлення.

2.3. Заява про реєстрацію бази персональних даних подається власником бази персональних даних до уповноваженого державного органу з питань захисту персональних даних.

Заява повинна містити:

– звернення про внесення бази персональних даних до Державного реєстру баз персональних даних;

– інформацію про власника персональних даних;

– інформацію про найменування і місцезнаходження бази персональних даних;

– інформацію про мету обробки персональних даних у базі персональних даних;

– інформацію про склад персональних даних, які обробляються;

– інформацію про третіх осіб, яким передаються персональні дані;

– інформацію про транскордонну передачу персональних даних;

– інформацію про інших розпорядників персональних даних;

– підтвердження зобов'язання щодо виконання вимог захисту персональних даних, встановлених законодавством про захист персональних даних.

2.4. Уповноважений державний орган з питань захисту персональних даних у порядку, затвердженому Кабінетом Міністрів України:

– повідомляє заявника не пізніше наступного робочого дня з дня надходження заяви про її отримання;

– приймає рішення про реєстрацію бази персональних даних протягом десяти робочих днів з дня надходження заяви.

Власнику бази персональних даних видається документ встановленого зразка про реєстрацію бази персональних даних у Державному реєстрі баз персональних даних.

2.5. Уповноважений Державний орган з питань захисту персональних даних відмовляє в реєстрації бази персональних даних, якщо заява про реєстрацію не відповідає встановленим вимогам.

2.6. Власник бази персональних даних зобов'язаний повідомляти уповноважений державний орган з питань захисту персональних даних про кожну зміну відомостей, необхідних для реєстрації відповідної бази, не пізніш як протягом десяти робочих днів з дня настання такої зміни.

2.7. Уповноважений державний орган з питань захисту персональних даних протягом десяти робочих днів з дня надходження повідомлення про зміну відомостей, необхідних для реєстрації відповідної бази, повинен прийняти рішення щодо зазначеної зміни та повідомити про це власника персональних даних.

3. Порядок обробки персональних даних у базах персональних даних.

3.1. Порядок обробки персональних даних встановлює загальні вимоги до організаційних та технічних заходів захисту персональних даних під час їх

обробки у базах персональних даних власниками та розпорядниками баз персональних даних. Обробка персональних даних може здійснюватися повністю або частково в інформаційній (автоматизованій) системі та/або у формі картотеки персональних даних.

3.2. Захист персональних даних покладається на власника персональної інформації. Розпорядник бази персональних даних здійснює обробку персональних даних відповідно до закону або на підставі укладеного з власником бази персональних даних договору в письмовій формі з метою і в обсязі, визначеному договором. На дії власника та/або розпорядника персональних даних поширюються усі вимоги щодо захисту персональних даних від незаконної обробки, а також від незаконного доступу до них.

3.3. Власник або розпорядник персональних даних дає суб'єкту персональних даних інформацію про мету обробки персональних даних до моменту отримання згоди від суб'єкта персональних даних.

3.4. Власник бази персональних даних зберігає персональні дані у строк не більше, ніж це необхідно відповідно до мети їх обробки, якщо інше не передбачено законодавством.

3.5. Власник бази персональних даних визначає:

– мету обробки, склад персональних даних у базі персональних даних та її місцезнаходження;

– порядок внесення, змін, оновлення, використання, поширення, знеособлення, знищення персональних даних у базі персональних даних;

– відповідальну особу або структурний підрозділ;

– порядок захисту персональних даних, в тому числі від незаконної обробки та незаконного доступу до них.

3.6. Відповідальна особа або структурний підрозділ відповідно до покладених завдань:

– забезпечує ознайомлення працівників власника і розпорядника бази персональних даних з вимогами законодавства про захист персональних даних, зокрема щодо їхнього обов'язку не допускати розголошення у будь-який спосіб персональних даних, які їм було довірено або які стали їм відомі у зв'язку з виконанням професійних, службових чи трудових обов'язків;

– забезпечує організацію обробки персональних даних працівниками власника та розпорядника бази персональних даних відповідно до їх професійних, службових або трудових обов'язків в обсязі, необхідному для виконання таких обов'язків;

– організовує роботу з обробки запитів щодо доступу до персональних даних суб'єктів відносин, пов'язаних з обробкою персональних даних;

– забезпечує доступ суб'єктів персональних даних до власних персональних даних;

– інформує керівника власника та розпорядника бази персональних даних про заходи, яких необхідно вжити для приведення складу персональних даних та процедур їх обробки у відповідність до Закону;

– інформує керівника власника та розпорядника бази персональних даних про порушення встановлених процедур з обробки персональних даних.

3.7. Власник бази персональних даних веде облік: фактів надання та позбавлення працівників права доступу до персональних даних та їх обробки; спроб та фактів несанкціонованих та/або незаконних дій з обробки персональних даних.

3.8. Власник бази персональних даних може розмежувати режими доступу працівників до обробки персональних даних в базі персональних даних відповідно до їх професійних, трудових чи службових обов'язків.

3.9. Знищення персональних даних здійснюється у спосіб, що виключає подальшу можливість поновлення цих персональних даних.

3.10. Власник бази персональних даних обробляє персональні дані в складі інформаційної (автоматизованої) системи, у якій забезпечується захист персональних даних від незаконної обробки, а також від незаконного доступу до них відповідно до вимог закону України «Про захист персональних даних» та відповідно до вимог нормативно-законодавчих актів з питань технічного захисту інформації.

4. Забезпечення захисту персональних даних в інформаційній (автоматизованій) системі.

4.1. Власник бази персональних даних повинен створити умови для захисту в інформаційній (автоматизованій) системі персональних даних і забезпечити захист цих персональних даних від незаконної обробки, а також від незаконного доступу до них.

4.2. Умови для захисту персональних даних залежать від конкретних реальних загроз, природи персональних даних, які обробляються, технології обробки інформації і типу інформаційної системи, в рамках якої обробляються персональні дані.

4.3. Забезпечення умов для захисту в інформаційній (автоматизованій) системі персональних даних не вирішується реалізацією визначеної сукупності заходів, а є постійним процесом, який включає:

– розробку політики захисту персональних даних від незаконної обробки, а також від незаконного доступу до них, виходячи з характеристик діяльності організації, цілей, процесів і процедур, суттєвих для управління ризиком небажаних подій щодо обробки персональних даних з урахуванням серйозності наслідків таких небажаних подій. Політика захисту персональних даних від

незаконної обробки, а також від незаконного доступу до них повинна бути узгоджена з загальною політикою інформаційної безпеки організації і з контекстом стратегічного управління ризиками організації;

– впровадження політики захисту персональних даних від незаконної обробки, а також від незаконного доступу до них і забезпечення функціонування заходів, процесів та процедур захисту персональних даних;

– оцінювання і, за можливості, вимірювання продуктивності процесів захисту персональних даних згідно з прийнятою політикою, цілями і практичним досвідом, підготовка пропозицій щодо коригувальних заходів;

– вживання коригувальних та запобіжних дій щодо захисту персональних даних на підставі результатів внутрішніх перевірок, періодичний перегляд політики захисту персональних даних, постійне удосконалення заходів;

4.4. У разі, коли обробка персональних даних здійснюється в інформаційній (автоматизованій) системі, то створюється комплексна система захисту інформації відповідно до Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджених Постановою Кабінету Міністрів України від 29 березня 2006 р. № 373.

4.5. Комплексна система захисту інформації забезпечує захист персональних даних від незаконної обробки, а також від незаконного доступу до них відповідно до плану захисту інформації в системі, який містить:

– завдання захисту персональної інформації, класифікацію персональної інформації, опис особливостей технології обробки інформації;

– модель загроз для персональних даних у системі;

– вимоги щодо захисту персональних даних та правила доступу до них;

– перелік документів, згідно з якими здійснюється захист інформації в інформаційній системі.

4.6. Для захисту персональних даних важливо, щоб організаційні заходи і використовувані засоби захисту, що визначають рівень захисту, відповідали реальним конкретним загрозам, даним, які обробляються, та процесам обробки даних, які виконуються. Повинні братися до уваги ймовірні ризики небажаних подій та серйозність наслідків таких небажаних подій. Чим вищі ризики, тим суворіші заходи захисту повинні бути реалізовані.

4.7. Якщо обробка персональних даних здійснюється в інформаційній (автоматизованій) системі, у якій створюється комплексна система захисту інформації, оцінка ризиків небажаних подій для персональних даних, що обробляються в автоматизованій системі, є складовою частиною оцінки ризиків відповідно до рекомендацій згідно з нормативним документом НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп’ютерних системах від

несанкціонованого доступу». Затверджено наказом ДСТСЗІ СБ України від 28.04.1999 № 22.

4.8. До основних факторів, які впливають на рівень необхідного захисту, належать:

– увага, що приділяється суспільством до оброблюваних даних;

– рівень поінформованості персоналу власника та/або розпорядника бази персональних даних щодо інформаційної безпеки, захисту персональних даних, авторських прав тощо;

– тип інформаційно-телекомунікаційної системи, в рамках якої обробляються персональні дані.

5. Обробка персональних даних.

5.1. Власник бази персональних даних здійснює обробку персональних даних у картотеках у порядку, описаному в розділі 4, з урахуванням таких вимог:

– документи, що містять персональні дані, формуються у справи залежно від мети обробки персональних даних;

– справи з документами, що містять персональні дані, повинні мати внутрішні описи документів із зазначенням мети обробки і категорії персональних даних;

– картотеки зберігаються в приміщеннях (шафах, сейфах), захищених від несанкціонованого доступу.

5.2. Двері у приміщеннях (шафах, сейфах) повинні бути обладнані замком або контролем доступу.

6. Відповідальність за порушення законодавства про захист персональних даних.

6.1. З метою забезпечення виконання громадянами, органами державної влади та місцевого самоврядування, підприємствами, установами, організаціями незалежно від форм власності вимог Закону України «Про захист персональних даних», Верховною Радою України прийнято Закон України «Про внесення змін до деяких законодавчих актів України щодо посилення відповідальності за порушення законодавства про захист персональних даних» № 3454-VI від 2 червня 2011 р., яким внесено зміни до Кодексу України про адміністративні порушення.

6.2. З 1 липня 2012 р. за порушення у сфері захисту персональних даних на громадян, посадових осіб, громадян-суб'єктів підприємницької діяльності покладається адміністративна відповідальність.

6.3. До адміністративної відповідальність громадяни, посадові особи, громадяни-суб'єктів підприємницької діяльності притягуються за такі види діянь:

– неповідомлення або несвоєчасне повідомлення суб'єкта персональних даних про його права у зв'язку із включенням його персональних даних до бази

персональних даних, мету збору цих даних та осіб, яким ці дані передаються, тягне за собою накладення штрафу відповідно до чинного законодавства;

– неповідомлення або несвоєчасне повідомлення спеціально уповноваженого центрального органу виконавчої влади з питань захисту персональних даних про зміну відомостей, що подаються для державної реєстрації бази персональних даних, тягне за собою накладення штрафу відповідно до чинного законодавства;

– ухилення від державної реєстрації бази персональних даних тягне за собою накладення штрафу відповідно до чинного законодавства;

– недотримання встановленого законодавством про захист персональних даних порядку захисту персональних даних у базі персональних даних, що призвело до незаконного доступу до них, тягне за собою накладення штрафу відповідно до чинного законодавства;

6.4. Незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконна зміна такої інформації, караються відповідно до чинного законодавства:

– штрафами;
– виправними роботами;
– арештом або обмеженням волі.

Ті самі дії, вчинені повторно, або якщо вони завдали істотної шкоди правам, свободам та інтересам особи, – караються (згідно чинного законодавства):

– штрафами;
– виправними роботами;
– арештом або обмеженням волі.

7. Створення умов для обробки персональних даних на підприємстві.

7.1. З моменту прийняття Закону України «Про внесення змін до деяких законодавчих актів України посилення відповідальності за порушення законодавства про захист персональних даних» № 3454-VI від 2 червня 2011 р. норми Закону України «Про захист персональних даних» перестають бути суто декларативними, а перетворюються в дієвий правовий інструмент у руках держави, оскільки порушення законодавства у сфері захисту персональних даних тягне за собою адміністративну або кримінальну відповідальність.

7.2. На виконання вимог Закону України «Про захист персональних даних» та з метою недопущення правопорушень у сфері захисту персональних даних на підприємстві необхідно створити систему управління персональними даними, що поєднує організаційні та технічні заходи щодо створення умов роботи з персональними даними.

7.3. На етапі створення системи управління персональними даними на підприємстві необхідно здійснити такі організаційні заходи:

– визначити мету обробки та склад персональних даних у базі персональних даних підприємства. Зазвичай на підприємстві може бути три бази персональних даних – база працівників, база контрагентів (клієнтів), база засновників;

– розробити і затвердити Порядок обробки персональних даних у базах персональних даних підприємства;

– призначити окремого виконавця або структурний підрозділ, відповідальний за відомості, що містять персональні дані, які забезпечать створення і функціонування на підприємстві комплексної системи захисту інформації в інформаційній (автоматизованій) системі від незаконної обробки та незаконного доступу, а також контроль за виконанням вимог законодавства щодо захисту персональних даних;

– провести реєстрацію баз персональних даних, що функціонують на підприємстві, в Державному реєстрі баз персональних даних;

– забезпечити оформлення письмової згоди суб'єктів персональних даних на обробку їх персональних даних у базах персональних даних підприємства, якщо створені умови щодо захисту інформації;

– забезпечити оформлення письмової згоди працівників підприємства не допускати розголошення персональних даних, які їм довірено або які стали їм відомі у зв'язку з виконанням професійних та трудових відносин;

– створити комплексну систему захисту інформації, що забезпечує захист персональних даних в інформаційній (автоматизованій) системі;

– розробити і затвердити необхідні положення, інструкції та інші розпорядчі документи, відповідно до яких буде забезпечуватися захист персональних даних у базах персональних даних підприємства.

7.4. Створення комплексної система захисту інформації, що забезпечить захист персональних даних в інформаційній (автоматизованій) системі від незаконної обробки, а також від незаконного доступу до них, здійснюється відповідно до Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджених Постановою Кабінету Міністрів України від 29 березня 2006 р. № 373 та іншими нормативно-законодавчими документами в галузі технічного захисту інформації.

2.4. Європейська система захисту персональних даних

Проблема захисту персональних даних стає все більш актуальною не лише в Україні, а й в усьому світі. Зі стрімким розвитком сучасних інформаційних технологій ідентифікація фізичної особи є необхідною для надання багатьох послуг: надання кредитів, виплата допомоги, оплата комунальних послуг, робота з банківськими установами, оплата товару через інтернет тощо. Оскільки більшість подібних послуг надається через мережу та видалений доступ і без

особистої присутності, можна впевнено сказати, що вимоги до захисту персональних даних мають бути більш жорсткими.

Розглядаючи поняття персональних даних, необхідно сказати, що це інформація, яка може ідентифікувати особу. Такими даними є: прізвище, ім'я, по батькові; дата, рік, місяць, місце народження; адреса реєстрації або прописки; номер паспорта і картки соціального страхування; відомості про соціальний та сімейний стан; власність на майно, освіта, професія, доходи.

Останнім часом з'явилося багато інших персональних даних: номери кредитних і дебетових банківських карт, PIN-коди, логіни та паролі від різних сервісів (наприклад, особистої пошти), дані GPS-приймача зі смартфону, що дають змогу відстежити переміщення користувача, та інше.

Новини про крадіжку даних були поширені в другій половині XX ст. в США. Найчастіше такі випадки стосувалися використання медичних та інших даних для отримання рецептурних препаратів шляхом обману. У Європі крадіжки персональних даних найчастіше використовувалися для надсилання фіктивних рахунків і отримання державних дотацій чи допомоги.

Для боротьби з шахрайством у багатьох країнах на законодавчому рівні розроблялися нові вимоги безпеки до компаній, що працюють із персональними даними. Цей процес має постійний характер, оскільки інформаційні технології розвиваються, і разом з ними з'являються нові вимоги до забезпечення безпеки інформації. З іншого боку, такий розвиток штовхає злочинців на винахід нових методів розкрадання даних.

Оскільки Україна підтримує курс європейського розвитку, розглянемо розвиток системи захисту персональної інформації в ЄС. Європейське законодавство вже більше двох десятиліть удосконалює систему захисту персональних даних. У 1995 р. на території Європи введена директива, що зобов'язує країни, які входять до складу ЄС, забезпечити захист персональних даних громадян. Кожна європейська країна ухвалила свої закони про захист персональних даних, що найчастіше не збігалися із законами інших країн ЄС. Багато міжнародних компаній, що передають дані через кордон, стали зазнавати труднощів, пов'язаних із дотриманням законів різних країн. Саме тому у 2012 р. було вирішено створити загальний регламент із захисту персональних даних на території ЄС (General Data Protection Regulation – GDPR), що прийшов на зміну чинної директиви [3].

Після кількох років переговорів регламент було затверджено 25 травня 2016 р. У травні 2018 р. набуло чинності нове положення про захист даних. Серед нововведень – заборона на збір персональних даних компаніями і державою без дозволу з боку фізичної особи. Винятки допускаються тільки якщо в країні існують законодавчі акти, що зобов'язують до передачі інформації.

Протягом двох років, до 25 травня 2018 р., усі компанії, що зберігають, передають і обробляють особисті дані європейців, зобов'язані були забезпечити безпеку таких даних відповідно до положень GPDR. Варто зазначити, що це також стосується компаній, що перебувають за межами країн ЄС, що працюють із персональними даними громадян європейських країн (наприклад, України).

Крім європейської системи захисту персональних даних, кожна країна пройшла свій шлях створення системи захисту персональних даних. Наприклад, у Німеччині перший закон у сфері захисту персональних даних був прийнятий ще в 1970 р. А через сім років з'явився перший федеральний закон, що захищає персональні дані громадян Німеччини. Його переглянули в 1990 р., адаптувавши під нові реалії. Головною метою закону став захист недоторканності приватного життя під час використання персональних даних.

Прикладом може бути і Франція. У процесі створення системи французьке суспільство пройшло через спробу тотального контролю за громадянами, але зуміло зберегти демократичні принципи. У 1978 р. уряд прийняв Закон «Про обробку даних, файли та свободи» у якому, крім визначення основних понять, встановлено покарання за порушення. Правопорушники штрафуються, а також можуть отримати тюремний строк до 5 років. Франція строго стежить за захистом прав і свобод своїх громадян. Будь-які порушення в області персональних даних висвітлюються в пресі. Франція – чудовий приклад країни з розвинутою системою захисту персональної інформації, що базується на якісному законодавстві і активно бореться з порушеннями, накладаючи великі штрафи.

В Англії профільний закон був прийнятий у 1984 р. У ньому, крім основних положень, вказувалися вимоги до структур, що збирають і обробляють персональну інформацію. Кожен із таких користувачів зобов'язаний повідомити про інформацію, яку він збирає, і з якою метою. Для цього уряд створив спеціальний «Реєстр захисту даних». Невиконання цієї вимоги карається законом. Особливо жорстко у Великобританії карають за втрату або виток персональних даних.

Ще одним прикладом може бути Польща. Закон про захист персональних даних, що адаптує польське законодавство регламенту щодо захисту персональних даних усіх осіб у межах ЄС та Європейської економічної зони (RODO), набув чинності 25 травня 2018 р. Серед нововведень Закону про захист даних – заборона на збір персональних даних компаніями і державою без дозволу з боку фізичної особи. Винятки допускаються лише в тому випадку, якщо в країні існують законодавчі положення, що зобов'язують до передачі інформації. Польща є однією з перших країн у Європейському союзі, яка змогла повністю адаптувати національну правову систему до положень про захист персональних

даних. Наприклад, кожен громадянин має можливість отримати детальну інформацію про цілі обробки своїх даних фінансовими установами та спосіб їх використання, а також право на отримання пояснення, на якій підставі банк вирішив відмовити у видачі кредиту. Організовано також якісний захист персональних даних у секторі освіти, медичній галузі, на всіх робочих місцях у державних та інших установах.

Також важливим для держав Європейського союзу є те, що підтверджувати дозвіл на обробку персональних даних можна не з 13 років, а лише з 16 років. На компанії з європейськими представництвами накладається низка обмежень. Їм не можна виконувати обмін даними з іншими підрозділами, якщо не виконуються правила із захисту даних. Також не можна передавати інформацію владі США та іншим країнам. Прикладом для України також є Литва, Латвія, Естонія.

Варто зазначити, що в ЄС новий GPDR-регламент сприяв масовому переходу інформаційних структур європейських підприємств у хмарні сховища. Щоб краще зрозуміти причини такої масової міграції, необхідно знати, що в GPDR усі підприємства поділяються на дві основні категорії:

– контролери даних – це підприємства, діяльність яких містить у собі збір персональних даних, їх передачу, а також роботу з ними. Основні вимоги до таких компаній полягають у дотриманні правил, що стосуються згоди громадян на зберігання, обробку і передачу їх персональних даних;

– обробники даних – це підприємства, що зберігають персональні дані безпосередньо на своїх серверах. Такі компанії зобов'язані забезпечити високий рівень інформаційної безпеки даних – від обмеження фізичного доступу до обладнання, де зберігається інформація, до жорстких вимог їх резервного копіювання та налагодження брандмауерів. Забезпечення цих стандартів – складний і вартісний процес.

Для багатьох компаній витрати на відповідність вимогам GDPR у якості обробника даних є дуже великими, тому більшість європейських підприємств переводять свої інформаційні системи в хмарні сховища.

Захист персональних даних українців знаходиться на критично низькому рівні. Лише у 2011 р. в Україні набув чинності Закон України «Про захист персональних даних» [3], згідно з нормами якого фізичні і юридичні особи (підприємства, установи і організації всіх форм власності), органи державної влади або органи місцевого самоврядування, фізичні особи-підприємці, що обробляють персональні дані, тобто відомості або сукупність відомостей про фізичну особу, яка ідентифікована або може бути ідентифікованою (ст. 2 Закону), повинні зареєструвати бази персональних даних у спеціальному реєстрі баз даних, роботу якого контролює Державна служба з питань захисту персональних даних.

Якщо на підприємствах створюються відомості про працівників, клієнтів та осіб, із якими компанія співпрацює або продає авіаквитки, туристичні послуги, проводить опитування, то таке підприємство зобов'язане зареєструвати таку базу даних. У випадку ж невиконання або неналежного виконання фізичними і юридичними особами вимог Закону України «Про захист персональних даних» передбачено покарання і адміністративна відповідальність за порушення законодавства про захист персональних даних» [3]. Кримінальна відповідальність відповідно до цього закону передбачена у випадку незаконного збору, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконної зміни такої інформації.

Усі персональні дані українців, починаючи з номера мобільного телефону і закінчуючи адресою проживання, сьогодні не захищені. Наприклад, багато користувачів неодноразово одержували СМС від різних служб таксі, магазинів, у яких ніколи не бували – це означає, що ваші особисті дані було продано. Характерно те, що спеціальне законодавство, розроблене в Україні для збереження й захисту персональних даних, фактично діє тільки в тому випадку, коли витік інформації походить із якихось державних установ і підприємств. Відповідальність може настати, тільки якщо власник цих даних звернувся в правоохоронні органи. Дуже небезпечна ситуація зараз існує у використанні баз персональних даних системи Міністерства охорони здоров'я України, що легко викрасти, бо вони практично не захищені.

Проблема в Україні ще збільшується тим, що громадяни добровільно передають свої дані під час одержання різних дисконтних карт та в інших випадках, не замислюючись про можливі наслідки. Будь-який витік персональних даних приносить серйозні фінансові неприємності. Ви будете здивовані, якщо на ваше ім'я було оформлено кредит. Але відповідальність нести вам. Добре, якщо вдасться довести, що не ви брали кредит, але морально ви постраждаєте.

За даними компанії Searchinform, провідного виробника засобів від витоків даних у СНД, більше 32 % українських витоків інформації пов'язано з персональними даними. Проконтролювати в Україні, як саме зберігаються та обробляються персональні дані, складно і майже неможливо.

Отже, система захисту персональних даних в Україні потребує державного моніторингу та реформування на законодавчому рівні. В умовах щораз вищого рівня кіберзлочинності у світі та низького рівня інформаційної культури громадян, а також відсутності розуміння ними всіх можливих кіберзагроз, необхідно на державному рівні забезпечити захист громадян від витоку персональних даних. Вести боротьбу з кіберзлочинністю з використанням персональних даних можна тільки на основі системного підходу на усіх рівнях.

Проблемою безпеки персональних даних повинно займатися не тільки відомство омбудсмена, але й структури, пов’язані з безпекою і правоохоронною діяльністю держави [3].

Питання для самоконтролю:

1. Види конфіденційної інформації.
2. Заходи формування режиму інформаційної безпеки.
3. Що не належить до основних аспектів інформаційної безпеки?
4. Що не належить до зовнішніх загроз інформаційної безпеки?
5. Що входить до комплексної системи захисту інформації?
6. Що таке інформаційна безпека?
7. Коли доцільно не робити жодних дій щодо виявлених ризиків?
8. Яка категорія є найбільш ризикованою з огляду на ймовірне шахрайство та порушення безпеки?
9. Що належить до персональних даних?
10. Система управління персональними даними.

ТЕМА 3
ЗАХИСТ ІНФОРМАЦІЇ В МОБІЛЬНИХ ПРИСТРОЯХ

У темі детально описані питання інформаційної безпеки мобільних і дистанційних телекомунікацій та загрози втрати конфіденційної інформації з мобільних пристроїв.

Ключові слова: *«троянські» програми, шпигунські програми, історія розвитку мобільних вірусів.*

План

3.1. Інформаційна безпека мобільних та дистанційних телекомунікацій.

3.2. Загрози втрати конфіденційної інформації з мобільних пристроїв.

3.1. Інформаційна безпека мобільних та дистанційних телекомунікацій

Широке застосування мобільних пристроїв і технології хмарних сховищ висуває підвищені вимоги до безпеки мобільних і дистанційних телекомунікацій, збереження і захисту корпоративних даних, зокрема від несанкціонованого поширення цієї інформації. У разі використання технології хмарних сховищ за моделлю на віддалених серверах і центрах опрацювання даних провайдера зберігається критично важлива для підприємства інформація, наприклад, фінансовий звіт. Багато керівників дублюють її на своїх персональних мобільних пристроях, що знижує рівень інформаційної безпеки підприємства. В цьому випадку потрібно передбачити заходи щодо захисту або знищення цих даних у разі втрати або крадіжки мобільного пристрою. Передача інформації по незахищених каналах зв'язку також може призвести до катастрофічних наслідків.

За статистикою 2019 р. спостерігалося подальше посилення загроз інформаційній безпеці для власників як особистих, так і корпоративних мобільних пристроїв. Аналітики цієї компанії зазначають низький рівень інформаційної безпеки корпоративних користувачів навіть у випадках не найскладніших атак. Кількість небезпечних програм за 2019 р. у 4 рази перевищила їх кількість за попередні п'ять років, а самі програми стали витонченішими і складнішими. Особливу небезпеку становлять шкідливі програми для пристроїв на основі операційної системи Android.

За відкритими даними, лише за перші три квартали 2019 р. кількість шкідливих програм для мобільних пристроїв на основі ОС Android наблизилося до 750. Разом з SMS-троянськими програмами особливу небезпеку для корпоративних користувачів становлять DDoS-атаки. Зросли і їх кількість, і їх потужність. На думку фахівців, основну групу ризику в нашій країні становитимуть компанії нафтогазової галузі, енергетики, а також сектори важкого машинобудування, інжинірингу та добувної промисловості.

Мобільні засоби часто використовуються поза контрольованою зоною корпоративного зв'язку. Вони є об'єктами крадіжки і зараження шкідливими програмами з метою викрадення грошових коштів або цінної інформації, здійснення хакерських атак, спрямованих на нанесення економічної або моральної шкоди компанії. Щоб захиститися від таких загроз, недостатньо антивірусних програм, що встановлюються на мобільні пристрої. Убезпечити може тільки комплексна система забезпечення інформаційної безпеки корпоративного класу.

Одним із рішень захисту трафіку мобільних пристроїв є послуга оператора зв'язку «Мобільний VPN». У цьому випадку весь трафік мобільних пристроїв передається закритими каналами оператора зв'язку і не потрапляє в інтернет, що виключає ризик перехоплення її зловмисниками.

Для мобільних користувачів інформаційна безпека забезпечується:

– готовими рішеннями, які встановлюються на мобільний апарат, щоб обмежити можливість витоку інформації;

– засобами, що надають захищену взаємодію співробітників з офісом компанії;

– засобами, що дають змогу реалізувати віртуальне робоче місце на мобільному терміналі з можливістю централізованого управління його безпекою;

– ефективним застосуванням уже наявних сертифікованих засобів захисту.

Як відповідь на серйозну і обґрунтовану стурбованість щодо безпеки мобільних пристроїв з'явилися нові комплексні захисти всього периметра інформаційної інфраструктури з урахуванням мобільності.

3.2. Загрози втрати конфіденційної інформації з мобільних пристроїв

Насамперед усім користувачам, які користуються мобільними телефонами, а особливо смартфонами, дуже важливо розуміти, що той пристрій, який вони носять у себе в кишені, – це повноцінний комп'ютер із функцією постійного доступу до мережі Інтернет, мікрофоном, камерою, GPS-навігатором і приєднаним до нього одним або декількома різними гаманцями. Тобто є власний мобільний рахунок у оператора і додатково прив'язана банківська карта. Всі ці рахунки можуть бути використані зловмисниками.

Для смартфонів характерні ті ж самі загрози, що і для персональних комп'ютерів, оскільки телефон, по суті, і є комп'ютером. Це обумовлює і можливість запуску «троянських» програм, і шпигунство, і крадіжку конфіденційної інформації, крадіжку грошей із мобільних рахунків.

«Троянські» програми. Розглянемо проблему дещо ширше. Які можливості мають троянські програми для мобільних пристроїв? На жаль, ми не думаємо про безпеку мобільних пристроїв. І якщо на комп'ютері використання антивірусу є вже нормою, то на мобільних пристроях це все ще щось екзотичне.

Сьогодні існує величезна кількість загроз: віруси, троянські програми, мережеві хробаки, рекламні модулі орієнтовані на абсолютно різні платформи для мобільних пристроїв.

Шпигунські програми. Ці програми належать до класу легальних шпигунських програм. Зверніть увагу – «легальних» шпигунських програм. Що мається на увазі? Це програми, які можна вільно придбати. У програм є технічна підтримка, власний сайт, офіційний власник, програму можна доволі просто видалили з приладу. Подібну програму можна вільно придбати, встановити на пристрій користувача і спокійно за ним стежити, тобто перехоплювати інформацію про всі здійснені дзвінки, показувати вміст sms-листування, показувати інформацію про відвідувані сайти, знімати за допомогою камери телефона навколишню обстановку, визначати місцерозташування, сканувати Bluetooth- чи Wi-Fi-оточення, включати мікрофон і записувати інформацію про все навколо. Встановлення подібного додатка на телефон користувача, по суті, дає змогу шпигувати за ним всюди, адже телефон практично завжди з нами. Слідкувати можна не лише в плані дій у телефоні, але і за безпосереднім оточенням користувача – реальним життям, де він перебуває, що бачить, що говорить.

Історія розвитку мобільних вірусів

Перші мобільні віруси не можна було навіть назвати повністю вірусами. Це були більше шкідливі sms-повідомлення, тобто на телефон користувача приходило певне sms-повідомлення, і якщо його відкрити – це призводило до збою роботи телефона: зависання, «обнулення» телефонної книги, здійснення певного дзвінка, тобто телефон виконував певну не потрібну користувачу функцію. Далі з’явились реальні віруси і хробаки. Перші віруси з’явились ще для комунікаторів на операційних системах Palm OS, Windows CE, Windows Mobile. Далі їм на заміну прийшов Symbian, для якого також було створено багато шкідливих програм, повноцінних хробаків, що мали можливість розповсюджуватись від одного пристрою до іншого за допомогою bluetooth-з’єднання і виконувати шкідливі дії.

Цікаво, що тоді розповсюдження хробаків було в основному побудовано на методах соціальної інженерії. Наприклад, смартфон на базі Symbian, заражений хробаком, що розповсюджується через Bluetooth. Радіус дії Bluetooth-передачі – 10–15 метрів, автоматичної передачі не відбувається. Тобто заражений смартфон сканував оточення, знаходив інші телефони із увімкненим Bluetooth і намагався їм розіслати копії себе. Що ж відбувалось зі сторони, яка приймала? Звичайний користувач перебував у метро чи кафе і бачив на телефоні пропозицію прийняти певний файл. Ця ситуація була не висвітлена у ЗМІ, і звичайної цікавості вистачало, щоб прийняти файл, тим паче, що він міг цікаво називатись. Людина приймала файл, відкривала його з цікавості, і якщо

приймаючий прилад був на базі Symbian, хробак активізувався, заражав пристрій, а потім заражав інших, виконуючи нову розсилку.

Перші модифікації вірусу просто розмножувались і наносили певну шкоду, блокуючи деякі додатки у смартфоні. Пізніші модифікації хробака вже намагались заробляти кошти зловмисникам, тобто вірус розповсюджувався так само через Bluetooth, але вже мав нову функцію – відправка sms на платні номери. Для цього зловмисники реєстрували короткі платні номери під час відправки sms-повідомлень, за відправлення яких із користувача знімаються певні кошти. І троянська програма із зараженого пристрою відправляла sms-повідомлення, а зловмисники в такий спосіб отримували зиск.

Далі мобільні пристрої почали володіти все більшою можливістю з'єднання з інтернетом. Спочатку це були WAP- та GPRS-з'єднання, потім з'явились 3G-мережі, далі повноцінні Wi-Fi-точки. Зараз є дуже багато місць, де не підключаючись через свого GSM-оператора, можна отримати доступ до глобальної мережі через Wi-Fi, що наявний практично всюди: в офісах, метро, кафе, вдома тощо.

Маючи доступ до інтернету, хробаки отримали можливість насамперед швидко розповсюджуватись через електронну пошту, вебсайти і наносити суттєву шкоду, адже вони вже могли не тільки відправляти платні sms-повідомлення, але й красти дані кредитних карток про акаунти в соціальних мережах, електронній пошті і т. ін. Віруси для мобільних пристроїв отримали всі ті властивості, що притаманні класичним шкідливим програмам для персональних комп'ютерів.

Для того, щоб провести аналогію, можна зазначити, що існує багато «троянських» програм, що, заражаючи телефон, перетворюють його на бота і формують цілу бот-мережу. Існують бот-нети на основі мобільних пристроїв. Так, у 2012 р. у Китаї був виявлений бот-нет, що складався із 1,5 мільйона заражених пристроїв. Кожен із цих пристроїв міг або відправити sms-повідомлення на певний номер або провести DDoS-атаку, СПАМ-розсилку. У такий спосіб DDoS-атаки на сайти можуть проводитись не тільки з заражених комп'ютерів, але й із заражених смартфонів, які, по суті, і є тими самими комп'ютерами, які ми постійно носимо з собою.

Класичні віруси для мобільних пристроїв в основному не розробляються. Переважно для мобільних пристроїв розробляють троянські програми, рекламні модулі, бекдор-програми (які дають змогу обійти автентифікацію).

Варто розуміти, що шкідливі програми створюються для всіх операційних систем, на які можна встановити додаткове програмне забезпечення. Тобто якщо у телефон можна встановити додаткові програми, значить, туди може потрапити шкідлива програма. Якщо вона не потрапить туди самостійно, автоматично, то програма може зробити це з вашою допомогою через методи соціальної

інженерії. Наприклад, вам запропонують встановити цікаву гру, а це виявиться і гра, і шкідлива програма. Або взагалі вона не буде маскуватись під гру, а просто почне надсилати sms-повідомлення на короткі номери. Тільки пристрої з повною забороною на встановлення додаткового ПЗ є захищеними. Віруси, у широкому сенсі, для операційної системи iOS (мобільна операційна система від Apple), на жаль, існують, і у доволі великій кількості.

Тут, імовірніше, виникає питання, в який спосіб ці шкідливі програми можуть проникнути на ваш мобільний пристрій. І в цьому плані служба App Store дійсно більш захищена, ніж служба Google Play Market. Але тут є і зворотна сторона. Зазвичай користувачі мобільних пристроїв iPhone не готові до того, що їх прилади можуть заражатись вірусами. Якщо для Android-пристроїв хоча б частина юзерів користуються антивірусами, то у разі виникнення епідемії вони можуть бути захищені набагато швидше. Користувачі ж операційної системи iOS-пристроїв змушені чекати, поки служба Apple випустить оновлення операційної системи, що усуне вразливість.

Ще один аспект загроз для користувачів мобільних телефонів полягає у моделі роботи з платними послугами, що можуть бути не зовсім зрозумілі користувачу. Тобто вас можуть ввести в оману, попросивши набрати певний номер, надіслати sms-повідомлення. У всіх цих випадках з мобільного рахунку знімаються певні кошти. Також дуже популярною є послуга sms-підписок, коли користувачу пропонують підписатись на певний сервіс за допомогою sms-повідомлень. Це може бути все, що завгодно: підписка на онлайн-гру, певний сайт, будь-який сервіс, який вимагає регулярної оплати. Далі користувач може забути про це, оскільки він лише один раз погоджується, а потім ініціювання зняття коштів буде відбуватись уже оператором. З вашого рахунку періодично буде зніматись певна сума коштів, і ви цього можете навіть не помічати. Інколи ми просто не пам’ятаємо, на що підписалися, а можливо, і взагалі цього не робили, бо це зробила «троянська програма». Тому треба бути дуже обережним під час використання коротких sms-повідомлень під час замовлення послуг через них. Не варто дзвонити на незнайомі номери, важливо контролювати послуги, на які ви підписуєтесь. Інколи підписка на послугу може коштувати 5 гривень, а вже за те, щоб відписатись, потрібно заплатити 25 грн. Тому варто бути якомога більш уважними і не користуватись підозрілими сервісами.

Питання для самоконтролю:

1. Головна характеристика троянської програми.
2. Що таке шпигунські програми?
3. Які є загрози через використання мобільних пристроїв?
4. Як проникають на мобільний телефон вірусні програми?
5. Яка шкода є від вірусів?

ТЕМА 4
УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

У матеріалах теми подані фундаментальні принципи управління, методи захисту інформації, організаційні засоби захисту інформації, технічні системи захисту даних, механізми інформаційної безпеки та методи визначення рівня інформаційного ризику, а також управління ризиками інформаційної безпеки.

Ключові слова: *регламент щодо забезпечення інформаційної безпеки, технічні заходи, опис бізнес-процесів, збір ризиків, оцінка ризиків, планування заходів, реалізація заходів, оцінка ефективності, ідентифікатор, ідентифікація, пароль, аутентифікація, профіль, авторизація.*

План

4.1. Методи захисту інформації.

4.2. Організаційні засоби захисту інформації.

4.3. Технічні системи захисту даних.

4.4. Механізми інформаційної безпеки.

4.5. Методи визначення рівня інформаційного ризику.

4.6. Управління ризиками інформаційної безпеки (сімейство стандартів ISO/IEC 27000).

4.1. Методи захисту інформації

Система управління інформаційною безпекою ґрунтується на трьох фундаментальних принципах управління:

– принцип розімкнутого керування;

– принцип компенсації;

– принцип зворотного зв’язку.

За принципом розімкнутого управління створюються власні політики безпеки, виконання яких контролюється відповідальними особами. Зараз більшість компаній виділяє для особи, відповідальної за розробку і реалізацію політик ІБ, позицію CISO (Chief Information Security Officer) – керівника відділу IT-безпеки або директора з IT-безпеки. Зазвичай CISO очолює керуюча рада з питань інформаційної безпеки.

Принцип компенсації передбачає, що в разі виникнення будь-яких відхилень від розробленої політики безпеки або зовнішніх факторів (а це неминуче, оскільки компанії розвиваються, з’являються нові загрози, приходять і йдуть нові співробітники, з’являються нові програмні продукти) необхідно негайно вносити відповідні корективи в алгоритм управління, що компенсували б негативний результат зовнішніх впливів. Тому для компаній дуже важливо не

тільки розглядати інциденти, що вже відбулися, але і будувати систему проактивного захисту, здатну відбити атаки до того, як з'являться проблеми, і навіть до того, як стане відомо про потенційні проблеми та слабкі місця.

Дуже важливо дотримуватися принципу зворотного зв'язку, що дає змогу управляти ІБ по замкнутому колу. За цим принципом будуються багато систем ІБ. Наявність ланки зворотного зв'язку в системі управління інформаційною безпекою дає змогу не тільки виявити окрему загрозу, але і відреагувати на цілу низку подій, на перший погляд ніяк не пов'язаних між собою. У цьому можуть допомогти продукти, що забезпечують централізоване зіставлення даних журналів подій з мережевих пристроїв і систем безпеки в режимі реального часу, автоматично зіставляючи дані і виділяючи події та загрози безпеці, що вимагають прийняття рішучих заходів, як-от Check Point Eventia Analyzer.

Побудова систем ІБ з урахуванням перерахованих принципів дає змогу використовувати наявні методи оптимізації для покращення різних показників якості системи, як-от стійкість управління, швидкість реакції на наявні та невідомі загрози. Розробка комплексу організаційних засобів захисту інформації повинна входити в компетенцію служби безпеки.

Найчастіше фахівці з безпеки:

– розробляють внутрішню документацію, що встановлює правила роботи з комп'ютерною технікою та конфіденційною інформацією;

– проводять інструктаж і періодичні перевірки персоналу;

– ініціюють підписання додаткових угод до трудових договорів, де вказана відповідальність за розголошення або неправомірне використання відомостей, що стали відомі з роботи;

– розмежовують зони відповідальності, щоб виключити ситуації, коли масиви найбільш важливих даних знаходяться в розпорядженні одного зі співробітників;

– організовують роботу в загальних програмах документообігу і стежать, щоб критично важливі файли не зберігалися поза мережевих дисків;

– впроваджують програмні продукти, що захищають дані від копіювання або знищення будь-яким користувачем, зокрема топ-менеджментом організації;

– складають плани відновлення системи на випадок виходу з ладу з якихось причин.

Якщо в компанії немає виділеної ІБ-служби, виходом стане запрошення фахівця з безпеки на аутсорсинг. Віддалений співробітник зможе провести аудит ІТ-інфраструктури компанії і дати рекомендації з її захисту від зовнішніх і внутрішніх загроз. Також аутсорсинг в ІБ передбачає використання спеціальних програм для захисту корпоративної інформації.

На практиці використовують кілька груп методів захисту, зокрема:

– перешкода на шляху передбачуваного викрадача, що створюють фізичними і програмними засобами;

– управління, або надання впливу на елементи, що захищається системи;

– маскування, або перетворення даних, зазвичай криптографічними способами;

– регламентація, або розробка нормативно-правових актів і набору заходів, спрямованих на те, щоб спонукати користувачів, які взаємодіють із базами даних, до належної поведінки;

– примус, або створення таких умов, за яких користувач буде змушений дотримуватися правил поводження з даними;

– спонукання, або створення умов, що мотивують користувачів до належної поведінки.

Регламент щодо забезпечення інформаційної безпеки – внутрішній документ організації, що враховує особливості бізнес-процесів і інформаційної інфраструктури, а також архітектуру системи. Захистити інформацію від несанкціонованого доступу можна за допомогою апаратно-програмних, програмних, біометричних, технічних і адміністративних засобів.

Апаратно-програмні засоби. Кожен із методів захисту інформації реалізується за допомогою різних категорій засобів.

Основні засоби – організаційні та технічні:

– спеціальні криптографічні плати, що вбудовуються в комп'ютер, за допомогою яких інформацію можна зашифрувати, створити електронний підпис, а також аутентифікувати користувача (аутентифікація – процес ідентифікації користувачів, пристроїв або будь-якої іншої одиниці, що бере участь в інформаційному обміні, перед початком якого треба мати дозвіл на доступ до даних);

– SmartCard – магнітна картка для зберігання секретного ключа, шифрування паролей;

– пристрої ActivCard для введення паролей, де пароль не вводиться, а розраховується (динамічний пароль), а також SmartReader для зчитування паролей. У цих пристроях всередині вмонтовано мікропроцесор, у пам'яті якого зберігається секретний код. Пароль, що вводиться користувачем (чотири цифри), в комп'ютері перераховується, тобто створюється спеціальний код.

Програмні заходи:

– вбудовані у програми функції захисту даних. Наприклад, система Netware після трьох спроб користувача ввійти в мережу з неправильним паролем блокує ідентифікатор цього користувача, і тільки адміністратор мережі має змогу розблокувати доступ;

– спеціальні криптографічні розробки.

За принципом побудови наявні засоби захисту інформації можна поділити на два типи:

– засоби, в основі роботи яких лежать симетричні алгоритми для побудови ключової системи і системи аутентифікації;

– засоби, основу роботи яких складають асиметричні алгоритми, що застосовуються для тих самих цілей.

У засобах першого типу обов'язковою є наявність центру розподілу ключів, що відповідає за їх створення, розповсюдження та вилучення. Водночас носії ключової інформації передаються абонентам із використанням фізично захищених каналів зв'язку. Ключі мають змінюватися доволі часто, кількість абонентів має бути значною, тому ці засоби негнучкі та дорогі. Питання аутентифікації вирішується довірою користувачів один одному, цифровий підпис неможливий. Центр розподілу ключів контролює всю інформацію. Захист інформації дуже низький.

У засобах другого типу ключі для шифрування автоматично генеруються, розповсюджуються і вилучаються для кожного сеансу зв'язку. Функції служби розповсюдження ключів виконує сертифікаційний центр, де користувач реєструється, встановлюється його аутентифікація, після чого ключі вилучаються. В таких засобах можливою є організація цифрового підпису та його перевірка. Протокол встановлення аутентичного зв'язку відповідає певному стандарту. Аутентифікація є простою та суворою. У разі простої аутентифікації відбувається обмін паролями між абонентами, які встановили зв'язок із подальшою перевіркою відповідності цих паролів еталонним. У разі суворої аутентифікації кожен абонент має два криптографічні ключі – секретний, відомий тільки цьому абоненту, і відкритий – той, що передається в банк. Використовуючи секретний ключ і спеціальний алгоритм, абонент формує цифровий підпис – послідовність бітів, яка однозначно відповідає документу, що підписується. Перевірка відповідності підпису виконується за допомогою відкритого ключа.

Біометричні засоби:

– візерунки сітківки ока;

– відбитки пальців;

– геометрія руки;

– динаміка підпису.

Адміністративні заходи:

– систему електронних перепусток для персоналу і відвідувачів;

– системи відеоспостереження та відеореєстрації, що дають змогу вести цілодобовий візуальний нагляд і за периметром об'єкта, і всередині з можливістю запису інформації на відеомагнітофон або комп'ютер;

– розподіл доступу до інформації. Тут необхідне чітке визначення осіб, які мають право на ту чи іншу інформацію. Наприклад, програмісти не повинні мати доступу до баз даних, а користувачі – до програмного забезпечення;

– систематичний аналіз мережевого протоколу роботи, блокування спроб введення паролів декілька разів;

– ретельний підбір співробітників, навчання, стажування, тренування. Кандидат повинен мати хороші характеристики з попередніх робочих місць, не мати нахилу до зловживання наркотиками та алкоголем, не мати вагомих заборгованостей, не виявляти доброзичливості до наймачів.

Технічні заходи:

1) заходи захисту від прослуховування, що включають:

– встановлення фільтрів на лініях зв'язку;

– обстеження приміщень із метою виявлення підслуховуючих пристроїв;

– використання звукопоглинаючих стін, стелі, підлоги;

– застосування систем віброакустичного й акустичного зашумлення для захисту мовної інформації від прослуховування за допомогою акустичних мікрофонів, стетоскопів, лазерних та інфрачервоних систем відбору інформації;

2) заходи захисту від електромагнітного випромінювання, куди входять:

– використання оптоволоконного кабелю;

– застосування захисної плівки на вікнах;

– користування захищеними дисплеями;

– заходи захисту від поновлення вилучених даних.

4.2. Організаційні засоби захисту інформації

На вершині СУІБ знаходиться директор з ІБ, який очолює керуючий комітет з ІБ – колегіальний орган, призначений для вирішення стратегічних питань, пов'язаних із забезпеченням ІБ. Директор з ІБ несе відповідальність за всі процеси управління ІБ, а саме: за управління інцидентами і моніторинг безпеки, управління змінами та контроль захищеності, інфраструктуру безпеки (політики, стандарти, інструкції, процедури, плани та програми), управління ризиками, контроль відповідності вимогам, навчання (програма підвищення обізнаності). Створення цієї структури управління є метою впровадження стандарту ISO 27001/17799 в організації. Один з основних принципів тут – «прихильність керівництва». Це означає, що така структура може бути створена тільки керівництвом компанії, яке розподіляє посади, відповідальність і контролює виконання обов'язків. Інакше кажучи, керівництво організації будує відповідну вертикаль влади, а точніше, модифікує наявну для задоволення потреб організації в безпеці. СУІБ може створюватися тільки зверху вниз. Іншим основним принципом є залучення до процесу забезпечення ІБ всіх співробітників

організації, які працюють з інформаційними ресурсами – «від директора до прибиральниці». Необізнаність конкретних людей, які працюють з інформацією, відсутність програми навчання по ІБ, – одна з основних причин непрацездатності конкретних систем управління. Не менш важливо і те, що в основі будь-якого планування заходів з ІБ повинна бути оцінка ризиків. Відсутність організації процесів управління ризиками призводить до неадекватності прийнятих рішень і невиправданих витрат. Отже, оцінка ризиків є тим фундаментом, на якому тримається СУІБ.

Настільки ж фундаментальним принципом є «впровадження і підтримка СУІБ власними руками». Залучення зовнішніх консультантів на всіх етапах впровадження, експлуатації та вдосконалення СУІБ у багатьох випадках цілком виправдано. Навіть більше, це є одним із механізмів контролю, описаних у стандарті ISO 17799. Проте створення СУІБ руками зовнішніх консультантів неможливо за визначенням, тому що СУІБ – це сукупність організаційних структур, яка формується керівництвом організації і процесів, що реалізуються її співробітниками, які в належний спосіб поінформовані про свої обов'язки і навчені навичкам поводження з інформацією та її захисту. СУІБ коштує чималих грошей, але ні за які гроші не можна купити досвід і знання.

Використання системного підходу дасть змогу уникнути зайвих витрат на доопрацювання, а можливо, і повного перебудування системи інформаційної безпеки в майбутньому. Побудова фінансових і математичних моделей систем ІБ, оцінка загроз та їх наслідків, класифікація інформації, облік активів – все це повинно використовуватися під час розробки системи інформаційної безпеки. Правильна оцінка ризиків дає змогу істотно знизити витрати на інформаційну безпеку.

Існує велика кількість рекомендацій та документів, що регламентують питання побудови систем інформаційної безпеки. Можливість централізованого управління є найважливішою вимогою для ефективної і безперервної роботи системи інформаційної безпеки. Наприклад, технологія Check Point SMART, що реалізує централізоване управління, дає змогу легко керувати найскладнішими системами, істотно знижуючи як витрати на адміністрування, так і кількість помилок, що допускаються персоналом. Використання ж «клаптикового» методу побудови системи інформаційної безпеки робить її в підсумку некерованою, слабо контрольованою і марною.

Система управління інформаційною безпекою (Information Security Management System) є частиною загальної системи управління, що базується на аналізі ризиків і призначеної для проєктування, реалізації, контролю, супроводу і вдосконалення заходів в області інформаційної безпеки. Систему складають організаційні структури, політика, дії з планування, обов'язки, процедури, процеси і ресурси.

Основними цілями інформаційної безпеки є:

– конфіденційність інформації, тобто необхідність введення обмежень доступу до цієї інформації для певного кола осіб;

– неможливість несанкціонованого доступу до інформації, тобто ознайомлення з конфіденційною інформацією сторонніх осіб;

– цілісність інформації та пов'язаних з нею процесів (створення, введення, обробка і виведення), що полягає в її існуванні в неспотвореному вигляді (незмінному відносно деякого фіксованого її стану);

– доступність інформації, тобто здатність забезпечувати своєчасний і безперешкодний доступ осіб до інформації, яка цікавить їх;

– мінімізація ризиків інформаційної безпеки шляхом виконання компенсаційних заходів;

– облік усіх процесів, пов'язаних з ризиками.

Досягнення заданих цілей здійснюється під час вирішення таких завдань:

– введення в систему термінів інформаційної безпеки;

– класифікації інформаційних ресурсів підприємства;

– визначення власників процесів, відповідальних за інформаційну безпеку;

– розробки спектру ризиків інформаційної безпеки і проведення їх експертних оцінок;

– визначення групи доступу до інформаційних ресурсів;

– розробки системи управління ризиками інформаційної безпеки (методи і їх оцінка);

– складання переліків адміністративних і технічних заходів для мінімізації та компенсації ризиків;

– здійснення заходів інформаційної безпеки і періодичного контролю за станом ризиків;

– забезпечення фізичної безпеки і безпеки персоналу;

– розробки вимог до інформаційної системи з погляду інформаційної безпеки;

– контролінгу інформаційної безпеки на підприємстві.

Виділяють чотири стадії реалізації системи управління інформаційною безпекою:

1) формування політики в галузі ризиків;

2) аналіз бізнес-процесів;

3) аналіз ризиків;

4) формування цільової концепції.

Формування політики в галузі ризиків визначає принципи управління ними для всього підприємства загалом. Ці принципи базуються на цілях підприємства, його стратегії, а також на вимогах, що пред'являються законом і стандартами

в області інформаційної безпеки. Фактором ефективності системи управління інформаційною безпекою є її побудова на базі міжнародних стандартів ISO/IEC 17799:2005 та ISO/IEC 27001:2005.

Стандарт ISO/IEC 17799:2005 визначає принципи і являє собою довідник із розробки, впровадження, супроводу і покращення системи управління інформаційною безпекою, а також описує механізми визначення цілей контролю і його засобів у таких областях:

– політика безпеки (встановлення принципів управління і засобів забезпечення захисту інформації);

– управління безперервністю бізнес-процесів (запобігання втручанню в ділові операції і захист процесів обробки інформації від наслідків серйозних несправностей або катастроф);

– дотримання правових норм (виняток порушень кримінального та цивільного права, встановлених законом зобов'язань, регулятивних або контрактних зобов'язань, а також вимог з безпеки);

– організація активів і ресурсів (управління захистом інформації всередині організації);

– фізична безпека і безпека навколишнього середовища (запобігання несанкціонованому доступу, пошкодженню та проникненню в службові приміщення або втручанню в ділову інформацію);

– класифікація та управління активами (виявлення і захист інформаційних активів);

– захист персоналу (зниження ризиків, пов'язаних із помилкою оператора, крадіжкою, шахрайством або зловживанням використання обладнання);

– управління доступом (контроль доступу до інформації);

– управління засобами зв'язку та експлуатацією устаткування (коректне і безпечне функціонування засобів обробки інформації);

– розробка та обслуговування систем (впровадження засобів захисту в інформаційні системи).

Стандарт ISO/IEC 27001:2005 встановлює вимоги до системи управління інформаційною безпекою підприємства, являє собою довідник із визначення, мінімізації та управління небезпеками і загрозами, яким може піддаватися інформація, і розроблений з метою забезпечення допомоги у виборі ефективних і адекватних засобів для його захисту. Застосування стандарту ISO/IEC 27001:2005 на підприємстві дає змогу:

– встановити вимоги і цілі в області інформаційної безпеки;

– гарантувати впевненість у тому, що управління ризиками в області інформаційної безпеки є ефективним, а також те, що діяльність підприємства відповідає законодавству та іншим нормативним документам;

– реалізувати процес контролю за впровадженням системи управління інформаційною безпекою;

– ідентифікувати і відстежувати наявні процеси управління інформаційною безпекою;

– керівництву підприємства визначити стан процесів управління захистом інформації;

– внутрішнім і зовнішнім аудиторіям встановити рівень відповідності політики безпеки регламентам;

– забезпечити партнерів і постачальників відповідною інформацією про стандарти, процедури та політику підприємства.

Модель системи інформаційної безпеки підприємства – це сукупність зовнішніх і внутрішніх факторів, їх вплив на стан інформаційної безпеки підприємства і забезпечення зберігання ресурсів. На рис. 4.1 подано модель системи інформаційної безпеки підприємства, в якій представлені напрями впливу між такими факторами:

– загрозами інформаційній безпеці, що характеризуються ймовірністю виникнення і реалізації;

– вразливістю системи інформаційної безпеки, що впливає на ймовірність реалізації загрози;

– ризиками, що відображають завдання шкоди внаслідок реалізації загрози інформаційній безпеці.

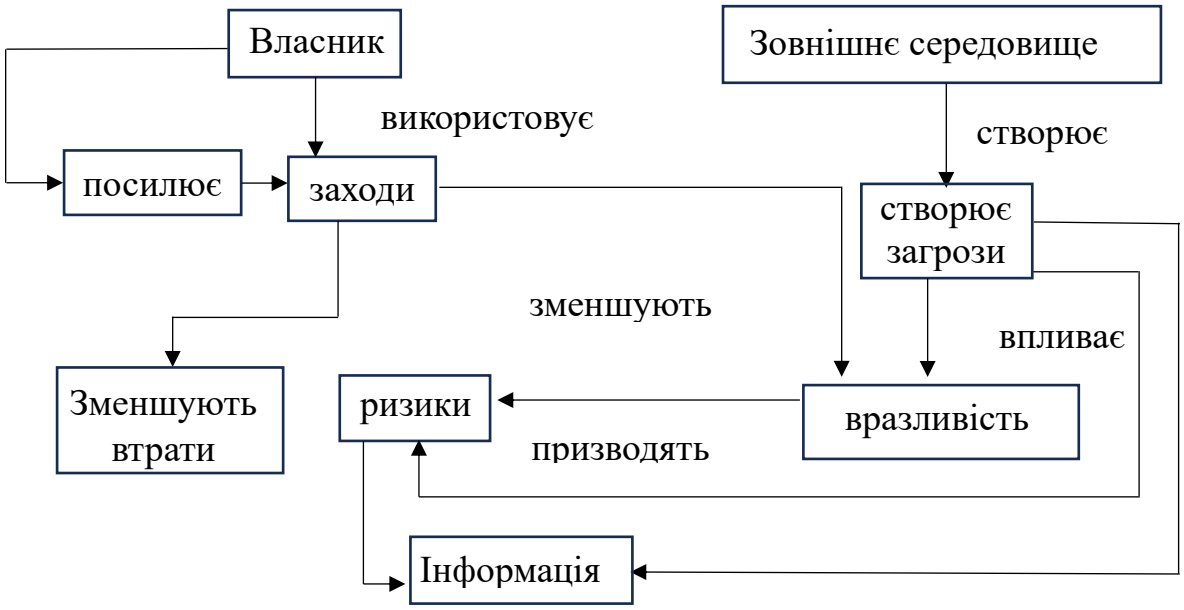

Рисунок 4.1. Модель системи інформаційної безпеки підприємства

Інформація та матеріальні ресурси, які необхідно захищати, називаються об’єктами захисту. До них належать:

– мовна інформація;

– інформація, що зберігається і обробляється за допомогою засобів зв'язку у вигляді різних носіїв;

– документи на паперових носіях;

– технічні засоби зв'язку та інформатизації;

– приміщення, призначені для обговорення, обробки і зберігання інформації;

– інформаційні системи загалом, включно з системою зв'язку;

– документація на технічні та програмні засоби зв'язку й інформатизації;

– програмні засоби.

Загрози, з якими може зіткнутися підприємство, класифікуються за своєю природою їх виникнення: як загрози випадкового або навмисного характеру; і за відношенням до того, хто захищається: зовнішні і внутрішні загрози.

Джерелами зовнішніх загроз є:

– діяльність конкурентів із перехоплення важливої інформації;

– навмисні дії зі руйнування, знищення або модифікації інформації;

– ненавмисні дії співробітників сторонніх організацій, що призвели до відмови в роботі елементів системи;

– стихійні лиха і катастрофи, аварії, екстремальні ситуації.

До джерел внутрішніх загроз належать:

– відсутність координації діяльності підрозділів підприємства у сфері захисту інформації;

– навмисні дії персоналу зі знищення або модифікації інформації;

– ненавмисні помилки персоналу, відмови технічних засобів і збої в інформаційних системах;

– порушення встановлених регламентів збору, накопичення, зберігання, обробки, перетворення, відображення і передачі інформації.

Порушення можуть бути декількох видів:

Організаційно-правові порушення – порушення, пов'язані з відсутністю єдиної узгодженої політики підприємства у сфері захисту інформації, невиконанням вимог нормативних документів, режимом доступу, зберігання та знищення інформації.

Організаційні види порушень включають несанкціоноване отримання доступу до баз і масивів даних, несанкціонований доступ до активного мережевого обладнання, серверів, некоректне вбудовування засобів захисту і помилки в управлінні ними, порушення в адресності розсилки інформації під час ведення інформаційного обміну.

Фізичні види порушень – пошкодження апаратних засобів автоматизованих систем, ліній зв'язку та комунікаційного обладнання, крадіжки або несанкціоноване ознайомлення зі змістом носіїв інформації, їх розкрадання.

До радіоелектронних видів порушень належать впровадження електронних пристроїв перехоплення інформації, отримання інформації шляхом перехоп-

лення і дешифрування інформаційних потоків, фотографування моніторів, нав'язування неправдивої інформації в локальних обчислювальних мережах, передачі даних лініями зв'язку.

Для протидії загрозам і припинення порушень на підприємствах організовується процес управління ризиками, який є основою системи інформаційної безпеки підприємства. Побудова ефективної системи інформаційної безпеки – це комплексний процес, спрямований на мінімізацію зовнішніх і внутрішніх загроз під час обліку обмежень на ресурси і час. З погляду процесного підходу систему інформаційної безпеки підприємства можна уявити як процес управління ризиками (рис. 4.2), що включає такі складники:

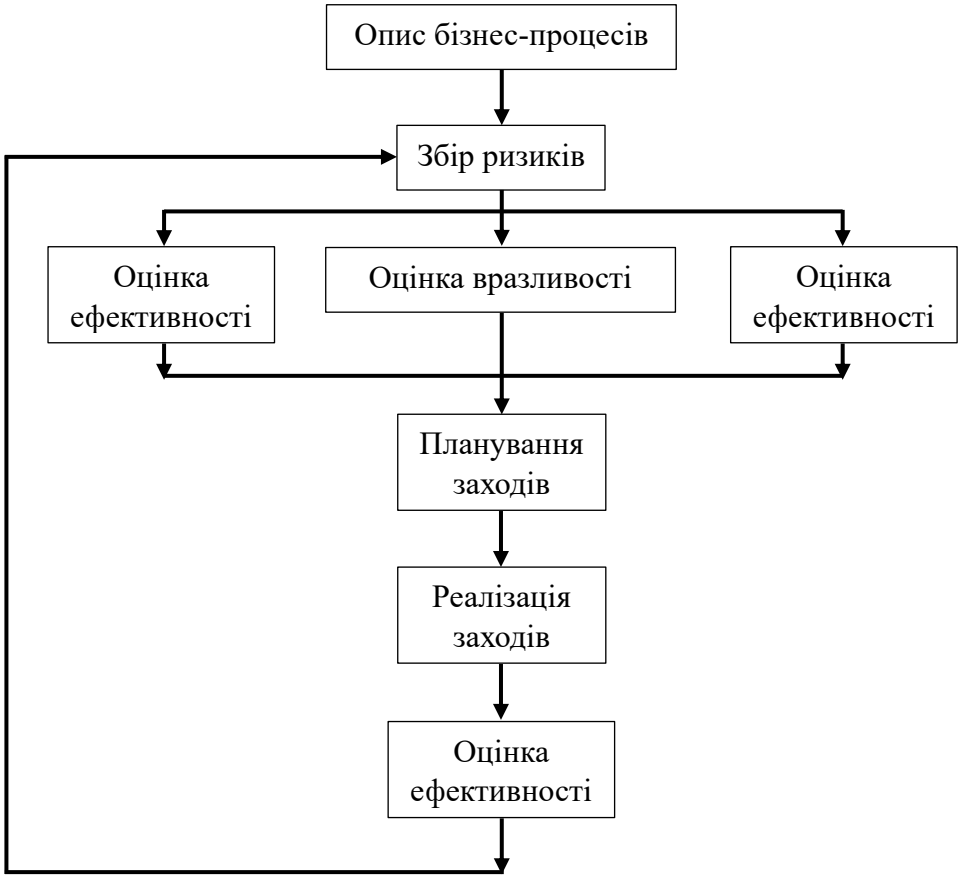

Рисунок 4.2. Модель процесу управління ризиками для системи інформаційної безпеки

1. Опис бізнес-процесів. Виконується коригування та аналіз бізнес-процесів. За критеріями, що визначаються під час формування політики в галузі ризиків, здійснюється ідентифікація бізнес-процесів.

2. Збір ризиків. Проводиться для виявлення ступеня схильності підприємства до загроз, що можуть завдати істотної шкоди. Для цього здійснюється аналіз його бізнес-процесів і опитування експертів предметної області. Результатом (виходом) цього процесу вважається класифікаційний перелік всіх потенційних ризиків.

До стандартних ризиків інформаційної безпеки належать:

– вилучення конфіденційної інформації з локальних місць;

– навмисна зміна інформації з метою знищення;

– копіювання важливих документів і передача конкуренту;

– незаконне проникнення в корпоративну мережу;

– знищення через технічні причини.

3. Оцінка ризиків. Визначаються характеристики ризиків і ресурси інформаційної системи. Основним результатом (виходом) цього процесу є перелік усіх потенційних ризиків із їх кількісними та якісними оцінками шкоди і можливості реалізації, а додатковим – перелік ризиків, що не будуть відслідковуватися на підприємстві.

Процес оцінки ризиків складається з таких кроків:

– опис об’єкту і заходів захисту;

– ідентифікація ресурсу і визначення його кількісних показників;

– аналіз загроз інформаційної безпеки;

– оцінка вразливостей;

– оцінка наявних і передбачуваних засобів забезпечення інформаційної безпеки.

4. Планування заходів. Метою планування заходів із мінімізації ризиків є визначення термінів та переліку робіт із виключення або мінімізації збитку в разі мінімізації ризику.

Виділяються такі види заходів з інформаційної безпеки:

– організаційні;

– правові;

– організаційно-технічні;

– програмні;

– інженерно-технічні.

5. Реалізація заходів. Під реалізацією заходів щодо мінімізації ризиків маються на увазі виконання запланованих робіт, контроль якості отриманих результатів і термінів. Результатом цього процесу є виконані роботи з мінімізації ризиків і час їх проведення.

6. Оцінка ефективності. Оцінка ефективності системи управління інформаційною безпекою – системний процес отримання та оцінки об’єктивних даних про поточний стан системи, дії і події, що відбуваються в ній, що встановлює рівень їх відповідності певним критеріям.

Цілями процесу є:

– оцінка поточного рівня ефективності системи;

– локалізація «вузьких» місць у системі;

– оцінка відповідності системи підприємства наявним стандартам в області інформаційної безпеки;

– вироблення рекомендацій та регламентів щодо забезпечення безпеки об’єктів захисту.

Результати процесу можуть використовуватися в цілях аудиту для підготовки підприємства до сертифікації за стандартом ISO/IEC 27001:2005.

4.3. Технічні системи захисту даних

Система захисту інформації, що обробляється з використанням технічних засобів, будується за певними принципами. Це обумовлено необхідністю протидії цілій низці загроз безпеці інформації.

Основним принципом протидії загрозам безпеці інформації є *превентивність вжитих заходів захисту,* оскільки усунення наслідків проявів загроз вимагає значних фінансових, часових і матеріальних витрат.

Диференціація заходів захисту інформації залежно від її важливості та частоти і ймовірності виникнення загроз безпеці є наступним основним принципом протидії загрозам.

До принципів протидії загрозам також належить *принцип достатності заходів захисту інформації,* що дає змогу реалізувати ефективний захист без надмірного ускладнення системи захисту інформації.

Протидія загрозам безпеці інформації завжди має агресивний характер відносно користувачів і обслуговуючого персоналу автоматизованих систем через накладання обмежень організаційного і технічного характеру. Тому одним із принципів протидії загрозам є *принцип максимальної дружності системи забезпечення інформаційної безпеки.* Водночас варто враховувати сумісність створюваної системи протидії загрозам безпеці інформації з операційною та програмно-апаратною структурою автоматизованої системи і сформованими традиціями установи. Важливість реалізації цього принципу заснована на тому, що додавати до наявної незахищеної автоматизованої системи засоби захисту інформації складніше і дорожче, ніж початково проєктувати і будувати захищену систему.

З принципу декомпозиції механізму впливу загроз безпеці інформації випливає принцип самозахисту і конфіденційності системи захисту інформації, що полягає в застосовності принципів протидії загрозам до самої системи захисту і дотримання конфіденційності реалізованих механізмів захисту інформації в автоматизованій системі. Реалізація цього принципу дає змогу контролювати цілісність системи захисту інформації, управляти безпекою через адміністратора безпеки, відновлювати систему захисту у разі її компрометації і відмов устаткування.

Засоби захисту інформації, присутні сьогодні на ринку, умовно можна поділити на кілька груп:

– активні і пасивні технічні засоби, що забезпечують захист від витоку інформації за різними фізичними параметрами, що виникають під час застосування засобів її обробки;

– програмні та програмно-технічні засоби, що забезпечують розмежування доступу до інформації на різних рівнях, ідентифікацію та автентифікацію користувачів;

– програмні та програмно-технічні засоби, що забезпечують захист інформації і підтвердження її справжності під час передачі каналами зв'язку;

– програмно-апаратні засоби, що забезпечують цілісність програмного продукту і захист від несанкціонованого його копіювання;

– програмні засоби, що забезпечують захист від впливу програм-вірусів та інших шкідливих програм;

– фізико-хімічні засоби захисту, що забезпечують підтвердження автентичності документів, безпеку їх транспортування і захист від копіювання.

Окремо виділяються захищені загальносистемні програмні продукти, що виключають можливість використання декларованих програмних можливостей. Таких систем поки що не дуже багато. Сюди ж віднесені і спеціальні пристрої – міжмережеві екрани: для забезпечення захисту корпоративних мереж від вторгнення з глобальних інформаційних мереж типу Internet.

Сьогодні засоби і системи, призначені для захисту інформації та підтвердження її справжності під час передачі каналами зв'язку, і насамперед криптографічні пристрої, виробляються більш ніж 700 закордонними фірмами. Для захисту конфіденційної інформації, що передається каналами зв'язку, можуть використовуватися скремблери (обробляють і шифрують сигнал) і шифратори (перетворення n-розрядного коду в k-розрядний код). Для захисту конфіденційної інформації в каналах радіосистем зв'язку призначені пристрої фірми Simens (Німеччина), Grundy & Pirtners (Великобританія).

Низка фірм випускає криптографічні пристрої, орієнтовані на роботу в мережах, наприклад, шифратор ScaNet фірми Dowty Network Systems (Великобританія), шифратор Datacryptor-64 фірми Racal Datacom (США) для користувачів мережі з пакетною комутацією за протоколом X.25 МККТТ. Фірма NFT (Норвегія) розробила серію криптомодулів зі швидкостями до 10 Мбіт/с, призначених для засекречування потоків і застосування в локальних мережах. Фірма Xerox (США) створила блок високоякісного шифрування даних Xerox Encription Unit, що забезпечує захист особливо секретної інформації, в локальній мережі. Фірма PE Systems (США) поставляє систему GILLAROO для передачі цифрового підпису та захисту секретної інформації, переданої в мережах і каналах зв'язку. Фірма Calmes Semiconductor Inc. (США) виробляє криптопроцесор СЛ34С168 для блочного шифрування на швидкості до 300 кбіт/с. Запропоно-

вано нові алгоритми шифрування, наприклад, NEWDES і FEAL, розраховані на шифрування потоків зі швидкостями до 1 гбіт/с.

Останнім часом все більшого поширення на ринку програмно-апаратних засобів захисту інформації отримують системи запобігання несанкціонованого копіювання програмних продуктів типу «HASP-ключів». Основою багатьох сучасних систем охорони приміщень і захисту від несанкціонованого доступу до інформації є електронні ідентифікаційні пристрої. Прикладом такого пристрою є автоматичний ідентифікатор, вироблений американською фірмою DALLAS SEMICONDUCTOR. Ідентифікатор може бути вбудований у брелок, візитну картку, перепустку. Залежно від варіанта застосування автоматичний ідентифікатор може використовуватися з різними додатковими пристроями: електронними замками, комп'ютерами.

Наявність в ідентифікаторі змінної пам'яті дає змогу використовувати його для широкого класу додатків, наприклад, для зберігання особистих, періодично змінюваних ключів шифрування користувача; для зберігання інформації про стан особового рахунку користувача для розрахункових систем; для зберігання інформації про дозволений час проходу в пропускних системах. Використання ідентифікатора разом з електронними замками дає широкі можливості для керування доступом користувачів у режимні приміщення: централізоване оперативне стеження за проходом у приміщення, дистанційне керування допуском, гнучке встановлення правил допуску в приміщення (наприклад, у певні дні і години).

Новітні технології засновані на використанні фізико-хімічних властивостей матеріалів і забезпечують підтвердження автентичності документів, безпеку їх транспортування і захист від копіювання. Це спеціальні тонкоплівкові матеріали зі змінною кольоровою гамою на основі технології Advateg, що наносяться на документи і предмети або голографічні мітки. Вони дають змогу однозначно ідентифікувати достовірність об'єкта і контролювати несанкціонований доступ до них. До того ж на основі технології Advateg розроблені спеціальні конверти, пакети та інший пакувальний матеріал, що дає змогу гарантувати конфіденційність документів і матеріальних засобів під час їх транспортування навіть звичайними поштовими каналами.

Група технічних засобів захисту інформації поєднує апаратні і програмні засоби. Основні:

– резервне копіювання і віддалене зберігання найбільш важливих масивів даних у комп'ютерній системі – на регулярній основі;

– дублювання і резервування всіх підсистем мереж, що мають значення для збереження даних;

– створення можливості перерозподіляти ресурси мережі в випадках порушення працездатності окремих елементів;

– забезпечення можливості використовувати резервні системи електроживлення;

– забезпечення безпеки від пожежі або пошкодження обладнання водою;

– установка програмного забезпечення, що забезпечує захист баз даних та іншої інформації від несанкціонованого доступу.

У комплекс технічних заходів входять і заходи щодо забезпечення фізичної недоступності об'єктів комп'ютерних мереж, наприклад, практичні способи, як-от обладнання приміщення камерами і сигналізацією.

4.4. Механізми інформаційної безпеки

Існують такі концептуальні механізми інформаційної безпеки:

– ідентифікація та автентифікація;

– контроль і управління доступом;

– протоколювання й аудит;

– шифрування;

– контроль цілісності;

– екранування.

Для надійного захисту інформації необхідна комплексна реалізація всіх перерахованих механізмів. Деякі з них можуть бути реалізовані більш повною мірою, інші – ні. Захист інтелектуальної власності насамперед залежить від реалізації механізму ідентифікації і автентифікації.

Ідентифікатор – унікальний набір символів, що відповідає об'єкту або суб'єкту в цій системі.

Ідентифікація – розпізнавання учасника процесу інформаційної взаємодії перед тим, як до нього будуть застосовані аспекти інформаційної безпеки.

Пароль – секретний набір символів, що дає змогу підтвердити відповідність суб'єкта пред'явленому ідентифікатору.

Автентифікація – забезпечення впевненості в тому, що учасник інформаційної взаємодії ідентифікований правильно.

Профіль – набір установок і конфігурацій для цього суб'єкта чи об'єкта, що визначає його роботу в інформаційної системі.

Авторизація – формування профілю прав для конкретного учасника інформаційної взаємодії.

Суб'єкт може підтвердити свою автентичність, пред'явивши принаймні один з об'єктів:

– щось, що він знає (пароль, криптографічний ключ і т. ін.);

– щось, чим він володіє (електронний ключ, смарт-карта і т. ін.);

– щось, що є частина його самого (свої біометричні дані).

Автентифікація буває односторонньою (зазвичай суб'єкт доводить свою справжність системі) і двосторонньою (взаємною). Розглянемо її особливості.

1. Ідентифікація та автентифікація

Надійна ідентифікація і автентифікація неможлива через низку причин. В інформаційній системі між сторонами може не існувати довіреного маршруту: це означає, що в загальному випадку дані, передані суб'єктом, можуть не збігатися з даними, отриманими і використаними для перевірки автентичності. Майже всі автентифікаційні об'єкти можна дізнатися, вкрасти або підробити. Є суперечності між надійністю автентифікації, з одного боку, і зручностями суб'єкта, з іншого. Так, із міркувань безпеки необхідно з певною частотою просити користувача повторно вводити автентифікаційну інформацію. Чим надійніший засіб захисту, тим він дорожчий.

2. Парольна автентифікація

Головна перевага парольної автентифікації – простота. Недолік – найслабший засіб перевірки автентичності. Основні порушення під час створення і використання паролів:

– простий пароль;

– використання стандартних значень із будь-якої документації, що ніколи не забути;

– запис пароля там, де його можна прочитати, підглянути тощо;

– передавання пароля іншому співробітнику.

Заходи, що дають змогу підвищити надійність парольного захисту:

– накладання технічних обмежень (довжина, використання букв, цифр, знаків);

– управління терміном дії паролів;

– обмеження доступу до файлу паролів;

– обмеження кількості невдалих спроб входу в систему;

– навчання користувачів;

– використання програмних генераторів паролів, які, ґрунтуючись на деяких правилах, можуть створювати складні, але легкі для запам'ятовування паролі;

– одноразові паролі.

3. Одноразові паролі

Маємо односторонню функцію f (функція, обчислити зворотну до якої за прийнятний час не видається можливим). Ця функція відома і користувачеві, і серверу автентифікації. Маємо секретний ключ K, відомий тільки користувачу. На етапі початкового адміністрування користувача функція f застосовується до ключа K n-разів, після чого результат зберігається на сервері.

Після цього процедура перевірки автентичності користувача виглядає так:

– сервер надсилає на призначену для користувача систему число $(n - 1)$;

– користувач застосовує функцію f до секретного ключа K (n – 1) разів і надсилає результат по мережі на сервер автентифікації;

– сервер застосовує функцію f до отриманого від користувача значення і порівнює результат із раніше збереженою величиною.

У разі збігу справжність користувача вважається встановленою, сервер запам'ятовує нове значення (надіслане користувачем) і зменшує на одиницю лічильник (n). Оскільки функція f необоротна, перехоплення пароля і отримання доступу до сервера автентифікації не дадуть змогу дізнатися секретний ключ K і передбачити наступний одноразовий пароль.

Інший підхід до реалізації одноразових паролів полягає в генерації нового пароля через невеликий проміжок часу (наприклад, кожні 60 секунд), для чого можуть використовуватися програми або smart-карти. Для цього необхідно виконання умов:

1. Сервер автентифікації повинен знати алгоритм генерації паролів і асоційовані з ним параметри.

2. Годинники клієнта і сервера повинні бути синхронізовані.

Автентифікація з використанням токенів можлива в таких випадках:

– На запит системи токен пред'являє їй секретне значення, що слугує для підтвердження автентичності. Один раз перехопивши цю відповідь, зловмисник може імітувати відповідь токена.

– Токен і система мають загальну, синхронізовану систему генерації одноразових паролів. На запит системи токен видає пароль, дійсний для цього проміжку часу. Система генерує в цей час свій варіант пароля, який порівнює з отриманим.

– Токен зареєстрований в системі (вона знає його секретний параметр). Для автентифікації вона формує випадкову величину, яку токен перетворює з використанням свого параметра. Система виконує аналогічне перетворення і порівнює результат з отриманим від токена. В цьому випадку перехоплення запиту і відповіді нічого не дає зловмиснику, синхронізація токена і системи не потрібна.

Варіанти використання токена спільно з паролем:

– Пароль слугує для доступу до токена, що без пароля не діє.

– Пароль разом із параметром токена є основою для вироблення одноразових паролів.

– Токен генерує відповідь системі на запит з випадковою величиною на основі свого параметра і пароля користувача.

4. Автентифікація за допомогою біометричних даних

Біометрія являє собою сукупність автоматизованих методів ідентифікації і автентифікації людей на основі їх фізіологічних і поведінкових характеристик.

До фізіологічних характеристик належать особливості:

– відбитків пальців,
– сітківки та рогівки очей,
– геометрія руки та обличчя.

До поведінкових характеристик належать:

– динаміка підпису,
– стиль роботи з клавіатурою.

До характеристик, що включають фізіологію і поведінку, належать аналіз особливостей голосу і розпізнавання мови.

У загальному вигляді робота з біометричними даними організована так. Спочатку створюється і підтримується база даних характеристик потенційних користувачів. Для цього біометричні дані користувача знімаються, обробляються, і результат обробки (званий біометричним шаблоном) заноситься в базу даних. Водночас вихідні дані, як-от результат сканування пальця або рогівки, зазвичай не зберігаються. Надалі для ідентифікації й одночасно автентифікації користувача процес зняття і обробки повторюється, після чого проводиться пошук у базі даних шаблонів. У разі успішного пошуку особистість користувача і його достовірність вважаються встановленими. Для автентифікації достатньо зробити порівняння з одним біометричних шаблоном, обраним на основі попередньо введених даних. Зазвичай біометрію застосовують разом з іншими автентифікатором, як-от smart-карти. Іноді біометрична автентифікація слугує для активізації smart-карт – у цьому разі біометричний шаблон зберігається на тій самій карті.

Біометрія схильна до тих самих загроз, що й інші методи автентифікації. Біометричний шаблон порівнюється не з результатом первісної обробки характеристик користувача, а з базою даних, що знаходиться в місці порівняння. Біометричні методи не є більш надійними, ніж база даних шаблонів. Треба враховувати різницю між застосуванням біометрії на контрольованій території і в «польових» умовах.

Біометричні дані людини змінюються, тому база шаблонів потребує супроводу. Але головна небезпека полягає в тому, що якщо біометричні дані виявляться скомпрометовані, доведеться як мінімум проводити істотну модернізацію всієї системи.

4.5. Методи визначення рівня інформаційного ризику

До одного з методів визначення рівня інформаційного ризику належить аналіз інформаційних ризиків. Аналіз інформаційних ризиків – процес комплексної оцінки захищеності інформаційної системи кількісними і якісними показниками. Однією з основних проблем аналізу інформаційних ризиків є оцінка

вартості (ціни) ризиків. Сьогодні не існує єдиної методики. Причини цього – відсутність достатнього обсягу статистичних даних про ймовірність реалізації конкретної загрози, неоднозначність оцінок вартості інформаційного ресурсу (матеріальних і нематеріальних). У цих умовах поширені якісні методи оцінки ризиків, засновані на експертних оцінках. Такий підхід ускладнює можливості моделювання ризикової ситуації і не дає змоги говорити про об'єктивність результату. У літературі визначають чинники, що впливають на величину ризику:

1. Міра тяжкості наслідків, яку можна виміряти у відсотковому відношенні від вартості ресурсу, якщо вона фіксована. Наприклад, якщо збиток у межах до 10 % вартості ресурсу, то тяжкість наслідків низька, в інтервалі 11–30 % – помірна, 31–80 % – критична, більше 81 % – катастрофічна:

а) трудовитрати, необхідні для виправлення наслідків інциденту і залежні від вартості одного інциденту і кількості інцидентів за оцінюваний період. Трудовитрати на виправлення наслідків одного інциденту складаються з трудовитрат на діагностування, документування, виправлення, повідомлення про результати;

б) матеріальні збитки (втрачена вигода);

в) репутаційний збиток.

2. Оцінка ймовірності реалізації загрози ранжується за шкалою від 1 до 5 (дуже низька, низька, середня, висока, дуже висока). Ймовірність залежить від рівня вразливості ресурсу до загрози та ефективності управління:

– Вразливість процесу, для якого ключова інформація є або входом, або виходом. Шкала включає значення: низький, середній, високий. Вразливість означає наявність передумов для створення іншої загрози.

– Частка інцидентів, спровокованих загрозою, і спричинили збитки в загальній кількості інцидентів, спровокованих цією загрозою, за минулий період. Шкала включає значення: дуже низький (0–19 %), низький (20–39 %), середній (40–60 %), високий (61–80 %), дуже високий (81–100 %).

– Ефективність керування ранжується за шкалою від 1 до 5 за класифікатором рівнів зрілості університету Carnegie Mellon. Відповідність понять ефективність управління і рівня зрілості компанії наведено в таблиці (табл. 4.1).

Проблема інформаційної безпеки для застосування зазначеної вище шкали підтверджується дослідженням компанії PricewaterhouseCoopers (PwC) на основі аналізу 21 підприємства і 68 проєктів. Організації з низькою ефективністю переважно володіють 1–2 рівнями зрілості. Організації з високою ефективністю володіють 3, 4, 5 рівнями зрілості. Крім того, аналітиками компанії PwC виявлено, що підвищення рівня зрілості дає істотне покращення результатів проєктів (30 % компаній покращили свої результати більш ніж на 25 %) [13].

Граничні значення у всіх цих випадках підбираються для кожного випадку індивідуально. Оцінка очікуваних втрат від конкретної загрози, на увазі застосування експертних оцінок і шкал, що містять лінгвістичні змінні, може бути здійснена за допомогою теорії нечітких множин. Відомо застосування методу нечітких множин при оцінці ефективності інвестиційних проектів [24].

Таблиця 4.1

Оцінка рівня зрілості за класифікатором університету Carnegie Mellon

Рівень зрілості	Критерії
1	Проблема формально не висувається
2	Проблема вирішується на основі практичних дій. Питання щодо ефективності захисту не розуміється. Серйозних порушень не відбувалося
3	Часткове впровадження стандартів і рекомендацій. Приділяється увага питанням документування
4	Актуальні питання вимірювання параметрів, що характеризують режим інформаційної безпеки. Застосування кількісних методів аналізу ризиків
5	Ставляться і вирішуються різні варіанти оптимізаційних задач в області інформаційної безпеки

4.6. Управління ризиками інформаційної безпеки (сімейство стандартів ISO/IEC 27000)

В основі організації, планування й здійснення практичних дій щодо забезпечення безпеки є аналіз концепції загрози, оцінка характеру реальних і потенційних внутрішніх / зовнішніх небезпек і загроз, кризових ситуацій, а також інших несприятливих факторів. Система реальних і потенційних загроз не є постійною; загрози можуть з’являтися й зникати, наростати й зменшуватися, при цьому змінюватиметься їхня значимість для безпеки.

Друге видання скасовує та замінює перше видання (ISO 31000:2009), що було технічно переглянуто.

Основні зміни, порівняно з попереднім виданням:

– огляд принципів управління ризиками, що є ключовими критеріями його успіху;

– виділення окремого керівництва з боку вищого керівництва і інтеграція управління ризиками, починаючи з управління організацією;

– акцентування на ітеративну природу управління ризиками, відзначаючи, що новий досвід, знання і аналіз можуть привести до перегляду елементів процесу, дій і засобів контролю на кожній стадії процесу;

– раціоналізація контенту з наданням більшої уваги підтримці моделі відкритих систем у відповідності з різними потребами і контекстами.

Цей документ призначений для використання людьми, які створюють і захищають цінності в організаціях шляхом управління ризиками, прийняття рішень, постановки і досягнення цілей і підвищення ефективності.

Багато організацій стикаються із зовнішніми і внутрішніми факторами і впливами, які заважають впевнено досягати своїх цілей.

Управління ризиками носить ітеративний характер і допомагає організаціям визначати стратегію, досягати мети і приймати обґрунтовані рішення.

Управління ризиками є частиною управління і лідерства і має основоположне значення для управління організацією на всіх рівнях. Це сприяє вдосконаленню систем управління.

Управління ризиками є частиною всієї діяльності, пов'язаної з організацією, і включає взаємодію з зацікавленими сторонами.

Управління ризиками враховує зовнішній і внутрішній контекст організації, включаючи поведінку людини і культурні фактори.

Управління ризиками засноване на принципах, структурі і процесі, викладених в цьому документі, як показано на рис. 4.3. Ці компоненти можуть вже існувати повністю або частково всередині організації, проте їх може знадобитися адаптувати або покращити, щоби управління ризиками було ефективним, дієвим і послідовним.

Управління безпекою великих організацій, що використовують інформаційні та телекомунікаційні технології, рекомендується здійснювати на основі стандартів BS 7799/ISO 17799 ISO/IEC 27001. Сьогодні активно використовується стандарт ISO 17799 і відбувається поступовий перехід до стандартів серії 27001. Управління безпекою націлено на захист усіх складових, що сприяють здійсненню бізнес-процесу, який організовано на підприємстві (рис. 4.3).

Серія 27001 являє собою модель системи менеджменту в сфері інформаційної безпеки (СМІБ, Information Security Management System, ISMS). Як і будь-яка сучасна система менеджменту, СМІБ – це набір організаційних заходів і процедур управління і вона не є, по суті, технічним стандартом. В основі стандарту полягає процесний підхід до розробки, реалізації, експлуатації, моніторингу, аналізу, супроводу та покращанню СМІБ організації. Він складається зі створення та використання системи процесів управління, що взаємопов'язані у безперервному циклі планування, використання, перевірки та покращання СМІБ (рис. 4.3, частина бізнес-процесу). Додатково в групі стандартів рекомендовано перелік механізмів захисту інформації програмно-технічного рівня, що можуть використовуватися на різних стадіях здійснення бізнес-процесу (рис. 4.4, частина технології).

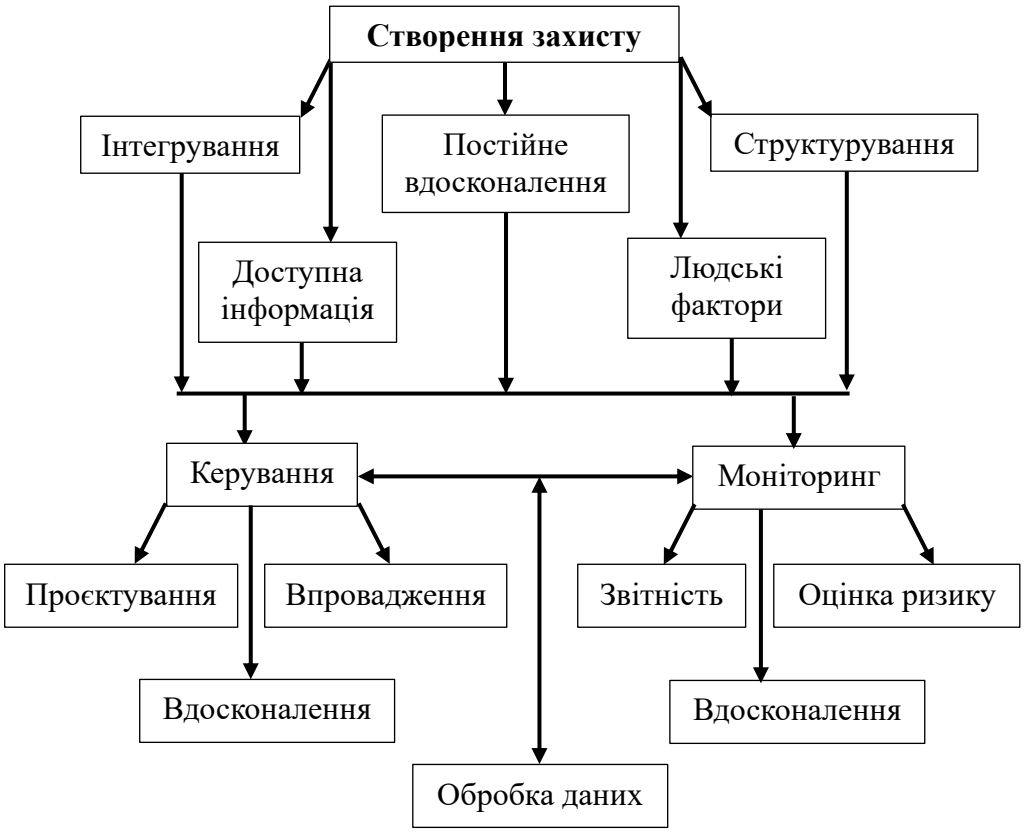

Рисунок 4.3. Принципи, структура і процес управління безпекою

В Україні діють такі стандарти по технічному захисту інформації:

– ДСТУ 3396.0-96. «Захист інформації. Технічний захист інформації. Основні положення». Цей стандарт встановлює об'єкт, мету, організаційні положення забезпечення технічного захисту інформації (ТЗІ), неправомірний доступ до якої може завдати шкоди громадянам, організаціям (юридичним особам) і державі, а також категорії нормативних документів системи ТЗІ.

– ДСТУ 3396.1-96. «Захист інформації. Технічний захист інформації. Порядок проведення робіт». Стандарт встановлює вимоги до порядку проведення робіт з технічного захисту інформації.

– ДСТУ 3396.2-96. «Захист інформації. Технічний захист інформації. Терміни й визначення». Цей стандарт встановлює терміни й визначення понять у сфері технічного захисту інформації.

Серед міжнародних стандартів про інформаційну безпеку найбільш відомим є британський – BS 7799, розроблений Британським інститутом стандартів (British Standards Institution – BSI). Стандарт BS 7799 складається із двох частин.

Серія стандартів з менеджменту інформаційної безпеки ISO/IEC 27000 розробляється технічним комітетом ISO/IEC JTC 1 підкомітетом SC 27.

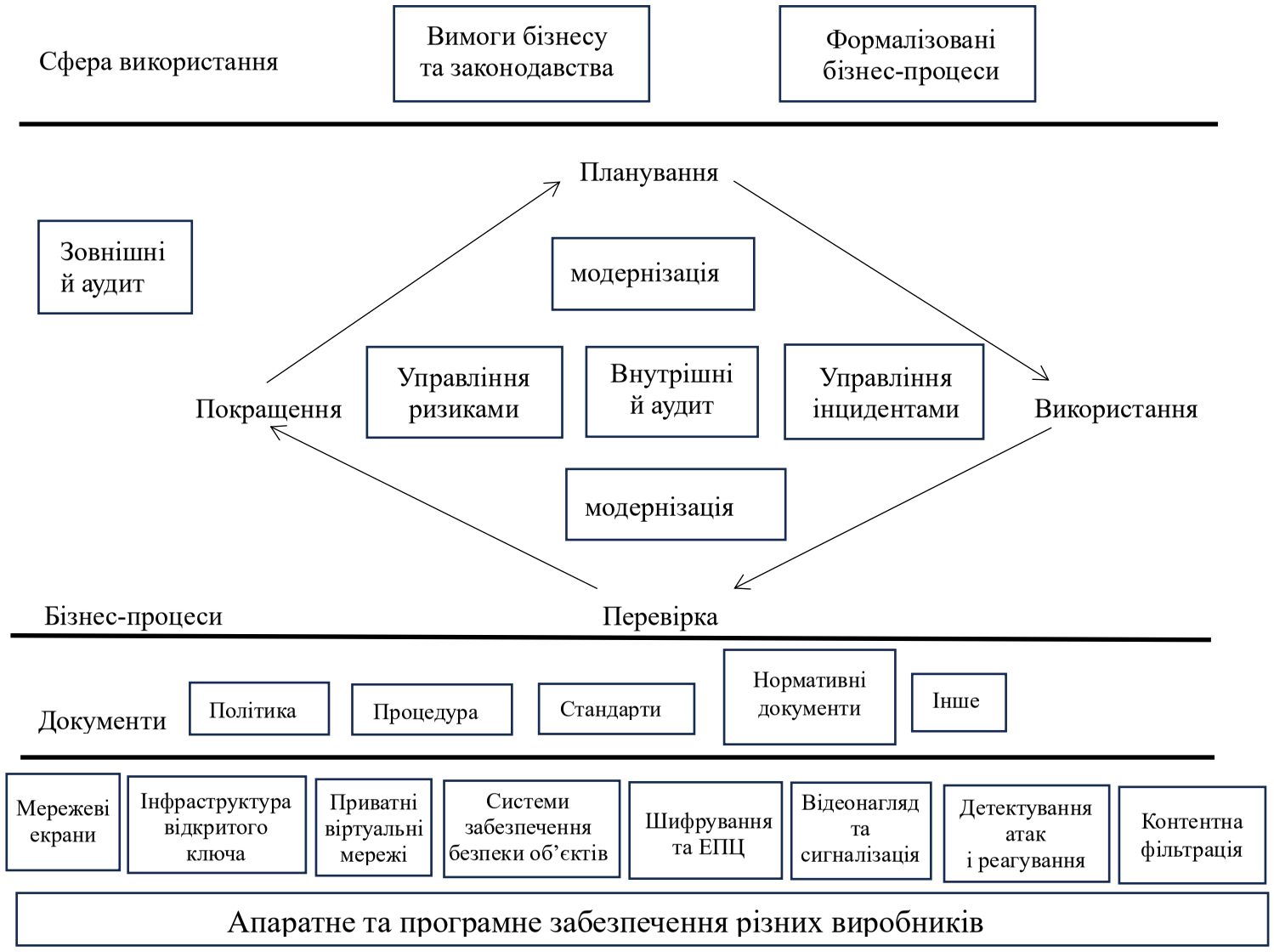

Рисунок 4.4. Загальна схема управління безпекою бізнес-процесів на основі телекомунікацій

Система менеджменту інформаційної безпеки (СМІБ) містить у собі вимоги щодо реалізації та вдосконалення систем управління захистом інформації і ґрунтується на моделі PDCA (Plan-Do-Check-Act):

– створення – ідентифікація активів, менеджмент ризиків;
– впровадження – етап реалізації відповідних заходів з управління безпекою;
– перевірка – моніторинг і аналіз;
– дія – підтримання в робочому стані і покращення.

З огляду на це видно, що крім розробки правил управління і забезпечення безпеки, не менш важливо забезпечити циклічність усіх процесів з управління безпекою, щоб усі процедури послідовно проходили етапи моделі PDCA. Саме це вказує на відповідність системи управління стандарту ISO 27001 і свідчить про готовність до сертифікації СМІБ.

Виконання вимог стандарту ISO/IEC 27001 в основному дає змогу мінімізувати ризики втрат активів підприємства / організації, а отже, скоротити фінансові втрати.

Стандарт ISO/IEC 27001 призначений для сертифікації систем інформаційної безпеки.

Сертифікація системи менеджменту інформаційною безпекою (сертифікація СМІБ) – ефективне управління бізнес-процесами організації, інформаційними ризиками, а також свідоцтво про стійкий розвиток і надійність компанії, що дає позитивне ставлення бізнес-партнерів.

СМІБ відповідно до стандарту ISO/IEC 27001 – це частина загальної системи менеджменту компанії.

Сімейство стандартів ISO 27000 включає в себе такі документи, що стосуються систем менеджменту ІБ:

ISO/IEC 27001 Information security management systems. Requirements – Системи менеджменту інформаційною безпекою. Вимоги.

ISO/IEC 27000 Information security management systems. Overview and vocabulary – Системи менеджменту інформаційної безпеки. Огляд і термінологія.

ISO/IEC 27003 Information Security Management Systems. Guidance – Системи менеджменту інформаційної безпеки. Керівництво.

ISO/IEC 27004 Information security management. Measurement – Вимірювання ефективності системи менеджменту інформаційної безпеки.

ISO/IEC 27006 Requirements for bodies providing audit and certification of information security management systems – Вимоги до органів, що здійснюють аудит і сертифікацію систем менеджменту інформаційною безпекою.

ISO/IEC 27007 Guidelines for Information Security Management Systems auditing (FCD) – Керівництво для аудиту СМІБ.

Основним механізмом СМІБ є періодичний аналіз ризиків інформаційної безпеки. Аналіз ризиків може здійснюватися на основі методів CORAS, CRAMM, Magerit, Mehari, Octave та інших. Аналіз ризиків має доповнюватися процедурами аудиту, що сприяє глибшому розумінню бізнес-процесів, які опановані в організації. Аудит може проводитися, наприклад, на основі стандарту CobiT (Control Objectives for Information and related Technology, цілі управління для інформаційних та суміжних технологій).

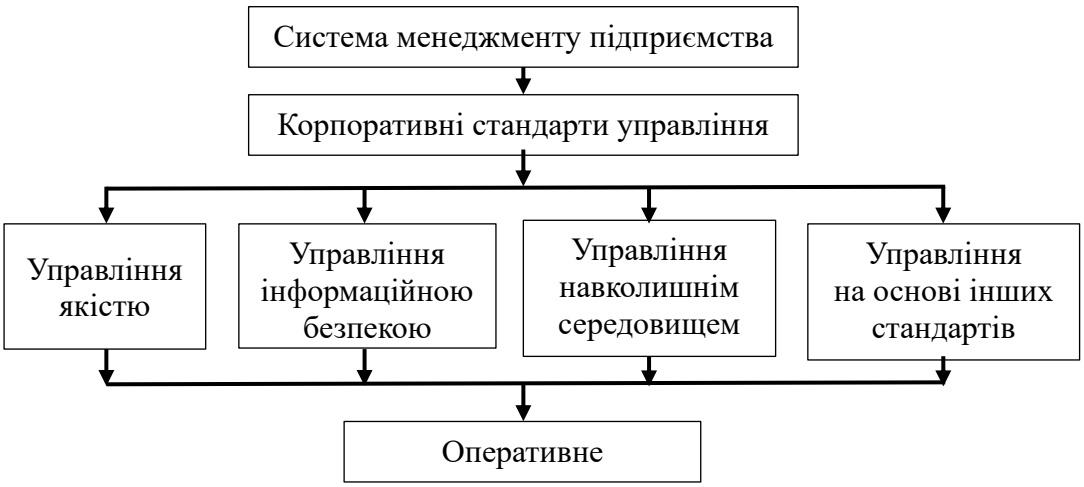

Рисунок 4.5. Місце системи управління інформаційною безпекою в системі менеджменту організації

Верхівка керівництва організації також здійснює процес управління СМІБ прийняттям рішень на основі результатів аналізу ризиків, результатів внутрішнього аудиту й інших механізмів СМІБ. З погляду процесів управління, СМІБ належить до загальної системи менеджменту організації та надає додаткові механізми управління щодо забезпечення захисту критичної інформації (рис. 4.5). Положення управління інформаційною безпекою формують політику безпеки організації – позицію керівництва щодо питань з захисту процесів накопичення, зберігання, передачі та знищення інформаційних цінностей, відповідності й організаційним зобов'язанням.

Питання для самоконтролю:

1. Що визначає міжнародний стандарт ISO/IEC 17799:2005?
2. Організаційні засоби захисту інформації.
3. Що таке принцип компенсації?
4. Які використовують засоби захисту інформації?
5. Що таке механізм ідентифікації?
6. Що таке механізм автентифікації?
7. Які паролі потрібно використовувати?
8. Як відбувається біометрична автентифікація?

ТЕМА 5
КІБЕРЗЛОЧИННІСТЬ

У темі приділено багато уваги питанням характеристики кіберзлочинності, стану кіберзлочинності в Україні та боротьбі з кіберзлочинами.

Ключові слова: *кіберзлочин.*

План

5.1. Характеристика кіберзлочинності.

5.2. Стан кіберзлочинності в Україні.

5.3. Боротьба із кіберзлочинами.

5.1. Характеристика кіберзлочинності

Кіберзлочин – дія, що порушує закон, яку вчинено з використанням інформаційно-комунікаційних технологій (ІКТ) і/або націлена на мережі, системи, дані, вебсайти і/або технології, або сприяє вчиненню злочину. Кіберзлочин відрізняється від традиційного злочину тим, що він «не визнає фізичні або географічні кордони» і може відбуватися з меншими зусиллями, більшою легкістю і з більшою швидкістю, ніж традиційні злочини (хоча це залежить від виду кіберзлочинів і виду традиційного злочину, з яким вони порівнюються).

Коли ІКТ є частиною способу вчинення злочину, кіберзлочинність включає в себе традиційний злочин (наприклад, шахрайство і крадіжку), вчинення якого в той чи інший спосіб сприяють мережа Інтернет та цифрові технології.

Кіберзлочини вчиняються фізичними особами, групами осіб, комерційними організаціями і державами. Хоча ці суб’єкти можуть застосовувати схожі тактичні методи (наприклад, використовувати шкідливе програмне забезпечення) і атакувати схожі цілі (наприклад, комп’ютерну систему), вони мають різні мотиви і наміри під час здійснення кіберзлочинів.

Зловмисники, які здійснювали кіберзлочини, націлювалися на фізичних осіб і вимагали від них невеликі суми грошей, але потім стали націлюватися на комерційні підприємства, компанії та організації і, нарешті, на інших суб’єктів у приватному і державному секторах, що надають важливі послуги (наприклад, лікарні). Атака з використанням вірусу-вимагача у 2020 р. торкнулася приблизно 150 країн, зокрема понад 80 організацій NHS (Національної служби охорони здоров’я) [1]. В одній тільки Англії спричинило за собою скасування майже 20 000 записів на прийом; 600 клінік лікарів загальної практики були змушені повернутися до паперового документообігу, а п’ять лікарень переадресовували карети швидкої допомоги в інші лікарні, оскільки більше не могли надавати термінову медичну допомогу.

Кіберзлочинність є одним з видів транснаціональної злочинності, виконавці і жертви якої можуть перебувати в будь-якій точці світу, де є підключення до мережі Інтернет. Через це слідчим, які ведуть розслідування кіберзлочинів, найчастіше потрібен транскордонний доступ до даних і обмін ними. Це завдання може бути виконано у разі, якщо запитувані дані зберігаються постачальниками послуг і приймаються заходи, що дають змогу правоохоронним органам отримувати доступ до даних.

Основними правовими проблемами під час розслідувань кіберзлочинів і судових переслідувань кіберзлочинців є:

– різні правові системи, чинні в різних країнах;

– відмінності в національних законодавствах про кіберзлочинність;

– відмінності в нормах доказового права і кримінального судочинства (наприклад, у процедурах отримання доступу до цифрових доказів правоохоронними органами; на підставі законного розпорядження, як-от ордер на обшук, або без нього);

– відмінності в охопленні та географічній застосовності регіональних і багатосторонніх договорів про боротьбу з кіберзлочинністю;

– відмінності в підходах до захисту даних і дотримання прав людини.

Кіберзлочинці часто використовують як технічні, так і соціальні підходи до скоєння злочинів. Деяким видам кіберзлочинів важко запобігти, однак користувачі технологій можуть робити певні дії, щоб захистити себе (якоюсь мірою) від кіберзлочинності. Інтерпол [28] розміщує численні керівництва з інформування громадськості та профілактики злочинності на своєму вебсайт. Проте навіть маленькі дії здатні привнести великі зміни.

Поради, які варто враховувати під час підключення до мережі Інтернет.

1. Регулярно оновлюйте операційну систему і встановлене програмне забезпечення.

2. Регулярно видаляйте програмне забезпечення, яке ви більше не використовуєте.

3. Використовуйте антивірусну програму, розроблену компанією з надійною репутацією.

4. Не завантажуйте програмне забезпечення, фільми або музику з сайтів загального доступу – вони часто мають шкідливу програму.

5. Не завантажуйте вкладення і не натискайте на посилання від невпізнаних відправників.

6. Не надавайте особисту інформацію на невідомих вебсайтах.

7. Підтвердіть правильність адресу вебсайта для введення фінансової інформації.

5.2. Стан кіберзлочинності в Україні

Сучасні процеси цифрової трансформації економіки пов'язані з розвитком бізнес-моделей, що використовують цифрові платформи. Фактично протягом останнього десятиріччя відбувається революція платформ. Особливістю цифрових платформ є об'єднання різних груп споживачів, виробників, власників ресурсів на одному віртуальному майданчику. Вітчизняний цифровий капітал перебуває на стадії формування, але вже спостерігається велика кількість позитивних прикладів. Оскільки можливості розвитку цифрової економіки в Україні пов'язані з розширенням використання цифрових платформ, що є точками зростання сучасної інформаційної економіки, перспективним напрямом розвитку цифрових платформ виступає технологія блокчейн (ланцюжок блоків транзакцій) [2].

Організована кіберзлочинність може бути асоційована не тільки з проблемами інформаційної безпеки, але й із загрозами для державної безпеки, військово-промислового і виробничого комплексів, інфраструктури життєзабезпечення. Характеризуючи стан організованої злочинності у сфері економіки, доцільно виділяти її в окрему категорію для вивчення злочинності саме у сфері цифрової економіки. Оцінка впливу цифрової економіки на національну та світову економіку дає змогу констатувати, що актуальним залишається суцільна модернізація злочинності, яка постійно вдосконалюється у межах активної суцільної електронізації та цифровізації суспільства.

Найбільш поширеними напрямами загроз інформаційній безпеці є шахрайські шкідливі платіжні програми, що ускладнюють, порушують або блокують роботу банківських терміналів, використовують для крадіжки даних громадян, злому паролей від банківських карток для заволодіння коштами цих громадян, шахрайства у сфері електронної комерції та застосування інших кримінальних інструментів і послуг у різноманітних сферах злочинної діяльності.

Зростання ділової активності із застосуванням хмарних технологій, придбання товарів через мережу Інтернет, інтернет-банкінгу, онлайн-розрахунки сприяють зростанню економічних злочинів із застосуванням ІТ-технологій.

До ефективних засобів протидії злочинності у сфері інформаційної безпеки пропонується розробка, створення та впровадження сучасних систем захисту інформації, а також вдосконалення наявної законодавчої та нормативно-правової бази, здатної забезпечити протидію сучасним кіберзагрозам. Для підвищення ефективності боротьби з кіберзлочинністю розвинені країни світу ведуть відповідні роботи, необхідні для створення власної стратегії кібербезпеки. Інциденти у сфері кібербезпеки позначаються на життєдіяльності споживачів інформаційних і багатьох інших послуг, кібератаки націлені на різноманітні об'єкти інфраструктури систем електронних комунікацій чи управління технологічними процесами.

Розглядаючи стан кіберзлочинності у світі, необхідно сказати, що відповідно до даних рейтингу GCI-2021 [1], перші сходинки належать таким країнам: Великобританії, США, Франції. Україна станом на 2021 р. займала 54 місце серед 193 країн (табл. 5.1), піднявшись на 5 позицій (59 місце), порівняно з 2020 р.

Позитивні зміни відбулися:

– у побудові законодавчої бази для гарантування кібербезпеки держави;

– стійкість державних ініціатив щодо підвищення кібербезпеки у сфері інформаційно-комунікаційних технологій;

– значне покращення кіберстійкості організацій за останній рік, незважаючи на збільшення більш ніж удвічі цілеспрямованих кібератак.

Таблиця 5.1

Стан кіберзлочинності у світі у 2021 р.

Місце	Країна	Бал
1	Великобританія	0,931
2	США	0,926
3	Франція	0,918
4	Литва	0,908
5	Естонія	0,905
29	Польща	0,815
53	Молдова	0,662
54	**Україна**	**0,661**
56	Кіпр	0,652

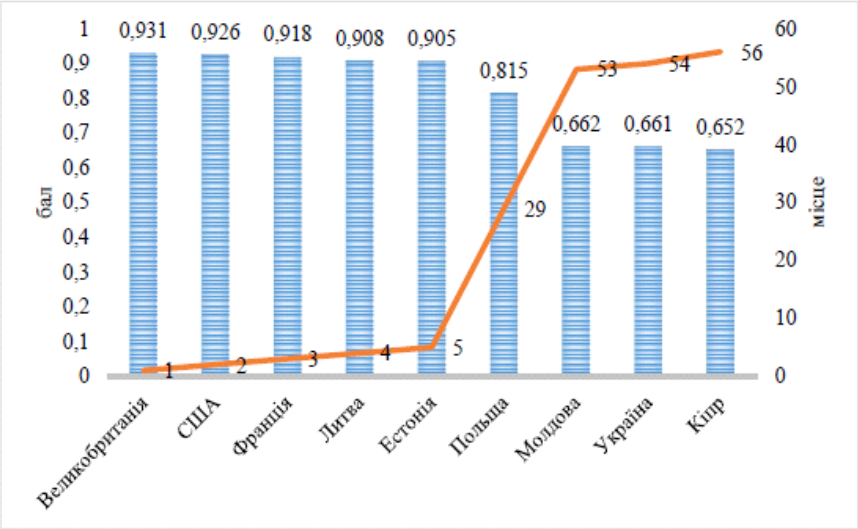

Рисунок 5.1. Стан кіберзлочинності у світі у 2021 р.

Але порівняно з показниками рейтингу GCI-2021 України, Литва посіла 4 позицію, Естонія – 5, Грузія – 18, Казахстан – 40, Латвія – 44, Молдова – 53 (рис. 5.1), тобто система боротьби із кіберзлочинністю у них значно краще побудована, кіберстійкість цих країн є вищою [1].

Рейтинг кіберзлочинності GCI-2021 побудовано на дослідженні основних показників, що відображають стан кібербезпеки в країні. Узагальнений індекс орієнтований на суспільні аспекти національної кібербезпеки, що здійснюються центральним урядом. Мета індексу полягає у вимірі готовності країн до запобігання кіберзагрозам та готовності управляти ними й контролювати кіберіциденти. Показники пов'язані з кібербезпекою і складникам інформаційного суспільства, як-от електронна ідентичність, цифровий підпис та існування безпечного середовища для електронних послуг. Індекс має механізм оцінки та ранжування.

Саме розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки посилює спроможність України у сфері кібербезпеки та відповідає національним інтересам для реалізації поглиблення співпраці з ЄС.

Кількість кіберзлочинів за статтею 361 із 2015 до 2021 р. суттєво зросла. Значний скачок відбувся у 2019 р. Так, у 2019 р. було зафіксовано 1 795 справ, у 2020 р. – 1 023, у 2021 – 1 450, а за прогнозними розрахунками у 2022 р. їх уже може бути 1 754 (рис. 5.2).

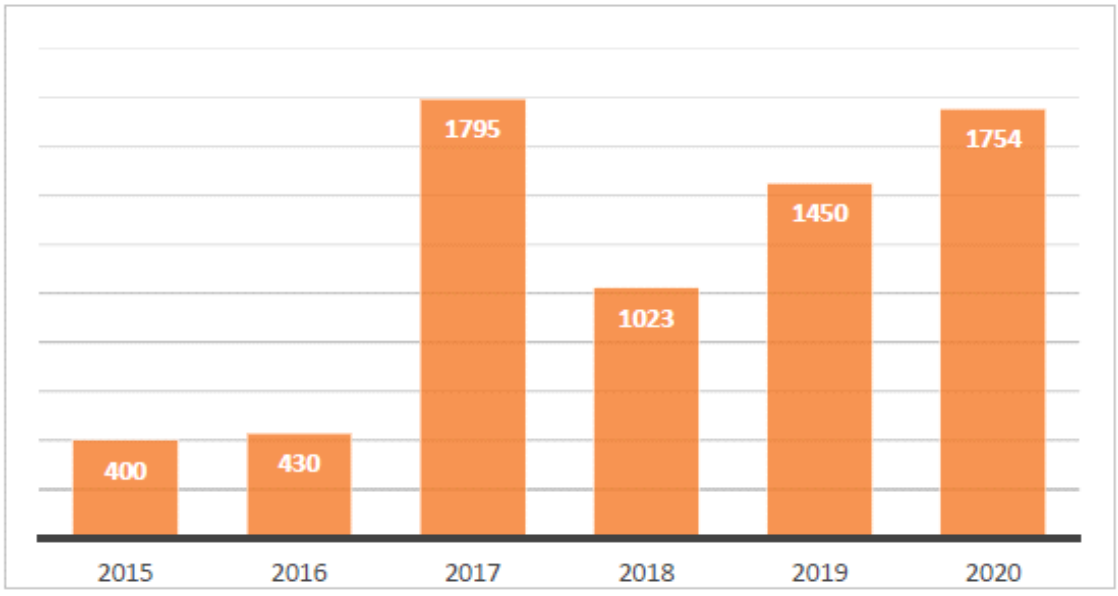

Рисунок 5.2. Кількість кіберзлочинів у 2015–2020 роках

Забезпечення кібербезпеки можливо тільки за рахунок комплексного і безперервного застосування організаційно-правових та технічних методів захисту на різних рівнях реалізації. З метою вироблення спільних підходів у протидії

кіберзагрозам, консолідації зусиль у розслідуванні та запобіганні кіберзлочинам, недопущення використання кіберпростору у протиправних та військових цілях країна має активізувати участь в організації спільних міжнародних проєктів із нарощування кібернетичного потенціалу.

Україна має продовжувати застосовувати європейські і міжнародні стандарти у сфері кібербезпеки, розвивати роботу відповідних органів, що здатні ефективно взаємодіяти з відповідними органами ЄС і НАТО.

Важливо підвищувати рівень обізнаності щодо кібербезпеки на всіх рівнях: від діючих центрів комп'ютерної безпеки до розгортання відповідних освітніх програм. За умов небезпек, що склалися нині у кіберпросторі, організаціям потрібно змінити ставлення до інформаційної безпеки. Для цього треба підвищувати обізнаність про важливість інвестування у кібербезпеку як невід'ємний складник будь-якої національної стратегії розвитку ІКТ.

Спеціалізований структурний підрозділ Державного центру кіберзахисту та протидії кіберзагрозам Державної служби спеціального зв'язку та захисту інформації України CERT-UA функціонує для взаємодії з Cisco Talos Intelligence Group та іншими державами-членами CERT щодо питань подолання наслідків кібератак на інформаційну інфраструктуру, виявлення причин та обставин таких інцидентів. CERT-UA також допомагає усунути загрози безпеці приватного сектору України та іноземних партнерів. Відповідно до закону «Про основні засади забезпечення кібербезпеки України» (2017), CERT-UA та Центр реагування на кіберзлочини координують заходи, спрямовані на оперативне реагування на кібератаки, а також контролюють впровадження контрзаходів, що передбачають мінімізацію вразливості систем зв'язку.

Україна бере участь у роботі Агентства ЄС з кібербезпеки, Європейського центру з досліджень і компетенції в сфері кібербезпеки, а також у навчаннях з реалізації Спільної оперативної схеми реагування ЄС і держав-членів на кібератаки.

Загалом усі заходи, що проводить світова спільнота у сфері кібербезпеки, – це спроба допомогти країнам вдосконалити цю сферу, а також мотивувати їх на вжиття заходів для покращення їх рейтингу, допомагаючи у такий спосіб підвищити загальний рівень кібербезпеки в усьому світі. Рейтинг «Глобального індексу кібербезпеки» допомагає аналізувати та використовувати найкращі засоби боротьби в ІТ-сфері для подолання та упередження кіберзлочинів та покращення стану їх кібербезпеки.

Потреба координації та переорієнтації наукових досліджень і розробок у сфері інформаційної безпеки, вдосконалення інформаційних технологій, використання математичних методів багатовимірного аналізу даних, розробка технологій виявлення ознак кібернетичного нападу з використанням активних і

пасивних методів та датчиків спостереження, створення систем контролю, які визначатимуть факт скоординованого широкомасштабного нападу і формуватимуть ранні попередження про можливу атаку та локалізацію джерел загрози, є актуальною.

Ця проблема потребує ефективного і комплексного вирішення питань на національному, регіональному та міжнародному рівнях для запобігання кіберзлочинам. Лише співпраця між державами для запобігання постійним загрозам в інтернеті і подолання проблем кібербезпеки забезпечить належний рівень захисту від сучасних інформаційних загроз.

З огляду на міжнародний досвід оцінкою вартості інформаційного капіталу може бути ринкова капіталізація цифрових платформ, що поступово впроваджуються в Україні. Актуальним є питання безпеки особистих даних, збір великих масивів даних, дистанційна праця.

Сучасні світові тенденції поширення кіберзлочинності та посилення кібератак свідчать про зростання значення боротьби з нею для подальшого розвитку суспільства, що зі свого боку зумовлює віднесення певних груп суспільних відносин кіберсфери до компетенції правового регулювання. Ситуація, що склалася сьогодні з кіберзлочинністю, вимагає постійного удосконалення методів боротьби з кіберзлочинами, розробки інформаційних систем та методів, спрямованих на забезпечення кібербезпеки країни.

Необхідним завданням є розробка національної стратегії з кібербезпеки, що міститиме тактичні та стратегічні пріоритети і завдання у цій сфері для державних органів. Отже, питання безпеки кіберпростору, боротьби з кіберзлочинністю є актуальним як на міжнародному рівні, так і на рівні окремої країни, а тому потребує подальшого розгляду.

5.3. Боротьба із кіберзлочинами

Від комп'ютерних злочинів страждають усі країни світу. Національна кібербезпека України найбільше стикається з комп'ютерними злочинами в економічній, інформаційній та фінансово-кредитній сферах. Застосування сучасної системи електронного управління повітряним, автомобільним, залізничним, річковим та морським рухом, поширення телекомунікаційної мережі в освіті, науці і практиці, впровадження системи електронних платежів, використання комп'ютерів у діяльності органів законодавчої, виконавчої, судової влади, правоохоронних органів та керуванні військами, розширили сферу діяльності для хакерів, кракерів (хто порушує безпеку системи), кібершахраїв та кібертерористів.

Із розвитком глобальних електронних комп'ютерних мереж набула поширення практика електронного промислового шпигунства. Саме тому проблеми розробки систем захисту та збереження приватної, державної, службової і

комерційної таємниці набувають сьогодні особливого значення. Багато питань виникає через крадіжки різноманітних послуг, зокрема вторгнення до телефонних мереж та незаконну торгівлю послугами зв'язку.

Мережу Інтернет широко використовують торговці піратським програмним забезпеченням, порнографією, зброєю та наркотиками для вчинення власних злочинних дій, обміну інформацією, координації дій тощо. Електронні комп'ютерні мережі можуть стати й об'єктом нападу кібершахраїв та кібертерористів.

Сьогодні особлива увага приділяється саме питанням міжнародного співробітництва у запобіганні, протидії й розслідуванні комп'ютерних злочинів. У багатьох країнах світу для запобігання і протидії цим видам злочинів створені спеціалізовані кіберпідрозділи, що займаються виявленням, розслідуванням комп'ютерних злочинів та збором іншої інформації з цього питання на національному рівні. Саме спеціалізовані національні поліцейські підрозділи утворюють головне ядро сил протидії міжнародній комп'ютерній злочинності. Такі підрозділи вже створені і діють тривалий час у Сполучених Штатах Америки, Канаді, Великобританії, Німеччині, Індії, Китаї, Швеції, Швейцарії, Бельгії, Португалії, Австрії, Польщі, Японії та багатьох інших країнах світу.

Законом «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 р. законодавчо закріплені доктринальні засади забезпечення кібербезпеки нашої країни, а також закладені правові основи діяльності Національного координаційного центру кібербезпеки. Згідно з положеннями цього Закону Національний координаційний центр кібербезпеки є робочим органом Ради національної безпеки і оборони України, який здійснює координацію та контроль за діяльністю суб'єктів сектору безпеки й оборони, які забезпечують кібербезпеку, вносить Президентові України пропозиції щодо формування та уточнення Стратегії кібербезпеки України.

У Законі «Про основні засади забезпечення кібербезпеки України» передбачено створення урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA. Основними її завданнями є:

– накопичення та проведення аналізу даних про кіберінциденти, ведення державного реєстру кіберінцидентів;

– надання власникам об'єктів кіберзахисту практичної допомоги з питань запобігання, виявлення та усунення наслідків кіберінцидентів щодо цих об'єктів;

– організація та проведення практичних семінарів з питань кіберзахисту для суб'єктів національної системи кібербезпеки та власників об'єктів кіберзахисту;

– взаємодія з правоохоронними органами, забезпечення їх своєчасного інформування про кібератаки;

– взаємодія з іноземними та міжнародними організаціями з питань реагування на кіберінциденти, зокрема в рамах участі у Форумі команд реагування на інциденти безпеки FIRST зі сплатою щорічних членських внесків;

– взаємодія з українськими командами реагування на комп'ютерні надзвичайні події, а також іншими підприємствами, установами та організаціями незалежно від форми власності, що провадять діяльність, пов'язану із забезпеченням безпеки кіберпростору;

– опрацювання отриманої від громадян інформації про кіберінциденти щодо об'єктів кіберзахисту;

– сприяння державним органам, органам місцевого самоврядування, військовим формуванням, утвореним відповідно до закону, підприємствам, установам та організаціям незалежно від форми власності, а також громадянам України, у вирішенні питань кіберзахисту та протидії кіберзагрозам.

Забезпечення функціонування діяльності CERT-UA здійснює Державна служба спеціального зв'язку та захисту інформації України. Відповідальність за забезпечення кіберзахисту комунікаційних і технологічних систем об'єктів критичної інфраструктури, захисту технологічної інформації відповідно до вимог чинного законодавства, за невідкладне інформування урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA про інциденти кібербезпеки, за організацію проведення незалежного аудиту інформаційної безпеки на таких об'єктах покладається на власників та/або керівників підприємств, установ та організацій, віднесених до об'єктів критичної інфраструктури.

Варто зазначити, що в багатьох провідних країнах світу вже сформовані і діють загальнодержавні системи кібернетичної безпеки критичної інфраструктури – як найбільш оптимальні організаційні структури, здатні в короткий проміжок часу швидко акумулювати сили та засоби різних державних і правоохоронних органів та установ приватного сектору для протидії кіберзагрозам, кібератакам, кіберзлочинам, кібершпигунству, кібертероризму. У США, Великій Британії, Канаді довгий час діють потужні кіберполіцейські структури (NIPS, FBI, FATF тощо). Сьогодні у Сполучених Штатах Америки, Польщі та інших країнах світу створено кібервійська.

Правову основу забезпечення кібербезпеки України становлять Конституція України, закони України щодо основ національної безпеки, засад внутрішньої і зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена Законом «Про основні засади забезпечення кібербезпеки України» та іншими законами України. Загальна декларація прав людини, Конвенція про кіберзлочинність, інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, укази Президента, акти Кабінету Міністрів України, а також інші

нормативно-правові акти, що приймаються на виконання законів України, фактично закладають міцний міждержавний правовий, організаційний, процедурний фундамент забезпечення кібербезпеки інформаційного простору в Україні, Європі та світі.

Питання для самоконтролю:

1. Що називають кіберзлочином?
2. Які основні правові проблеми розслідування кіберзлочинів?
3. Найбільш поширені напрями загроз інформаційній безпеці.
4. Які закони для протидії кіберзлочинності існують в Україні?

ТЕМА 6
ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ

У темі багато уваги приділено питанням інформаційної безпеки як інтегрованому складнику національної безпеки та доктрині інформаційної безпеки України.

Ключові слова: *інформаційна безпека.*

План

6.1. Інформаційна безпека як інтегрований складник національної безпеки.

6.2. Доктрина інформаційної безпеки України.

6.1. Інформаційна безпека як інтегрований складник національної безпеки

Інформаційна безпека є інтегрованим складником національної безпеки, що розглядають як пріоритетну функцію держави. Інформаційна безпека, з одного боку, передбачає забезпечення якісного всебічного інформування громадян та вільного доступу до різних джерел інформації, а з іншого – це контроль за непоширенням дезінформації, сприяння цілісності суспільства, збереження інформаційного суверенітету, протидія негативним інформаційно-психологічним пропагандистським впливам та захист національного інформаційного простору від маніпуляцій, інформаційних війн та операцій. Вирішення комплексної проблеми інформаційної безпеки дасть змогу як захистити інтереси суспільства й держави, так і гарантувати права громадян на отримання всебічної, об'єктивної та якісної інформації.

Рівень інформаційної безпеки держави значною мірою обумовлений рівнем її інформаційної інфраструктури. На жаль, низький загальний рівень інформаційної інфраструктури України сприяє експансії іноземними компаніями ринку інформаційних послуг, що створює сприятливі умови для перерозподілу ефірного часу на користь іноземних програм, окремі з яких засмічують український інформаційний простір своїм баченням подій, пропагують спосіб життя та традиції, деструктивно впливаючи на суспільство та державу, руйнуючи морально-етичні основи генофонду української нації.

Недостатній професійний, інтелектуальний і творчий рівень вітчизняного виробника інформаційного продукту та послуг, його неконкурентоспроможність не лише на світовому ринку, а й в Україні, призводить до того, що українська аудиторія, природно, віддає перевагу іноземним інформаційним програмам. Недостатній контроль з боку держави за дотриманням законів України політичними силами, ЗМІ та окремими особами, які займаються підприємницькою

діяльністю в інформаційній сфері, призводить до того, що сьогодні трапляються непоодинокі випадки надання ефірного часу теле- та радіопрограмам, спрямованим на руйнування моральних цінностей, свідомості української нації [35].

Отже, національний інформаційний простір України, на жаль, зазнає суттєвих загроз, викликів, що становлять небезпеку функціонування держави, її політичного та економічного розвитку, інтеграції у європейські та євроатлантичні структури. Загрози національній безпеці України в інформаційній сфері – сукупність умов та чинників, що становлять небезпеку життєво важливим інтересам держави, суспільства і особи через можливість негативного інформаційного впливу на свідомість та поведінку громадян, а також на інформаційні ресурси та інформаційно-технічну інфраструктуру [35]. Як зазначено у Законі України «Про основи національної безпеки», однією з основних загроз інформаційній безпеці є «намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації» [37]. У Доктрині інформаційної безпеки України визначено такі загрози інформаційній безпеці країни: поширення у світовому інформаційному просторі викривленої, недостовірної та упередженої інформації, що завдає шкоди національним інтересам України; зовнішні деструктивні інформаційні впливи на суспільну свідомість через ЗМІ, а також мережу Інтернет; деструктивні інформаційні впливи, що спрямовані на підрив конституційного ладу, суверенітету, територіальної цілісності та недоторканності України; прояви сепаратизму в ЗМІ, а також у мережі Інтернет за етнічною, мовною, релігійною та іншими ознаками [44].

З метою протидії негативним впливам інформаційної пропаганди та інформаційних війн, задля нейтралізації та упередження реальних та потенційних загроз в інформаційному просторі України Рада національної безпеки і оборони України ухвалила рішення «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України». У документі зазначено, що РНБО, враховуючи необхідність вдосконалення нормативно-правового забезпечення та запобігання й нейтралізації потенційних і реальних загроз національній безпеці в інформаційній сфері, вирішила: розробити і внести на розгляд Верховної Ради України законопроекти про до деяких законів України щодо протидії інформаційній агресії іноземних держав, передбачивши, зокрема, визначення механізму протидії негативному інформаційно-психологічному впливу, зокрема забороною ретрансляції телевізійних каналів; посилити контроль за дотриманням законодавства з питань інформаційно-психологічної та кібернетичної безпеки; вжити заходів щодо забезпечення поширення у світі об'єктивних відомостей про суспільно-політичну ситуацію в Україні, зокрема, через створення відповідного медіахолдингу для підготовки якісного конкурентоздатного інформаційного продукту; розробити порядок

аналізу інформаційних матеріалів іноземних ЗМІ, що мають представництва в Україні, з метою впровадження дієвого механізму акредитації журналістів; вжити заходів до активізації міжнародного співробітництва з питань протидії негативним інформаційно-психологічним впливам та кібернетичній злочинності [6].

Отже, інформаційна безпека є складним, системним, багаторівневим явищем, на стан якого впливають зовнішні та внутрішні чинники, зокрема політична ситуація у світі; внутрішньополітична ситуація в державі; стан і рівень інформаційно-комунікаційного розвитку країни тощо.

Загрози інформаційній безпеці здебільшого супроводжують виникнення й реалізацію загроз в економічній та політичній сферах, у сфері виконання функцій держави тощо, і заподіяння шкоди в інформаційні сфері є передусім засобом досягнення інших цілей. Інформаційні загрози пов'язані з розпалюванням міжнаціональної, міжконфесійної та іншої ворожнечі, дискредитацією правоохоронної системи й органів державної влади загалом, заподіянням шкоди честі, гідності та ділової репутації фізичних осіб, у тому числі публічних, формуванням «образу ворога», «зомбуванням» населення задля створення умов щодо управління масовою свідомістю.

Водночас потенціал інформаційної сфери через її інтегрувальний характер і здатність «проникнення» до інших сфер життєдіяльності суспільства внаслідок їх інформаційного обслуговування поки що недостатньо усвідомлюється політиками та правоохоронцями (за винятком виявів кіберзлочинності), однак успішно використовується представниками організованих злочинних співтовариств і політичними супротивниками нашої держави.

Рисунок 6.1. Структура обмежень, що погіршують підприємницький клімат

Стратегічне інформаційне протистояння сьогодні становить небезпечний компонент гібридної війни, розгорнутої Росією проти України, причому головною загрозою інформаційній безпеці нашої держави сьогодні залишається загроза впливу ворога на інформаційну інфраструктуру, інформаційні ресурси, на суспільство, свідомість і підсвідомість особистості з метою нав'язати власну систему цінностей, поглядів, інтересів та рішень у життєво важливих сферах суспільної й державної діяльності.

6.2. Доктрина інформаційної безпеки України

Комплексний характер актуальних загроз національній безпеці в інформаційній сфері потребує визначення інноваційних підходів до формування системи захисту та розвитку інформаційного простору в умовах глобалізації та вільного обігу інформації.

Розглянемо особливості Доктрини «Інформаційної безпеки України» від 25 лютого 2017 р. № 47/2017.

Принципи, пріоритети та напрями забезпечення кібербезпеки України визначені Стратегією кібербезпеки України, затвердженою Указом Президента України від 15 березня 2016 р. № 96 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 р. «Про Стратегію кібербезпеки України» [8].

Доктрина інформаційної безпеки України (далі – Доктрина) визначає національні інтереси України в інформаційній сфері, загрози їх реалізації, напрями і пріоритети державної політики в інформаційній сфері.

Правовою основою Доктрини є Конституція України, закони України, Стратегія національної безпеки України, затверджена Указом Президента України від 26 травня 2015 р. № 287 «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 р. "Про Стратегію національної безпеки України"», а також міжнародні договори, згода на обов'язковість яких надана Верховною Радою України.

Метою Доктрини є уточнення засад формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу Російської Федерації в умовах розв'язаної нею гібридної війни.

Доктрина базується на принципах дотримання прав і свобод людини і громадянина, поваги до гідності особи, захисту її законних інтересів, а також законних інтересів суспільства та держави, забезпечення суверенітету і територіальної цілісності України.

Національними інтересами України в інформаційній сфері є:

1) життєво важливі інтереси особи:

– забезпечення конституційних прав і свобод людини на збір, зберігання, використання та поширення інформації;

– забезпечення конституційних прав людини на захист приватного життя;

– захищеність від руйнівних інформаційно-психологічних впливів;

2) життєво важливі інтереси суспільства і держави:

– захист українського суспільства від агресивного впливу деструктивної пропаганди, передусім з боку Російської Федерації;

– захист українського суспільства від агресивного інформаційного впливу Російської Федерації, спрямованого на пропаганду війни, розпалювання національної і релігійної ворожнечі, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України;

– всебічне задоволення потреб громадян, підприємств, установ і організацій усіх форм власності у доступі до достовірної та об'єктивної інформації;

– забезпечення вільного обігу інформації, крім випадків, передбачених законом;

– розвиток і захист національної інформаційної інфраструктури;

– збереження і примноження духовних, культурних і моральних цінностей Українського народу;

– забезпечення всебічного розвитку і функціонування української мови в усіх сферах суспільного життя на всій території України;

– вільний розвиток, використання та захист мов національних меншин та сприяння вивченню мов міжнародного спілкування;

– зміцнення інформаційних зв'язків з українською діаспорою, сприяння збереженню її етнокультурної ідентичності;

– розвиток медіа-культури суспільства та соціально відповідального медіасередовища;

– формування ефективної правової системи захисту особи, суспільства та держави від деструктивних пропагандистських впливів;

– створення з урахуванням норм міжнародного права системи і механізмів захисту від негативних зовнішніх інформаційно-психологічних впливів, передусім пропаганди;

– розвиток інформаційного суспільства, зокрема його технологічної інфраструктури;

– безпечне функціонування і розвиток національного інформаційного простору та його інтеграція у європейський і світовий інформаційний простір;

– розвиток системи стратегічних комунікацій України;

– ефективна взаємодія органів державної влади та інститутів громадянського суспільства під час формування, реалізації державної політики в інформаційній сфері;

– забезпечення розвитку інформаційно-комунікаційних технологій та інформаційних ресурсів України;

– захищеність державної таємниці та іншої інформації, вимоги щодо захисту якої встановлені законом;

– формування позитивного іміджу України у світі, донесення оперативної, достовірної і об'єктивної інформації про події в Україні до міжнародної спільноти;

– розбудова системи іномовлення України та забезпечення наявності іншомовного українського каналу в кабельних мережах та у супутниковому мовленні за межами України.

Актуальними загрозами національним інтересам та національній безпеці України в інформаційній сфері є [8]:

– здійснення спеціальних інформаційних операцій, спрямованих на підрив обороноздатності, деморалізацію особового складу Збройних Сил України та інших військових формувань, провокування екстремістських проявів, підживлення панічних настроїв, загострення і дестабілізацію суспільно-політичної та соціально-економічної ситуації, розпалювання міжетнічних і міжконфесійних конфліктів в Україні;

– проведення державою-агресором спеціальних інформаційних операцій в інших державах з метою створення негативного іміджу України у світі;

– інформаційна експансія держави-агресора та контрольованих нею структур, зокрема шляхом розширення власної інформаційної інфраструктури на території України та в інших державах;

– інформаційне домінування держави-агресора на тимчасово окупованих територіях;

– недостатня розвиненість національної інформаційної інфраструктури, що обмежує можливості України ефективно протидіяти інформаційній агресії та проактивно діяти в інформаційній сфері для реалізації національних інтересів України;

– неефективність державної інформаційної політики, недосконалість законодавства стосовно регулювання суспільних відносин в інформаційній сфері, невизначеність стратегічного наративу (контентного елементу інформаційної та пропагандистської діяльності держави), недостатній рівень медіа-культури суспільства;

– поширення закликів до радикальних дій, пропаганда ізоляціоністських та автономістських концепцій співіснування регіонів в Україні.

Пріоритетами державної політики в інформаційній сфері мають бути [8]:

1) щодо забезпечення інформаційної безпеки:

– створення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них;

– удосконалення повноважень державних регуляторних органів, що здійснюють діяльність щодо інформаційного простору держави, з метою досягнення адекватного рівня спроможності держави відповідати реальним та потенційним загрозам національним інтересам України в інформаційній сфері;

– законодавче врегулювання механізму виявлення, фіксації, блокування та видалення з інформаційного простору держави, зокрема з українського сегмента мережі Інтернет, інформації, що загрожує життю, здоров'ю громадян України, пропагує війну, національну та релігійну ворожнечу, зміну конституційного ладу насильницьким шляхом або порушення територіальної цілісності України, загрожує державному суверенітету, пропагує комуністичний та/або націонал-соціалістичний (нацистський) тоталітарні режими та їхню символіку;

– визначення механізмів регулювання роботи підприємств телекомунікацій, поліграфічних підприємств, видавництв, телерадіоорганізацій, телерадіоцентрів та інших підприємств, установ, організацій, закладів культури та засобів масової інформації, а також використання місцевих радіостанцій, телевізійних центрів та друкарень для військових потреб і проведення роз'яснювальної роботи серед військ та населення; заборони роботи приймально-передавальних радіостанцій особистого та колективного користування і передачі інформації через комп'ютерні мережі в умовах запровадження правового режиму воєнного стану;

– оптимізація законодавчих механізмів реалізації зобов'язань України в межах Європейської конвенції про транскордонне телебачення щодо держав, що не є підписантами зазначеної Конвенції;

– створення і розвиток структур, що відповідають за інформаційно-психологічну безпеку, насамперед у Збройних Силах України, з урахуванням практики держав – членів НАТО;

– розвиток і захист технологічної інфраструктури забезпечення інформаційної безпеки України;

– забезпечення повного покриття території України цифровим мовленням, насамперед у прикордонних районах, а також тимчасово окупованих територій;

– розвиток цифрового мовлення, унеможливлення впливу на його інфраструктуру суб'єктів, що пов'язані з державою-агресором;

– побудова дієвої та ефективної системи стратегічних комунікацій;

– розвиток механізмів взаємодії держави та інститутів громадянського суспільства щодо протидії інформаційній агресії проти України;

– боротьба з дезінформацією та деструктивною пропагандою з боку Російської Федерації;

– посилення спроможностей сектору безпеки і оборони щодо протидії спеціальним інформаційним операціям, спрямованим на зміну конституційного ладу

насильницьким шляхом, порушення суверенітету і територіальної цілісності, підрив обороноздатності України, деморалізацію особового складу Збройних Сил України та інших військових формувань, загострення суспільно-політичної ситуації;

– виявлення та притягнення до відповідальності згідно із законодавством суб'єктів українського інформаційного простору, що створені та/або використовуються державою-агресором для ведення інформаційної війни проти України, та унеможливлення їхньої підривної діяльності;

– унеможливлення вільного обігу інформаційної продукції (друкованої та електронної), насамперед походженням з території держави-агресора, що містить пропаганду війни, національної і релігійної ворожнечі, зміни конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України, провокує масові заворушення;

– проведення розвідувальними органами України акцій сприяння реалізації та захисту національних інтересів України в інформаційній сфері, протидії зовнішнім загрозам інформаційній безпеці держави за межами України;

– недопущення використання інформаційного простору держави в деструктивних цілях або для дій, що спрямовані на дискредитацію України на міжнародному рівні;

2) щодо забезпечення захисту і розвитку інформаційного простору України, а також конституційного права громадян на інформацію:

– стимулювання розвитку національного виробництва текстового і аудіовізуального контенту, зокрема шляхом створення системи квотування та проведення цільових конкурсів на надання грантів;

– забезпечення функціонування Суспільного телебачення і радіомовлення України, у тому числі його належного фінансування;

– створення системи мовлення територіальних громад, що сприятиме розширенню комунікативних можливостей та зниженню конфліктності всередині громад;

– підтримка вітчизняної книговидавничої справи, зокрема перекладів іноземних творів, забезпечення ними навчальних закладів і бібліотек;

– розвиток правових інструментів захисту прав людини і громадянина на вільний доступ до інформації, її поширення, оброблення, зберігання та захист;

– комплексна підтримка розвитку механізмів саморегуляції засобів масової інформації на засадах соціальної відповідальності;

– підвищення медіа-грамотності суспільства, сприяння підготовці професійних кадрів для медіа-сфери з високим рівнем компетентності;

– удосконалення законодавчого регулювання інформаційної сфери відповідно до актуальних загроз національній безпеці;

– задоволення потреб населення тимчасово окупованих територій в об'єктивній, оперативній і достовірній інформації;

– повне покриття території України цифровим та інтернет-мовленням замість аналогового і надання рівних можливостей доступу кожному громадянину до інформаційних ресурсів мережі Інтернет;

– формування системи державної підтримки виробництва вітчизняного аудіовізуального продукту;

– пропагування через аудіовізуальні засоби, зокрема соціальну рекламу, основних етапів і досвіду державотворення, цінностей свободи, демократії, патріотизму, національної єдності, захисту України від зовнішніх і внутрішніх загроз;

3) щодо відкритості та прозорості держави перед громадянами:

– розвиток механізмів електронного урядування;

– сприяння розвитку можливостей доступу та використання публічної інформації у формі відкритих даних;

– інформування громадян України про діяльність органів державної влади, налагодження ефективної співпраці зазначених органів із засобами масової інформації та журналістами;

– проведення реформи урядових комунікацій;

– розвиток сервісів, спрямованих на більш масштабне та ефективне залучення громадськості до прийняття рішень органами державної влади та органами місцевого самоврядування;

– сприяння формуванню культури суспільної дискусії;

4) щодо формування позитивного міжнародного іміджу України:

– ґрунтовне реформування системи представлення інформації про Україну на міжнародній арені;

– розвиток публічної дипломатії, у тому числі культурної та цифрової;

– активізація скоординованої інформаційної роботи закордонних дипломатичних установ України;

– сприяння поширенню та розвитку системи іномовлення України;

– створення та забезпечення функціонування правового механізму взаємодії державних органів з інститутами громадянського суспільства з метою інформаційної підтримки комерційної, гуманітарної, просвітницької, культурної та іншої діяльності таких інститутів за межами України;

– постійний моніторинг пропаганди держави-агресора, розроблення та оперативна реалізація адекватних заходів протидії;

– недопущення використання міжнародного інформаційного простору в деструктивних цілях або для дій, що спрямовані на дискредитацію України на міжнародному рівні;

– реформування системи взаємовідносин з українською діаспорою шляхом забезпечення більш тісної співпраці та проведення ефективних заходів, зокрема в рамках комунікацій «від людини до людини»;

– участь у міжнародних культурних заходах з метою представлення національної культури та ідентичності;

– запровадження міжнародних культурних фестивалів в Україні з метою популяризації української культури та розвитку комунікацій «від людини до людини» [8].

Отже, Доктрина інформаційної безпеки України передбачає постійний моніторинг загроз національним інтересам і національній безпеці в інформаційній сфері.

Контрольні питання:

1. Інформаційна безпека як інтегрований складник національної безпеки.
2. Рівень інформаційної безпеки держави.
3. Загрози національній інформаційній безпеці України.
4. Мета і завдання Доктрини інформаційної безпеки України.
5. Національні інтереси України в інформаційній сфері.
6. Напрями розвитку інформаційного суспільства держави.
7. Особливості розвитку системи стратегічних комунікацій України.
8. Завдання державної інформаційної політики щодо забезпечення інформаційної безпеки.
9. Особливості захисту технологічної інфраструктури забезпечення інформаційної безпеки України.
10. Боротьба з дезінформацією та деструктивною пропагандою інших країн.
11. Забезпечення захисту і розвитку інформаційного простору України.

ТЕМА 7
ПЕРЕДУМОВИ ТА ОСНОВНІ НАПРЯМИ РОЗВИТКУ МЕНЕДЖМЕНТУ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У темі визначаються цілі, завдання, передумови, напрями організаційної та управлінської роботи у сфері інформаційної безпеки. Розглядаються поняття ризик і загроза, представлено їх класифікацію. Наведено основні, найбільш поширені на практиці, способи порушення інформаційної безпеки та сучасні технології захисту інформації. Пояснюється загальна структура курсу, яка включає в себе розгляд основних форм і прийомів організації роботи щодо забезпечення інформаційної безпеки на основних рівнях (рівень міжнародних професіональних організацій; рівень великих постачальників технічних (програмних і апаратних) засобів обробки і передачі інформації; рівень державних органів; рівень окремих підприємств, установ та організацій).

Ключові слова: *безпека, збиток, ймовірність, операційні ризики, захист інформації, об'єкт, активи, загроза інформаційній безпеці.*

План

7.1. Загальні відомості.
7.2. Ризики, їх класифікація.
7.3. Способи порушення інформаційної безпеки.
7.4. Організаційне забезпечення інформаційної безпеки.

7.1. Загальні відомості

Поняття «інформаційна безпека» з'явилось завдяки розвитку засобів інформаційних комунікацій серед суспільства. У сучасному світі стрімкий розвиток інформаційних технологій не є новиною. Збільшується кількість інформаційних систем, програмних забезпечень, які допомагають персоналу підприємства управляти інформаційними потоками. Відповідно до цього збільшується кількість цінної інформації. Тому питання про її захист стоїть досить гостро. Необхідно зазначити, що в науковій літературі відсутній єдиний погляд на зміст поняття «інформаційна безпека».

Під поняттям «інформаційна безпека» розуміють стан (рівень) захищеності інформаційних ресурсів – інформаційних об'єктів та інформаційних систем – від негативних впливів (як випадкових, так і здійснюваних навмисно), які можуть завдати шкоди самій інформації та засобам її передачі та обробки, а також негативно відбитися на власниках інформаційних ресурсів, державі, суспільстві та інших учасниках процесів інформаційного обміну. Більшість сучасних інформаційних ресурсів та інформаційних систем практично не можуть розглядатися

у відриві від комплексу елементів (факторів), пов'язаних із забезпеченням інформаційної безпеки: загроз для інформаційних ресурсів, різних засобів і заходів захисту, бар'єрів для проникнення, а також вразливостей у системах захисту інформації. Отже, під інформаційною безпекою в більш загальному вигляді можна визначити як сукупність засобів, методів і процесів (процедур), які забезпечують захист інформаційних активів і гарантують збереження ефективності та практичної корисності як технічної інфраструктури інформаційних систем, так і відомостей, які в таких системах зберігаються та обробляються. Мета інформаційної безпеки полягає в тому, щоб зберегти цілісність, повноту і точність інформації, зменшити ризик несанкціонованих змін в інформаційних системах. Для того, щоб забезпечити підприємству розвиток та конкурентоспроможність, необхідно створити систему управління інформаційною безпекою.

Система управління інформаційною безпекою СУІБ (information security management system, ISMS) – частина загальної системи управління, яка призначена для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення інформаційної безпеки.

Для процесів СУІБ застосована модель PDCA (плануй – виконуй – перевіряй – дій; Plan – Do – Check – Act, PDCA):

– *Plan (планування)* – фаза створення СУІБ, створення переліку активів, оцінки ризиків та вибору заходів;

– *Do (дія)* – етап реалізації та впровадження відповідних заходів;

– *Check (перевірка)* – фаза оцінки ефективності та продуктивності СУІБ. Зазвичай виконується внутрішніми аудиторами;

– *Act (поліпшення)* – виконання превентивних і коригуючих дій.

Побудова СУІБ дає змогу чітко визначити, як взаємопов'язані процеси та підсистеми ІБ, хто за них відповідає, які фінансові та трудові ресурси необхідні для їх ефективного функціонування та ін.

Основні функції системи управління інформаційною безпекою:

– виявлення та аналіз ризиків інформаційної безпеки;

– планування та практична реалізація процесів, спрямованих на мінімізацію ризиків ІБ;

– контроль цих процесів;

– внесення в процеси мінімізації інформаційних ризиків необхідних коригувань.

Якісне управління інформаційною безпекою базується на таких принципах:

– комплексний підхід – управління ІБ має бути всеосяжним, охоплювати всі компоненти ІС і враховувати всі актуальні ризикоутворюючі фактори, що діють в інформаційній системі підприємства та за її межами;

– узгодженість з бізнес-задачами та стратегією підприємства;

– високий рівень керованості;

– адекватність інформації, яка використовується та генерується;

– ефективність – оптимальний баланс між можливостями, продуктивністю та витратами СУІБ;

– безперервність управління;

– процесний підхід – зв'язування процесів управління в замкнутий цикл планування, впровадження, перевірки, аудиту та коригування, підтримка нерозривного зв'язку між етапами.

Відповідно до ISMS Framework (https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-isms/framework), що є Європейським аналогом СУІБ, який розроблено міжнародною європейською агенцією з кібербезпеки, управління безпекою відбувається за схемою, відображеною на рис. 7.1.

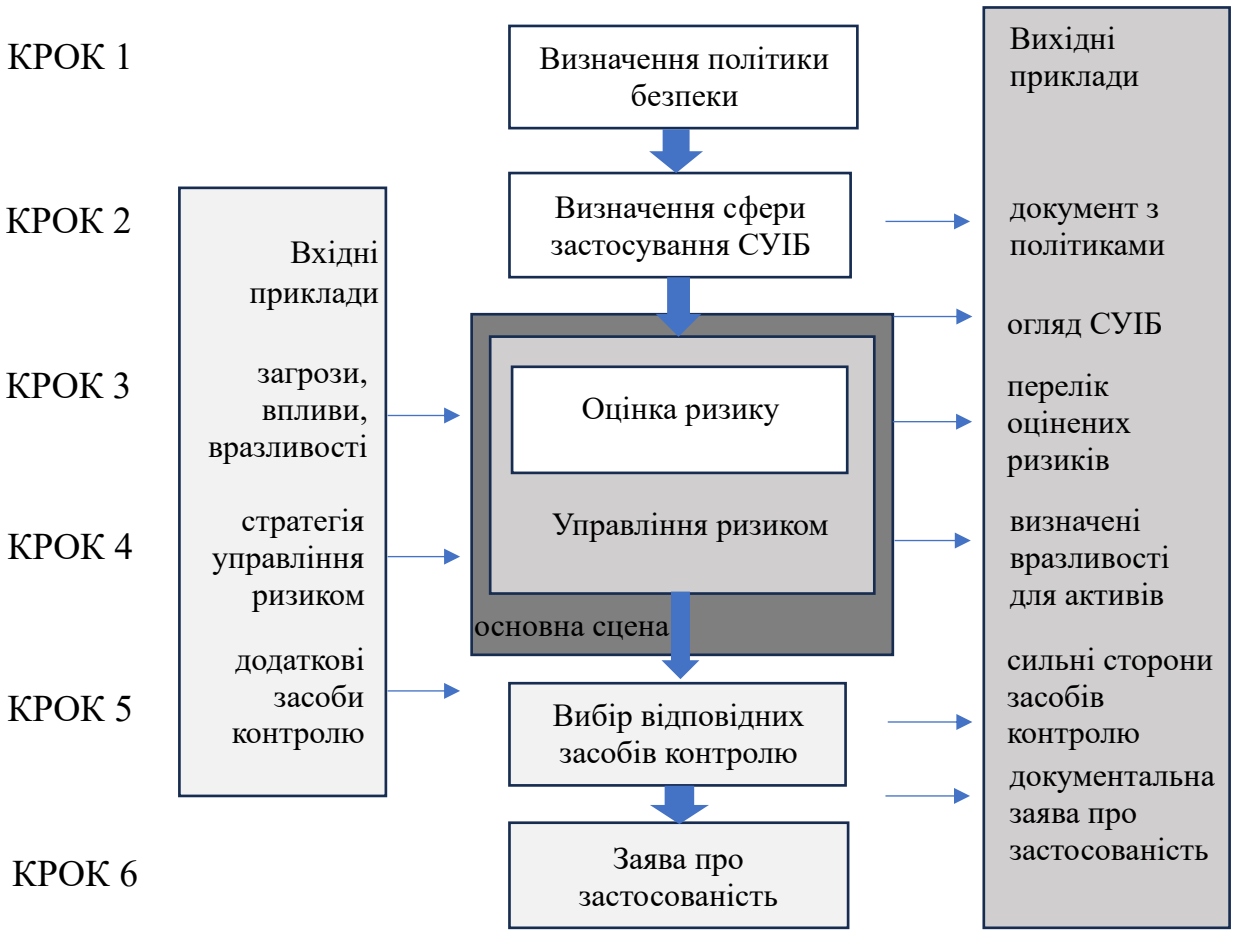

Рисунок 7.1. СУІБ відповідно до фреймворку ISMS від ENISA

І розмір компанії, й конкретна діяльність організації диктує вимоги, пов'язані з безпекою, на правовому, регуляторному та операційному рівнях.

Малі підприємства з обмеженою інфраструктурою інформаційних систем, діяльність яких не вимагає обробки, зберігання та обробки персональних або конфіденційних даних, зазвичай стикаються з незначними ризиками або ризиками з меншою ймовірністю чи наслідком. Ці організації, ймовірніше, не підтримують незалежну СУІБ та зазвичай займаються ризиками інформаційної безпеки спеціально або як частина більш широкого процесу управління ризиками.

Більші організації та організації, як-от банки та фінансові інститути, оператори телекомунікацій, лікарні та інститути охорони здоров'я, державні чи державні органи, мають багато причин для того, щоб дуже серйозно вирішувати питання захисту інформації. Законодавчі та нормативні вимоги, спрямовані на захист конфіденційних або особистих даних, а також загальні вимоги громадської безпеки спонукають їх приділяти найбільшу увагу та пріоритет ризикам інформаційної безпеки. За цих обставин розробка та впровадження окремого та незалежного процесу управління, а саме Системи управління інформаційною безпекою, є єдиною альтернативою.

Як показано на рисунку вище, розробка системи СУІБ передбачає такі шість кроків:

– визначення політики безпеки;
– визначення сфери застосування СУІБ;
– оцінка ризику (як частина управління ризиками);
– управління ризиками;
– вибір відповідних засобів контролю;
– заява про застосовність.

Етапи 3 та 4, процес оцінки та управління ризиками, складають суть СУІБ і є процесами, які, з одного боку, «перетворюють» правила та керівні принципи політики безпеки та цілей; а з іншого – перетворюють цілі СУІБ у конкретні плани реалізації засобів контролю та механізмів, спрямованих на мінімізацію загроз та вразливостей. Варто зазначити, що кроки 3 та 4 розглядаються як єдине ціле, а саме – управління ризиками.

Процеси та дії, пов'язані з кроками 5 та 6, не стосуються інформаційних ризиків. Вони пов'язані з оперативними діями, необхідними для технічного впровадження, обслуговування та контролю вимірювань безпеки.

Відповідні засоби контролю можуть бути отримані або з наявних (вичерпних) наборів засобів контролю або механізмів, зазвичай включених до стандартів захисту інформації (наприклад, [ISO 17799]) та керівних принципів, або бути результатом поєднання або адаптації запропонованих засобів контролю до конкретних організаційних вимог або експлуатаційні характеристики.

В обох випадках кроком 6 є документоване відображення виявлених ризиків, застосованих до конкретної організації з технічним впровадженням механізмів безпеки, які організація вирішила застосувати.

Варто зазначити, що хоча СУІБ – це повторюваний процес у цілому, у більшості типів організацій, згаданих вище, кроки 1 та 2 повторюються у більш тривалому циклі, ніж кроки 3, 4, 5 та 6. Так відбувається в основному тому, що встановлення політики безпеки та визначення сфери застосування СУІБ частіше є управлінськими та (до певної міри) стратегічними проблемами, тоді як процес управління ризиками є «повсякденною» оперативною проблемою.

Один із ключових чинників успішності системи управління інформаційною безпекою підприємства – це побудова її на базі міжнародних стандартів ISO/IEC 27001.

Міжнародний стандарт ISO 27001 надає інструмент для розробки, впровадження, супроводу, моніторингу, підтримки та вдосконалення добре документованої системи управління інформаційною безпекою в контексті розгляду бізнес-ризиків.

СУІБ забезпечує вибір адекватних та пропорційних методів і засобів контролю та захисту інформації, а отже, – довіру зацікавлених сторін. Проте треба брати до уваги й інші стандарти в сфері інформаційної безпеки. Сьогодні у світовій практиці використовується велика кількість стандартів, методик та інших документів, що регламентують процеси управління інформаційною безпекою, наприклад, ISM3, COBIT, ITIL/ITSM, BSI-100-2, ISO 13335-4, CRAMM, ISO 15408. Але варто зазначити, що всі вони сумісні з ISO 27001, а також подібні до нього.

Поняття інформаційної безпеки нерозривно пов’язане з **ризиками** для інформаційних ресурсів, під якими (ризиками) розуміється можливість (ймовірність) нанесення шкоди інформаційним ресурсам, зниження рівня їх захищеності.

7.2. Ризики, їх класифікація

Ризики можуть мати різну природу і характеристики; однією з основних класифікацій ризиків для інформаційної безпеки (так само, як і багатьох інших ризиків в економіці та управлінні) є їх поділ на:

– системні ризики – некеровані ризики, пов’язані з тим середовищем і технічною інфраструктурою, в якій функціонують інформаційні системи;

– операційні ризики – зазвичай керовані ризики, пов’язані з особливостями використання певних інформаційних систем, їх технічної реалізації, застосовуваними алгоритмами, апаратними засобами тощо.

Усі негативні впливи на інформаційні активи, захист від яких передбачає інформаційна безпека, можуть бути розділені на три основні види:

– порушення конфіденційності інформації;

– руйнування (втрата, необоротна зміна) інформації;

– недоступність інформаційних ресурсів – виникнення ситуацій, коли користувачі (всі або їх частина) на деякий період часу втрачають можливість доступу до необхідних даних (або інформаційних систем).

Безпосереднім джерелом ризиків і негативних впливів є загрози, під якими розуміються потенційні або реально можливі дії відносно інформаційних ресурсів, що порушують інформаційну безпеку. Виділяють безліч типів загроз і безліч критеріїв для класифікації загроз інформаційній безпеці.

Одним з **основних** таких **критеріїв є розташування джерела порушень** до інформаційних ресурсів, щодо яких здійснюється негативний вплив. Відповідно до цього критерію порушення можуть бути поділені так:

– обумовлені внутрішніми факторами (персоналом підприємства, роботою власних інформаційних систем);

– обумовлені зовнішніми факторами (зловмисниками, які не мають безпосереднього відношення до компанії – власника інформаційних активів, природними факторами тощо).

Іншим **важливим критерієм є наявність намірів здійснити порушення.** Відповідно до нього виділяють:

– цілеспрямовані дії (можуть бути здійснені як власним персоналом, так і зовнішніми противниками);

– випадковий вплив (помилки користувачів та адміністраторів, збої і випадкові порушення в роботі обладнання, непередбачений вплив природних факторів).

Також можна виділити такі **класифікації загроз:**

– за об’єктом (персонал, матеріальні та фінансові кошти, інформація);

– за величиною збитку (граничний, значний, незначний);

– за ймовірністю виникнення (дуже ймовірні, ймовірні, малоймовірні);

– за типом збитку (моральний, матеріальний);

– деякі інші.

7.3. Способи порушення інформаційної безпеки

На практиці основними, найбільш поширеними, способами порушення інформаційної безпеки є:

– отримання несанкціонованого доступу (зокрема і шляхом перевищення прав під час санкціонованої роботи з інформаційними системами) до певних відомостей або масивів даних, поширення яких обмежене, з метою їх вивчення, копіювання, поширення, незаконного використання тощо;

– несанкціоноване використання інформаційних ресурсів (ресурсів обчислювальних і телекомунікаційних систем) з метою отримання вигоди або нанесення збитку (як системам, які незаконно використовуються, так і третім особам);

– несанкціонована зловмисна модифікація (зміна) даних;

– крадіжка грошових коштів в електронних платіжних системах і системах «клієнт-банк»;

– виведення з ладу (повне або часткове) програмних і апаратних засобів обробки, передачі та зберігання інформації;

– здійснення атак типу «відмова в обслуговуванні» – DoS (зокрема щодо серверів в мережі Інтернет);

– поширення вірусів та інших шкідливих програм, що здійснюють різні негативні впливи.

Сучасна практика використання інформаційних систем характеризується великою кількістю нагромадження порушень інформаційної безпеки. Одним з важливих чинників цього є все більша доступність сучасних інформаційних технологій для злочинців, а також привабливість інформаційних систем як потенційних об'єктів нападу. Також важливою обставиною є постійне ускладнення і зростання різноманітності інформаційних систем, що використовуються, і зокрема програмних продуктів. З урахуванням того, що в середньому кожна тисяча рядків програмного коду може містити від 5 до 15 помилок, поява різних вразливостей, що створюють загрози для інформаційної безпеки, стає практично неминучою. Результатом цього є постійне зростання кількості різних порушень, пов'язаних з інформаційною безпекою.

Отже, всі перераховані обставини: зростання різноманіття можливих порушень, збільшення їх кількості, збільшення складності інформаційних технологій, усе більша доступність комп'ютерів і телекомунікаційних засобів для злочинців – пояснюють зростання потреби власників інформаційних ресурсів (підприємств, організацій, державних відомств) у реалізації систематичних, всеосяжних заходів щодо забезпечення інформаційної безпеки.

Окремі процеси, процедури, механізми та інструменти захисту інформації, використовувані власниками інформаційних ресурсів та інформаційних систем, можуть бути спрямовані на таке:

– обмеження і розмежування доступу;

– інформаційне приховування;

– введення надлишкової інформації і використання надлишкових інформаційних систем (засобів зберігання, обробки і передачі інформації);

– використання методів надійного зберігання, перетворення і передачі інформації;

– нормативно-адміністративне спонукання і примус.

На практиці сучасні технології захисту інформації побудовані на різних базових сервісах (автентифікація, забезпечення цілісності, контроль доступу та ін.), і використовують різні механізми забезпечення безпеки (шифрування, цифрові підписи, управління маршрутизацією тощо). Однак комплексність і масовість використання інформаційних технологій, їх інтеграція в повсякденну діяльність підприємств, організацій, урядових установ не дають можливості вирішувати завдання інформаційної безпеки тільки одними технічними засобами.

7.4. Організаційне забезпечення інформаційної безпеки

У всьому комплексі діяльності із захисту інформації одне з найбільш важливих місць займає організаційно-управлінська діяльність – організаційне забезпечення інформаційної безпеки, яке являє собою один з чотирьох основних напрямів роботи в загальній системі заходів у сфері інформаційної безпеки, що включає в себе також розробку спеціалізованого програмного забезпечення, виготовлення і використання спеціальних апаратних засобів та вдосконалення криптографічних (математичних) методів захисту інформації (рис. 7.2).

Основними завданнями організаційно-управлінської діяльності (менеджменту) у сфері інформаційної безпеки є:

– забезпечення комплексності всіх рішень, реалізованих у процесі забезпечення інформаційної безпеки;

– забезпечення безперервності і цілісності процесів інформаційної безпеки;

– вирішення методичних завдань, що лежать в основі ефективного управління інформаційною безпекою, як-от питання управління ризиками, економічне моделювання тощо;

– управління людськими ресурсами та поведінкою персоналу з урахуванням необхідності вирішення завдань інформаційної безпеки.

Рисунок 7.2. Структура діяльності у сфері інформаційної безпеки

Під комплексністю вирішення завдань інформаційної безпеки маються на увазі взаємопов’язані виявлення всіх значущих інформаційних об’єктів, а також

наявних і потенційно можливих загроз. На основі цього аналізу необхідно забезпечити вичерпне, повне (комплексне) впровадження і застосування засобів захисту інформації, які могли б нейтралізувати всі істотні загрози на всіх потенційно вразливих ділянках проходження інформаційних потоків протягом всіх етапів життєвого циклу інформаційних систем та організаційних процедур. Заходи щодо нейтралізації ризиків також повинні бути реалізовані в комплексі з іншими механізмами, наприклад, страхування. Інакше кажучи, завданням менеджменту є системне використання всіх необхідних (вузькоспеціальних) технологій і рішень для кожної конкретної ситуації, щоб у всій системі заходів із захисту інформаційних ресурсів не залишилося «вузьких місць» – уразливих ділянок, через які можуть бути здійснені напади і в яких можуть відбутися ненавмисні порушення. Складність таких завдань пов'язана з тим, що вони припускають за можливості вичерпний аналіз як усіх інформаційних ресурсів, так і всіх можливих сценаріїв нападу на них та подальший підбір найбільш придатних засобів захисту.

Неперервність процесів забезпечення інформаційної безпеки передбачає виділення необхідних ресурсів та організацію виконання необхідних функцій із захисту інформації протягом усього часу функціонування інформаційних систем і виконання бізнес-функцій.

Розробка, вдосконалення та підтримка в актуальному стані методичних основ управління інформаційною безпекою включає в себе застосування загальних для багатьох сфер менеджменту концепцій і теорій – наприклад, математичні моделі оцінки ризиків або теорія інвестиційного аналізу – стосовно ресурсів, що використовуються для забезпечення інформаційної безпеки та інформаційних процесів.

Управління людськими ресурсами в межах управління інформаційною безпекою включає в себе комплекс завдань, що охоплює всі основні аспекти діяльності людей: відбір і допуск персоналу до роботи з певними інформаційними ресурсами, навчання, контроль правильності виконання обов'язків, створення необхідних умов для роботи тощо.

Водночас конкретна структура і склад усіх основних завдань управління та організації у сфері інформаційної безпеки, а також методи, що безпосередньо використовуються, будуть визначатися як рівнем, на якому здійснюється управлінська та організаційна діяльності, так і конкретними умовами, в яких функціонують інформаційні системи, які потребують захисту. Курс заснований на концепції поділу усього різноманіття методів і завдань організації та управління у сфері інформаційної безпеки на кілька основних рівнів і подальшому поданні організаційно-управлінських методів для кожного з цих рівнів.

Під організаційним забезпеченням та менеджментом у сфері інформаційної безпеки зазвичай прийнято розуміти вирішення управлінських питань на рівні окремих суб'єктів (підприємств, організацій) або груп таких суб'єктів (партнерів по бізнесу, організацій, що спільно вирішують певні завдання і потребують захисту інформації).

Однак складність і комплексність сучасних проблем у сфері інформаційної безпеки, глобалізація інформаційних взаємодій вимагають більш повного і широкого розуміння організаційної роботи та менеджменту в цій галузі.

Зокрема, в час глобалізації інформаційних взаємодій, ускладнення програмних і апаратних засобів обробки інформації, проникнення інформаційних технологій у повсякденну діяльність усіх організацій і життя більшості людей з'явилася необхідність у спеціальних організаційних і управлінських зусиллях, спрямованих не скільки на забезпечення захищеності окремих інформаційних активів, як на підтримку різних елементів інформаційної інфраструктури, яка тією чи іншою мірою працює на забезпечення інформаційної безпеки певних спільнот (заздалегідь не визначеної множини користувачів інформаційних систем і власників інформаційних ресурсів).

Отже, з розвитком інформаційних технологій, інтенсифікацією інформаційного обміну організаційна та управлінська робота у сфері інформаційної безпеки виявляється спрямованою не тільки на власне захист певних інформаційних ресурсів, але і на більш «глобальний» об'єкт – створення і розвиток безпечної інформаційної інфраструктури (у різних значеннях цього терміна та з урахуванням різних його аспектів). На практиці така інфраструктура може включати в себе:

– надійну інфраструктуру передачі інформації і ринок послуг доступу до таких каналів зв'язку;

– ринок програмних і апаратних засобів, що забезпечують захист інформації;

– систему підготовки, перепідготовки та підвищення кваліфікації фахівців у сфері інформаційної безпеки;

– загальні правила використання інформації, а також її передачі, спільної експлуатації інформаційних мереж (зокрема протоколи інформаційного обміну);

– систему обміну інформацією та поширення знань про наявні вразливості тих чи інших інформаційних технологій, про можливі загрози інформаційній безпеці та способи їх нейтралізації;

– законодавчу і правочинну систему, що забезпечує охорону майнових та інших інтересів усіх учасників інформаційного обміну;

– інші складники.

Потреба в цілеспрямованому розвитку та підтримці такої інфраструктури породжує необхідність у виробленні специфічних організаційних і управлінських прийомів, здебільшого не характерних для інформаційної безпеки у звичному («вузькому») її розумінні.

Таке розширення сфери інтересів менеджменту інформаційної безпеки пояснює причини, за якими необхідно розділяти кілька відносно самостійних організаційних рівнів, що характеризуються специфічними завданнями, підходами до вирішення цих завдань і організаційними методами, які застосовуються:

– Рівень міжнародних професійних об'єднань (зазвичай неурядових і некомерційних), так чи інакше пов'язаних зі сферою інформаційних технологій, телекомунікацій та інформаційної безпеки.

– Рівень великих компаній, що працюють у сфері інформаційних технологій і значною мірою визначають (прямо чи опосередковано) стан інформаційної безпеки в співтоваристві користувачів інформаційних систем, а також впливають на безпеку різних елементів інформаційної інфраструктури.

– Державний рівень – рівень державних і міжурядових організацій, які так чи інакше впливають на життя суспільства, стан правової системи, розвиток економіки і технологій.

– Рівень окремих компаній (підприємств та організацій) – спільнота користувачів інформаційних систем, які так чи інакше зацікавлені у власній інформаційній безпеці та забезпечують захист наявних у них інформаційних ресурсів власними силами.

Також окремо можна виділити додатковий проміжний рівень, до складу якого входять консалтингові та впроваджувальні компанії, навчальні центри (включно зі спільнотою фахівців, що займаються консультаціями, впровадженням і навчанням в індивідуальному порядку), що працюють у сфері інформаційної безпеки та діють як сполучна ланка між різними організаційними рівнями, а також представляють інтереси різних учасників інформаційної взаємодії. Всі ці складники утворюють своєрідну організаційну ієрархію, представлену на рис. 7.3.

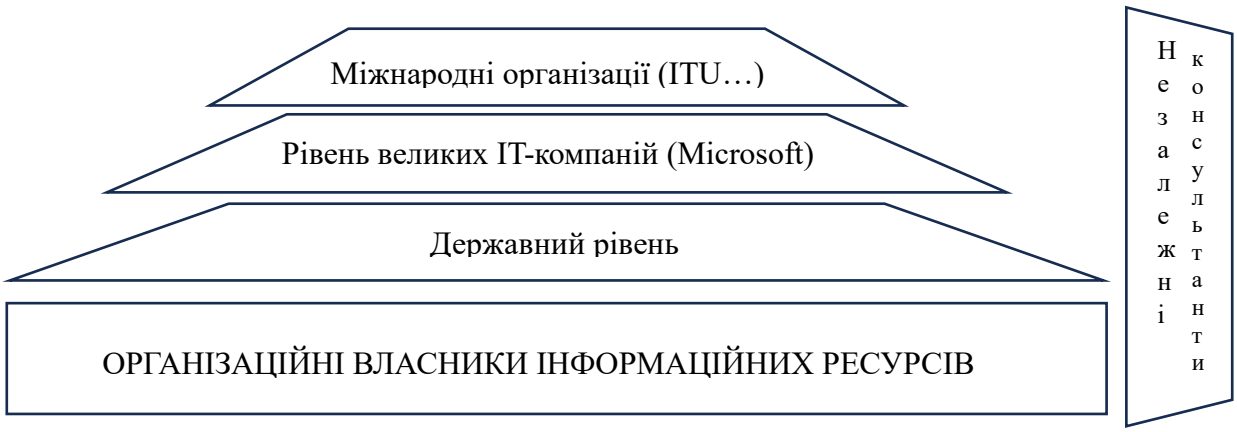

Рисунок 7.3. Ієрархія рівнів організаційної роботи у сфері інформаційної безпеки

Варто розуміти, що суб'єкти, що перебувають на верхніх щаблях цієї ієрархії (зокрема державні органи, великі IT-корпорації), виступають не тільки як володільці власних інформаційних ресурсів, що вимагають захисту, але і як суб'єкти, які впливають на інфраструктуру, що лежить в основі обміну та збереження інформації, а також на суспільно-економічні відносини, що впливають на інформаційну безпеку. Факт, що такі суб'єкти самі приділяють значну увагу захисту власних ресурсів (вкладають істотні кошти в забезпечення інформаційної безпеки, ініціюють нові розробки для власних потреб, використовують найбільш передові технології в цій сфері тощо), не повинен відволікати увагу від тієї обставини, що ці суб'єкти фактично створюють інфраструктуру для повсякденної діяльності безлічі компаній, організацій, людей, професійних і бізнес-співтовариств і використовують для цього організаційні методи та прийоми, які суттєво відрізняються за своєю природою від методів, характерних для роботи із забезпечення інформаційної безпеки окремих суб'єктів і захисту окремих інформаційних активів.

Отже, необхідність самостійного розгляду суб'єктів, які належать до верхнього рівня, з погляду організаційного забезпечення інформаційної безпеки обумовлена тим, що своєю особливою («інфраструктурною») роллю у системі суспільних відносин та інформаційного обміну ці суб'єкти використовують специфічні методи організаційно-управлінської роботи. Водночас здебільшого паралельно із застосуванням таких специфічних методів вони використовують методи, характерні для суб'єктів нижнього рівня представленої ієрархії, які є володільцями власних інформаційних ресурсів.

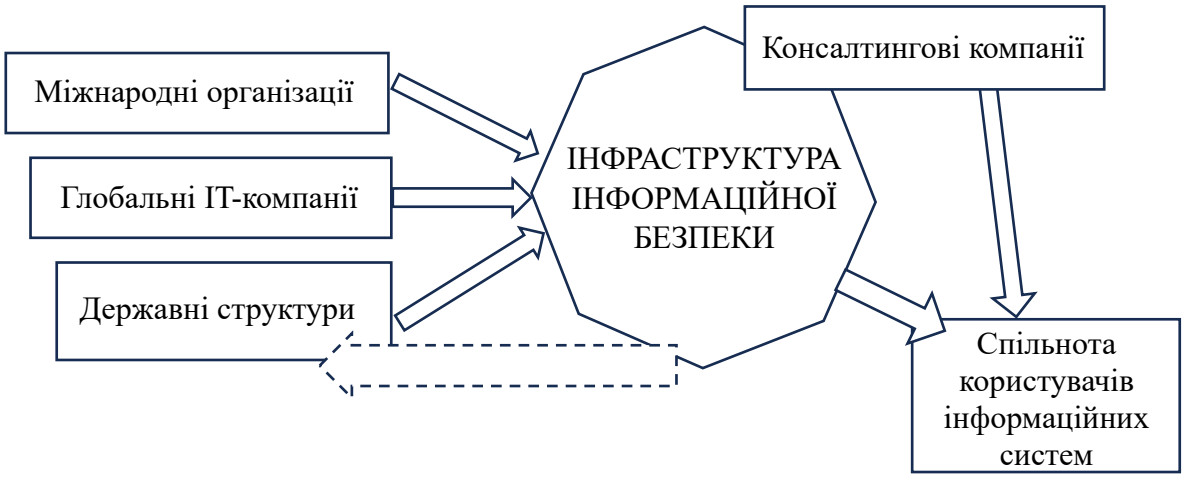

Рисунок 7.4. Взаємозв'язки рівнів організації інформаційної безпеки

Представлений поділ на рівні повинен бути основою для більш цілеспрямованого розвитку системи менеджменту та налагодження взаємозв'язків між різними рівнями організаційної роботи (див. рис. 7.4). Важливість виділення і

самостійного розгляду верхніх рівнів управлінської роботи обумовлена тим, що цілеспрямоване усвідомлення організаційних питань, специфічних для верхніх рівнів ієрархії та їх вирішення дає змогу більш ефективно вирішувати завдання розвитку національних та регіональних економік загалом та окремих галузей (телекомунікації, фінансові послуги тощо), а не тільки вирішувати завдання окремих суб'єктів, що беруть участь в інформаційному обміні.

Основні особливості організаційної роботи на кожному з перерахованих рівнів організації представлені в табл. 7.1. Табл. 7.1, а також рис. 7.3 наочно демонструють причини, за якими кожен з рівнів організаційної роботи у сфері інформаційної безпеки потребує індивідуального підходу й застосування специфічних методів організації та управління.

Таблиця 7.1

Завдання, ролі і методи, що використовуються на різних рівнях організаційної роботи у сфері інформаційної безпеки

Організаційний рівень	Основні завдання і ролі	Основні специфічні методи організаційної роботи
1. Міжнародні організації	Розробка правил і стандартів (зокрема і мережевих протоколів), що мають глобальне значення. Обмін актуальною інформацією і попередження про нові загрози	Координація роботи фахівців, експертів та дослідників, що представляють різні зацікавлені сторони
2. Глобальні IT-компанії	Методологічна та організаційна підтримка використання продуктів і послуг, що поставляються на ринок	Гнучка взаємодія з клієнтами (користувачами продуктів і послуг) з метою підвищення використання інформаційних систем і отримання відгуків для подальшого підвищення якості наданих продуктів і послуг
3. Державні організації	Регулювання використання інформаційних систем і поширення інформації з метою недопущення протиправних дій, збитку іншим учасникам інформаційного обміну, суспільству та державним органам	Розробка національних і міжнародних правил (законів, конвенцій, угод тощо), що регулюють відносини в інформаційній сфері. Здійснення контролю (в різних формах). Здійснення правочинної та правоохоронної діяльності
4. Користувачі інформаційних систем – власники інформації	Захист власних інформаційних ресурсів	Виділення підрозділів та фахівців, що відповідають за ІБ. Розробка і застосування внутрішніх політик і правил безпеки
5. Консалтингові та впроваджувальні компанії, що працюють у сфері ІБ	Виконання деяких функцій ІБ на умовах аутсорсингу. Розробка та впровадження індивідуальних рішень у сфері ІБ більш ефективно, ніж це змогли б зробити самі власники інформаційних ресурсів	Накопичення та узагальнення теоретичних знань і практичних навичок з метою створення та впровадження організаційних і технічних рішень в інтересах клієнтів

Відповідно до цього поділу і будується структура даного курсу – вона включає в себе розгляд основних форм і прийомів організації роботи щодо забезпечення інформаційної безпеки на основних організаційних рівнях:

– на рівні міжнародних професіональних організацій та бізнес-спільнот;

– на рівні великих постачальників технічних (програмних і апаратних) засобів обробки і передачі інформації, що мають вплив на стан інформаційної безпеки великої кількості підприємств, організацій та індивідуальних користувачів;

– на рівні державних органів (зокрема урядів окремих країн);

– на рівні окремих підприємств, установ та організацій, що є безпосередніми власниками та користувачами інформаційних ресурсів.

Також розглядаються питання роботи спеціалізованих компаній (консалтингових, технологічних, страхових), що надають різні послуги, пов'язані із забезпеченням інформаційної безпеки.

Контрольні питання:

1. Дайте визначення поняття інформаційна безпека. Назвіть основні чинники, які на неї негативно впливають, та методи, завдяки яким цьому можна запобігти.
2. Що таке загроза?
3. Назвіть види загроз.
4. Дайте визначення поняття ризик.
5. Назвіть види ризиків.
6. Назвіть основні способи порушення інформаційної безпеки.
7. Дайте визначення поняття СУІБ.
8. Прокоментуйте модель PDCA.

ТЕМА 8
ДІЯЛЬНІСТЬ МІЖНАРОДНИХ ОРГАНІЗАЦІЙ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У темі розкриваються цілі, принципи та специфіка роботи міжнародних незалежних організацій у сфері інформаційної безпеки. Наводиться масштабована класифікація і перераховуються напрями роботи таких структур. Описується робота організацій широкого профілю, як-от Міжнародний союз електрозв'язку, Інститут інженерів з електроніки та електротехніки, Асоціація обчислювальної техніки, Консорціум Всесвітньої Павутини, Міжнародна організація з стандартизації, що надають фундаментальний вплив на стан і розвиток інфраструктури мереж передачі даних і глобальних механізмів захисту інформації.

Ключові слова: *діяльність, telecommunications, electronic engineering, computing machinery, internet engineering taskforce, ICSA, computationally secure, internet security, bureau, conference, lead, study, datanetwork, communication system, архітектура безпеки, системи автентифікації, інформаційне суспільство, computer society, technical committee, workshop, special interest group, SIG, CCS, communication security, electronic commerce.*

План

8.1. Загальні відомості.

8.2. Робота міжнародних професійних об'єднань.

8.3. International Telecommunication Union (ITU) – Міжнародний союз електрозв'язку.

8.4. Institute of Electrical and Electronics Engineers (IEEE) – Інститут інженерів з електроніки та електротехніки.

8.5. Association for Computing Machinery (ACM) – Асоціація обчислювальної техніки.

8.6. World Wide Web Consortium (W3C) – Консорціум Всесвітньої Павутини.

8.7. NIST – Національний інститут стандартів і технологій.

8.8. International Organization for Standardization (ISO) – Міжнародна організація з стандартизації.

8.1. Загальні відомості

Серед міжнародних організацій, що діють у сфері інформаційної безпеки та роблять істотний вплив на функціонування глобальних інформаційних систем і діяльність всього інформаційного співтовариства, виділяються організації таких типів:

1. Великі міжнародні некомерційні та неурядові організації, що об'єднують фахівців у певних областях, що існують, як правило, вже протягом багатьох років і охоплюють безліч основних напрямків розвитку комп'ютерної інженерії, електроніки та телекомунікацій, включаючи в тому числі і певні питання забезпечення безпеки сучасних інформаційних технологій.

2. Окремі відносно невеликі організації, які спеціалізуються на більш-менш вузьких питаннях інформаційної безпеки, що мають глобальне значення для всього співтовариства користувачів інформаційних систем, і з'явилися на базі приватних компаній або дослідницьких структур протягом останнього десятиліття, коли проблеми інформаційної безпеки стали особливо актуальними.

3. Спільні структури (комітети, альянси та ін.), створювані (іноді тимчасово) великими компаніями (іноді за участю великих дослідницьких центрів, навчальних закладів та урядових структур) для вирішення певних завдань у сфері інформаційних технологій та інформаційної безпеки.

Кожна з них також має свої специфічні організаційні особливості, проте всі вони здебільшого вирішують завдання розробки, узгодження та подальшого поширення загальних для всього співтовариства користувачів інформаційних систем технічних і організаційних рішень, як-от:

– протоколи глобальних мереж;

– архітектури, алгоритми, протоколи загально доступних засобів шифрування даних;

– правила побудови глобальних мереж обміну даними та інших елементів глобальної інфраструктури інформаційної безпеки.

Також важливими елементами організаційної роботи на рівні міжнародних структур є:

– організація обміну знаннями та актуальними новинами в середовищі фахівців з інформаційної безпеки у формах, як-от публікація спеціалізованих періодичних видань та збірників наукових праць, організація спеціалізованих науково-практичних конференцій, семінарів тощо;

– організація та підтримка в актуальному стані баз даних і баз знань, які містять відомості, необхідні користувачам інформаційних систем, адміністраторам, розробникам та іншим учасникам для забезпечення інформаційної безпеки. Прикладами таких баз даних є бази даних, що містять відомості про виявлені вразливості різних програмних і апаратних платформ інформаційних систем.

Загалом організаційна робота на рівні міжнародних структур не є універсальною, і в більшості випадків вони будують свою роботу самостійно. Однак можна виділити деякі основні організаційні принципи, характерні для діяльності багатьох з них:

– принцип добровільності участі в роботі таких структур і в окремих проєктах або у всій роботі;

– принцип відкритості (доступності) результатів роботи (всіх або їх частини) для спільноти фахівців у сфері інформаційних технологій;

– принцип самофінансування.

8.2. Робота міжнародних професійних об'єднань

Робота великих міжнародних професійних (галузевих) організацій (об'єднань) здебільшого має такі особливості:

– не спрямована тільки на вирішення завдань інформаційної безпеки – завдання інформаційної безпеки вирішуються в комплексі з безліччю інших проблем (розвитку інформаційних технологій, побудови телекомунікаційних систем тощо);

– певною мірою може спиратися на підтримку з боку різних державних структур;

– об'єднує велику кількість фахівців з різних дослідних, навчальних, комерційних організацій, але водночас більшість учасників (членів) може не мати конкретних зобов'язань, що змушують вносити вклад в роботу і досягати певних цілей.

Основними найбільш великими і відомими міжнародними професійними об'єднаннями, так чи інакше пов'язаними з питаннями інформаційної безпеки, є:

– ITU – International Telecommunication Union;

– IEEE – Institute of Electrical and Electronics Engineers;

– ACM – Association for Computing Machinery;

– *W3* Consortium;

– ISSA – Information Systems Security Association;

– ISO – International Organization for Standardization;

– IETF – Internet Engineering Task Force;

– ICSA – International Computer Security Association;

– ISACA – Information Systems Audit and Control Association;

– Internet Security Alliance.

8.3. International Telecommunication Union (ITU) – Міжнародний союз електрозв'язку

ITU є найстарішою міжнародною організацією, пов'язаною з інформаційними технологіями. Вона була заснована в 1885 р. як Міжнародний телеграфний союз, і отримала свою нову назву в 1934 р. Сьогодні ITU об'єднує приблизно 180 держав. Як зрозуміло з назви, основним її завданням спочатку було управління та координація діяльності у сфері передачі інформації, і зокрема в радіозв'язку та телеграфного зв'язку. Однак у міру розвитку глобальних комп'ютерних

мереж і інтеграції комп'ютерних та телекомунікаційних систем сфера діяльності ITU була значно розширена, зараз включає в себе безліч питань, пов'язаних із побудовою комп'ютерних мереж, передачею цифрових даних, обробкою інформації тощо.

Членами ITU-T є:

– державні органи влади (міністерства і відомства зв'язку окремих країн);

– наукові організації і компанії – виробники телекомунікаційного обладнання;

– регіональні та міжнародні телекомунікаційні організації.

Функціональними органами ITU-T є:

– Всесвітня асамблея з стандартизації телекомунікацій (World Telecommunication Standardization Assembly), що проводиться кожні чотири роки, – основний керівний орган сектору стандартизації;

– Бюро з стандартизації телекомунікацій (Telecommunication Standardization Bureau) – виконавчий підрозділ сектору стандартизації;

– Дослідницькі групи (всього їх 14);

– Консультативна група з стандартизації телекомунікацій (Telecommunication Standardization Advisory Group) – допоміжний підрозділ, що здійснює координаційну роботу.

Вищим органом влади Союзу є Повноважна Конференція (Plenipotentiary Conference), збори делегацій держав – членів Союзу, що проходить раз на чотири роки. Основні виконавчі органи – Рада і Генеральний секретаріат ITU. Основні робочі підрозділи розділені на три сектори:

– сектор стандартизації зв'язку, ITU-T;

– сектор радіозв'язку, ITU-R;

– сектор розвитку електрозв'язку ITU-D.

ITU-R і ITU-D виконують окремі дослідницькі, координаційні та технічні функції (наприклад, реєстрація радіочастот або координація роботи космічних телекомунікаційних супутників), тоді як Сектор стандартизації зв'язку – ITU-T – більшою мірою відповідає за вирішення стратегічних завдань розвитку інформаційних технологій та інфраструктури, зокрема за розробку методик і стандартів, необхідних для всієї світової спільноти.

Основною метою роботи ITU-T є розробка універсальних рекомендацій та міжнародних стандартів, що належать до різних сфер телекомунікаційних технологій та управління телекомунікаціями. Розроблювані рекомендації забезпечують основу для розвитку ринку послуг зв'язку, створення сумісних технічних та організаційних систем тощо. З погляду забезпечення інформаційної безпеки найбільш значущими стали рекомендації, що належать до серії «X – Мережі передачі даних і зв'язок відкритих систем», зокрема до серії «X.8xx – Безпека».

Відповідно до Резолюції 1 Всесвітньої асамблеї зі стандартизації телекомунікацій 2000-го р., була введена практика призначення Провідних дослідницьких груп (Lead Study Groups, LSGs) з певних питань, що вимагають одночасної координації зусиль кількох дослідницьких груп, які працюють у різних областях. Починаючи з вересня 2001 р. функціонує «Дослідницька група 17: Мережі передачі даних та телекомунікаційне програмне забезпечення» («StudyGroup 17: Data Networks and Telecommunication Software»), утворена на основі «Дослідницької групи 7» і «Дослідницької групи 10». З моменту свого утворення вона є Провідною дослідницькою групою з питань безпеки комунікаційних систем (Communication Systems Security, CSS), і відповідно, не тільки працює над забезпеченням безпеки технологій, що безпосередньо належать до її компетенції, а й контролює питання забезпечення безпеки різних комунікаційних технологій, що розробляються іншими дослідницькими групами.

Однією з найбільш значимих розробок цієї групи у сфері інформаційної безпеки вважається Стандарт X.509, що заклав основи розвитку інфраструктури відкритих ключів. Найбільш актуальними проблемами, над якими нині працює Провідна дослідницька група з питань безпеки комунікаційних систем, є:

– управління безпекою;

– безпека мобільних систем;

– безпека систем зв'язку служб реагування на надзвичайні ситуації;

– телебіометрія.

Загалом же робота цієї дослідницької групи охоплює такі основні сфери:

– безпека управління мережами (включає в себе роботу над рекомендаціями: M.3010 – Принципи мереж управління телекомунікаціями, M.3016 – Огляд безпеки мереж управління телекомунікаціями та деякі інші);

– автентифікація і служби каталогів (X.500 – Огляд концептуальних моделей і сервісів, X.509 – Основи технології відкритих ключів і сертифікатів та деякі інші);

– управління системами (X.733 – Функція звіту про подію, X.740 – Функція проведення аудиту безпеки та деякі інші);

– основи архітектури безпеки (X.800 – Архітектура безпеки інфраструктури відкритих систем для додатків ITU; X.802 – Модель безпеки нижніх рівнів, X.803 – Модель безпеки верхніх рівнів та деякі інші);

– факсимільний зв'язок (T.36 – Можливості забезпечення безпеки використовуючи факсимільні апарати третьої групи; T.563 – Характеристики терміналів для використання з факсимільними апаратами четвертої групи та деякі інші);

– телевізійні та кабельні системи (J.170 – Специфікація безпеки IPCabelcom та деякі інші);

– техніка забезпечення безпеки (X.841 – Об’єкти інформаційної безпеки для контролю доступу та деякі інші);

– мультимедійні комунікації (H.233 – Система забезпечення конфіденційності для аудіовізуальних сервісів, H.234 – Управління ключами шифрування і системою аутентифікації в аудіовізуальних сервісах та деякі інші).

Крім розробки рекомендацій і стандартів, одним із важливих напрямів роботи ITU також стало забезпечення інформаційного обміну в різних формах: поширення методичних матеріалів, що стосуються забезпечення інформаційної безпеки, проведення семінарів і конференцій. Одним з найбільш масштабних таких заходів є Всесвітній саміт з інформаційного суспільства (WSIS: The World Summit On The Information Society).

8.4. Institute of Electrical and Electronics Engineers (IEEE) – Інститут інженерів з електроніки та електротехніки

IEEE є однією з найбільш відомих професійних організацій, існує з 1884 р. і тепер налічує майже 380 тисяч членів зі 150 країн світу. У сферу її інтересів входить безліч питань, пов’язаних з електротехнікою, радіоелектронікою, обчислювальною технікою, інформатикою, а також деякими розділами фізики і математики.

Основні напрями роботи цієї організації:

– проведення спеціалізованих професійних конференцій;

– публікація спеціалізованих видань;

– підтримка освітньої діяльності;

– підтримка інноваційних технічних та методичних розробок у різних сферах;

– розробка та поширення технічних стандартів.

До складу IEEE входять 10 регіональних відділень, 38 професійних товариств, 4 ради та 1 450 студентських відділень. Поточне управління діяльністю на верхньому рівні здійснюється Радою директорів і Виконавчим комітетом, роботу яких очолюють Президент та Виконавчий директор.

Одним з основних підрозділів IEEE, що спеціалізуються на питаннях інформаційної безпеки, є Технічний комітет з безпеки і захисту приватної інформації – «IEEE Computer Society Technical Committee on Security and Privacy» (http://www.ieee-security.org/). У його складі функціонують три підкомітети:

– підкомітет з стандартів (Subcommittee on Standards);

– підкомітет з академічної роботи (Subcommittee on Academic Affairs);

– підкомітет зі спеціалізованих конференцій (Subcommittee on Security Conferences).

Основними заходами, які проводить цей комітет, є:

– щорічний симпозіум з безпеки і захисту приватної інформації (IEEE CS Symposium on Security and Privacy);

– щорічний семінар з основ інформаційної безпеки (Computer Security Foundations Workshop).

Також комітет проводить роботу зі збору та узагальнення актуальної інформації про події в співтоваристві фахівців з інформаційної безпеки: оголошення про заплановані конференції, звіти про минулі конференції і семінари, огляди літератури та періодики, посилання на ресурси в мережі Інтернет і под. Спеціальний інформаційний бюлетень із цією інформацією – «Cipher» – розсилається передплатникам в середньому один раз на два місяці.

8.5. Association for Computing Machinery (ACM) – Асоціація обчислювальної техніки

ACM є однією з найстаріших організацій, пов'язаних з інформаційними технологіями, – вона була заснована в 1947 р., на зорі розвитку комп'ютерної техніки. Основні завдання ACM – підтримка освітніх проєктів у сфері інформаційних технологій, організація науково-практичних конференцій, симпозіумів та семінарів, суспільно-політична робота, пов'язана з інформаційними технологіями, публікація періодичних видань та збірників наукових праць, присвячених проблемам сучасних інформаційних технологій, підтримка електронного архіву таких публікацій, а також інша подібна діяльність. Основним керуючим органом цієї організації є Рада ACM, до якої входить 16 осіб, зокрема президент і віцепрезидент. Управління поточними справами Асоціації здійснюють чотири профільні комітети. Штаб-квартира ACM, у якій працюють основні виконавчі органи, розташовується у Нью-Йорку з 1960 р.

Однією з основ організації роботи ACM є поділ всієї спільноти членів асоціації на так звані групи спеціальних інтересів *(Special Interests Group – SIG)* – підрозділи, що спеціалізуються на окремих відносно вузьких проблемах розвитку інформаційних технологій. Всього ACM об'єднує 34 групи, що спеціалізуються на різних питаннях розробки та використання програмного забезпечення, апаратних засобів і телекомунікацій. Кожна з груп самостійно визначає для себе межі своєї діяльності, а їх політика та фінансові питання координуються одним з комітетів.

Одна з цих груп – **Special Interest Group on Security, Audit and Control** (SIGSAC, Група спеціальних інтересів з питань безпеки, аудиту та контролю, http://www.acm.org/sigs/sigsac/) – спеціалізується на питаннях інформаційної безпеки.

Основним завданням цієї групи є організація роботи спеціалізованих науково-практичних конференцій, як-от:

– Симпозіум з технологій і моделей управління доступом (SACMAT: ACM Symposium on Access Control Models and Technologies), що проводиться щорічно починаючи з 1995 р.;

– Конференція з безпеки комп'ютерів і комунікацій (CCS : ACM Conference on Computer and Communications Security), проводиться щорічно починаючи з 1993 р.

До того ж питання інформаційної безпеки прямо або побічно зачіпають у роботі інших спеціалізованих груп Асоціації, як-от, наприклад, Special Interest Group on Electronic Commerce (Група з проблем електронної комерції).

8.6. World Wide Web Consortium (W3C) – Консорціум Всесвітньої Павутини

Створення W3C було ініційовано в 1989 р. з метою розробки єдиних, узгоджених стандартів обміну інформацією в глобальних мережах передачі даних, а офіційно створення консорціуму було оформлено в 1994 р. Його основними завданнями є:

– забезпечення можливості доступу до мережі Інтернет для якомога більшої кількості людей незалежно від знання іноземних мов, культурної приналежності, географічного положення і доступних їм технічних засобів і технічної інфраструктури;

– забезпечення можливості підключення до інтернету різних технічних пристроїв;

– забезпечення можливості структурування та формалізації інформації, доступної через інтернет, з метою зробити її якомога більш придатною для автоматизованої обробки;

– забезпечення надійності та безпеки обміну інформацією, а також можливості брати участь в інформаційному обміні з тим рівнем захищеності, який окремі користувачі вважають для себе за потрібний.

До теперішнього часу консорціум об'єднує більше чотирьохсот провідних технологічних і телекомунікаційних компаній, урядових організацій, дослідницьких центрів, інститутів і університетів по всьому світу. До того ж у штаті консорціуму знаходяться приблизно 70 незалежних технічних експертів, які забезпечують його роботу. Фінансування діяльності здійснюється завдяки членським внескам, а основні адміністративні функції і повсякденна діяльність виконуються на базі трьох організацій:

– Массачусетський технологічний інститут (США);

– Європейський консорціум з досліджень в галузі інформатики та математики (Франція);

– Університет Кейо (Японія).

Крім формування стандартів («рекомендацій»), ця організація також займається освітньою діяльністю та надає можливості для обговорення різних питань, пов'язаних із функціонуванням мережі Інтернет.

Діяльність консорціуму організована у вигляді груп: Робочі групи (займаються опрацюванням технічних питань), Групи спеціальних інтересів і Координаційні групи (забезпечують взаємодію між іншими групами). У кожну групу входять представники організацій-учасників консорціуму і запрошені експерти. Сфери роботи консорціуму («домени», Domain), розділені на напрями (Activities). Робота за двадцяти чотирма напрямами виконується загалом шістдесятьма групами.

Питаннями інформаційної безпеки займається сфера «Технологія і суспільство» (Technology and Society Domain) в межах спеціального напряму «Безпека» (W3C Security Activity), що складається з двох робочих груп. Також до 2006 р. в складі Консорціуму функціонував напрям «Захист приватної інформації» (Privacy).

До робіт консорціуму у сфері інформаційної безпеки належать:

– розробка стандарту цифрових підписів для інформаційних ресурсів (PICS Signed Labels 1.0 Specification);

– розробка системи електронного підпису для документів XML;

– розробка стандартів передачі зашифрованих даних з використанням мови XML.

8.7. NIST

NIST – Національний інститут стандартів і технологій, США (The National Institute of Standards and Technology) – заснований в 1901 р. і до 1988 р. відомий як Національне бюро стандартів (National Bureau of Standards (NBS)). Інститут є підрозділом Управління з технологій США, одного з агентств Департаменту торгівлі США.

Основні завдання: сприяння підвищенню інноваційної та індустріальної конкурентоспроможності США шляхом розвитку наук щодо вимірювання, стандартизації і технології з метою підвищення економічної безпеки і поліпшення якості життя.

Інститут реалізує свою місію в чотирьох спільних програмах:

– NIST Laboratories – лабораторії NIST – проводять дослідження в галузі розвитку технологічної інфраструктури промисловості США для постійного поліпшення вироблених товарів і послуг;

– Baldrige National Quality Program – національна програма контролю якості ім. Балдріджа – забезпечує перевірку якості діяльності виробничих і сервісних під-

приємств, освітніх і медичних установ, некомерційних організацій; організовує програми підтримки організаціям і проводить щорічне вручення Національної премії якості імені Малкома Балдріджа за досягнення високих результатів діяльності і високу якість;

– Hollings Manufacturing Extension Partnership – мережа локальних центрів, що пропонують технічну і підприємницьку допомогу невеликим підприємствам;

– Technology Innovation Program – програма підтримки інноваційних технологій – пропонує часткову компенсацію досліджень перспективних технологій для задоволення державних і соціальних потреб суспільства.

Національний інститут стандартів і технології (NIST) разом з Американським національним інститутом стандартів (ANSI) бере участь у розробці стандартів і специфікацій до програмних рішень, що застосовуються як у державному секторі США, так і має комерційне застосування. З більш детальною інформацією щодо діяльності Інституту можна ознайомитись за посиланням: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-100.pdf

8.8. International Organization for Standardization (ISO) – Міжнародна організація по стандартизації

ISO в нинішньому вигляді була заснована в 1946 р. І являє собою неурядове об'єднання національних організацій зі стандартизації, націлене на уніфікацію стандартів (в основному технічних) у різних областях виробничої діяльності та надання послуг.

Крім основних членів (близько 150 країн), які безпосередньо беруть участь у роботі, в ISO також входять члени-кореспонденти (Correspondent member) – країни, що не мають повноцінних органів стандартизації, а також члени-передплатники (Subscriber member) – країни з невеликими економіками, які отримують необхідну довідкову інформацію на пільгових умовах.

Головним органом управління ISO є щорічна Генеральна Асамблея, яка приймає стратегічні рішення, що стосуються розвитку всієї організації. Підготовкою матеріалів для прийняття таких рішень займається Рада ISO, збори якої проходять два рази на рік. Безпосередньою розробкою стандартів займаються технічні комітети і підкомітети, в роботі яких беруть участь представники зацікавлених країн. За розробку кожного документа в підкомітеті відповідає спеціально створювана для цього робоча група. Проєкти міжнародних стандартів, прийняті технічними комітетами, розсилаються в національні організації для голосування; документ набуває статусу міжнародного стандарту, якщо за нього проголосувало не менше 75 % членів, які брали участь у голосуванні.

Основним підрозділом ISO, який займається питаннями інформаційної безпеки, є Об'єднаний технічний комітет JTC 1 «Інформаційні технології», до складу

якого входить підкомітет SC 27 Засоби безпеки в інформаційних технологіях (IT Security techniques). За час своєї роботи цей підкомітет розробив понад 60 міжнародних стандартів, що відносяться до інформаційної безпеки.

З питаннями інформаційної безпеки також пов'язана робота підкомітету SC 37 «Біометрична ідентифікація» (Biometrics) та підкомітету SC 17 «Картки і персональна ідентифікація» (Cards and personal identification).

Контрольні питання:

1. Що є елементами організаційної роботи на рівні міжнародних структур?
2. Назвіть основні найбільш великі і відомі міжнародні об'єднання, пов'язані з питаннями інформаційної безпеки.
3. Назвіть основні завдання Консорціуму Всесвітньої Павутини.
4. Назвіть головні завдання Міжнародної організації зі стандартизації.

ТЕМА 9
СТАНДАРТИЗАЦІЯ В СФЕРІ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У темі розглянуто сучасний стан стандартизації одного з найважливіших напрямів захисту інформації – менеджменту інформаційної безпеки. Стандартизація є інструментом забезпечення якості продукції, робіт і послуг – важливого аспекту багатогранної комерційної діяльності. Мета стандартизації – досягнення оптимального ступеня упорядкування в тій чи іншій галузі за допомогою широкого і багаторазового використання встановлених положень, вимог, норм для вирішення реально наявних, що плануються або потенційних завдань. Розглянуто серію стандартів ISO 27000 «Міжнародні стандарти для системи управління інформаційною безпекою».

Ключові слова: *інформаційна безпека, модель систем менеджменту, стандарт, управління ризиками, керівні вказівки, процесний підхід.*

План

9.1. Вимоги до розроблюваних стандартів.
9.2. Типи стандартів.
9.3. Елементи стандартів.
9.4. Огляд стандартів РГ 1.

9.1. Вступ

Для розробки стандартів у галузі безпеки інформаційних технологій засновано підкомітет SC 27 «Security techniques» (Методи забезпечення безпеки) у межах об'єднаного технічного комітету ISO/IEC JTC 1 «Information technology» (Інформаційні технології). Широкий спектр питань інформаційної безпеки, розглянутих фахівцями, залученими до діяльності SC 27, розподілений між п'ятьма робочими групами, що становлять весь підкомітет. За кожною групою закріплено відповідний напрям.

Перша робоча група (РГ 1) «Information Security Management Systems» (Системи менеджменту ІБ) займається розробкою стандартів і настановчих вказівок щодо побудови систем менеджменту інформаційної безпеки (ISMS).

Друга робоча група (РГ 2) «Cryptography and security mechanisms» (Шифрування і механізми безпеки) стосується стандартизації методів і механізмів забезпечення безпеки ІТ.

Третя робоча група (РГ 3) «Security evaluation criteria» (Критерії оцінки безпеки) розробляє стандарти для оцінювання безпеки та сертифікації інформаційних систем та їх компонентів.

Четверта робоча група (РГ 4) «Security controls and services» (Контроль безпеки і послуг) займається розробкою і підтримкою стандартів і настановчих вказівок, що стосуються послуг і додатків, які сприяють реалізації заходів щодо захисту інформації, визначених у стандартах ISO/IEC 27001, 27002.

П'ята робоча група (РГ 5) «Identity management and privacy technologies» (Управління ідентифікаціями і конфіденційністю) розробляє стандарти та настановчі вказівки, що стосуються керування ідентифікаційними даними, біометрії та захисту персональних даних (privacy).

У своїй діяльності робочі групи дотримуються принципів і правил, прийнятих в ISO і IEC. Зокрема, у робочих групах повинні розроблятися і через кожні шість місяців переглядатися дорожні карти (roadmaps). Нижче ми зупинимося на змісті дорожньої карти, прийнятої в РГ 1.

Метою дорожньої карти є:

– точна ідентифікація стандартів, що стосуються РГ 1, як уже розроблених, так і розроблюваних або тих, що готуються до розробки;

– опис логічних зв'язків між розроблюваними в РГ 1 стандартами;

– створення підстав, за допомогою яких робота зі створення стандартів може бути скоординована для уникнення дублювання);

– можливість планування роботи з стандартизації в рамках РГ 1 в майбутньому;

– більша координація між різними технічними комітетами ISO і IEC.

9.2. Вимоги до стандартів, що розробляються

Стандарти, що розробляються в РГ 1, стосуються захисту інформації, яка може існувати в різних видах (наприклад, бути надрукованою або написаною на папері, збереженою на електронних або магнітних носіях, переданою звичайною або електронною поштою, відеоінформацією, мовною інформацією). Також в РГ 1 розробляються стандарти, що стосуються механізмів, які мінімізують шкоду, завдану організації через неналежний захист інформації (помилки у фінансових звітах, неправильні документи, випущені організацією, втрата репутації і престижу тощо).

Щоб ефективно вирішувати питання інформаційної безпеки, організації необхідно:

– систематично управляти діяльністю, пов'язаною з інформаційною безпекою;

– демонструвати свою здатність задовольнити вимоги внутрішніх і зовнішніх зацікавлених сторін.

Для того, щоб бути корисними різним організаціям, стандарти, які стосуються РГ 1, повинні бути:

– згодженими (тобто мати спільну модель систем менеджменту, спільну структуру, узгоджену термінологію);

– взаємопов'язаними з іншими стандартами ISO, як-от ISO 9000 (серія стандартів з систем менеджменту якості), ISO 14000 (система стандартів з менеджменту навколишнього середовища).

Стандарти РГ 1 повинні відповідати основним принципам, що застосовуються до стандартів з систем менеджменту:

– допомогти користувачам реалізувати системи менеджменту;

– допомогти розробникам стандартів встановити узгоджену і логічну структуру.

9.3. Типи стандартів

Дорожня карта РГ 1 дотримується чотирирівневої моделі, в межах якої розробляються стандарти, які стосуються РГ 1:

– тип А – термінологічний стандарт;

– тип В – стандарт, що стосується вимог;

– тип С – стандарт, що стосується надання настановних вказівок (guidelines);

– тип D – суміжний стандарт.

Розглянемо ці типи більш детально.

Тип А – термінологічний стандарт.

Стандарт призначений для надання основної інформації, що включає загальну термінологію, яка узгоджено використовується у всій серії стандартів РГ 1.

Тип В – стандарт, що стосується вимог.

Стандарт призначений для надання специфікацій, які відносяться до справи, що дають змогу організаціям демонструвати свою здатність задовольнити внутрішні та зовнішні вимоги з інформаційної безпеки.

Прикладами стандартів типу В є:

В–1: ISO/IEC 27001:2013. Системи менеджменту інформаційної безпеки – Вимоги.

В–2: ISO/IEC 27006:2015. Вимоги до органів, які проводять аудит і сертифікацію систем менеджменту інформаційної безпеки.

Тип С – стандарт, що стосується надання настановчих вказівок.

Стандарт призначений для допомоги організаціям у реалізації стандартів типу В.

Прикладами стандартів типу С є:

С–1:

– стандарти, що містять настанови щодо задоволення вимог до ISMS;

– стандарти, що містять настанови щодо вибору та реалізації заходів з інформаційної безпеки.

С–2:

– стандарти, що містять посібники з реалізації конкретних заходів / методів інформаційної безпеки (Менеджмент інцидентів інформаційної безпеки);

– стандарти, що містять настанови щодо досягнення специфічних процесів, пов'язаних з менеджментом інформаційної безпеки (наприклад, вимірювання ефективності заходів).

С–3:

– стандарти, що містять настанови щодо реалізації вимог з інформаційної безпеки, що враховують особливості галузі (банківська справа, розробка програмного забезпечення, охорона здоров'я, телекомунікації).

Тип D – суміжний стандарт.

Стандарт призначений для надання подальших настанов, що стосуються конкретних сторін інформаційної безпеки або суміжних методів підтримки. У загальному випадку ці стандарти розробляються на односторонній основі без точних описів, що стосуються зв'язків зі стандартами типу В та/або типу С.

9.4. Елементи стандартів

Досвід, пов'язаний зі стандартами щодо систем менеджменту, які розробляються в ISO, показує, що в них існує низка спільних елементів. Ці загальні елементи можна впорядкувати за такими основними темами:

– політика;
– планування;
– реалізація та експлуатація;
– оцінювання;
– покращення;
– перегляд керівництвом.

9.5. Огляд стандартів РГ 1

Розглянемо стан стандартів, розроблюваних РГ 1.

ISO/IEC IS 27000:2018 – Information security management systems – Overview and vocabulary (published) [Системи менеджменту інформаційної безпеки – Огляд і словник (опублікований)]. З метою полегшення гармонізації стандартів, що належать до РГ 1, і забезпечення єдиного і чіткого їх розуміння необхідно документувати в одному стандарті основні положення, систематичний словник і набір основних понять і термінів, що використовуються у всій серії стандартів, що належить до РГ 1. Цей стандарт є ключовим документом для досягнення ефективності розробки стандартів у РГ 1.

ISO/IEC IS 27001:2013 – Information security management systems – Requirements [Системи менеджменту інформаційної безпеки – Вимоги]. Цей стандарт утворює серцевину сімейства ISMS стандартів. Він визначає вимоги для встановлення, реалізації, експлуатації, моніторингу, перегляду, підтримки документованої ISMS в контексті загальних ділових ризиків організації. Він також визначає

вимоги до реалізації заходів безпеки, адаптованих до потреб конкретних організацій або їх частин.

ISO/IEC IS 27006:2015 – Requirements for bodies providing audit and certification of information security management systems (published) [Вимоги до органів, що здійснюють аудит і сертифікацію систем менеджменту інформаційної безпеки (опублікований)]. Цей стандарт визначає вимоги та надає настанови для органів, що здійснюють аудит і сертифікацію систем менеджменту інформаційної безпеки, на додаток до вимог, що містяться в стандартах ISO/IEC 17021 та ISO/IEC 27001.

ISO/IEC IS 27002:2013 – Code of practice for information security controls (published) [Практичні правила для заходів з інформаційної безпеки] (опублікований). ISO/IEC 27002 – це стандарт, що надає всеохопні настанови щодо реалізації заходів інформаційної безпеки, і безпосередньо підтримує стандарт ISO/IEC 27001.

ISO/IEC 27003:2012 – Information security management systems implementation guidance (published) [Настанова з реалізації систем менеджменту інформаційної безпеки (опублікований)]. Цей стандарт безпосередньо підтримує стандарт ISO/IEC 27001 і надає матеріал з настанов, який стосується реалізації ISMS.

ISO/IEC 27004:2011 – Information security management measurements (published) [Вимірювання менеджменту інформаційної безпеки (опублікований)]. ISO/IEC 27004 запропонований як стандарт з настанов, який надає можливість оцінювати рівень ефективності реалізованих відповідно до стандарту ISO/IEC 27001 заходів і процесів. ISO/IEC 27004 розглядає низку одиниць вимірювання, що включають показники результативності заходів. Також надає такі засоби, які б дали смогу фективно вимірювати діяльність з інформаційної безпеки, яка використовується для захисту інформаційних активів організації.

ISO/IEC IS 27005:2011 – Information security risk management (published) [Керування ризиками інформаційної безпеки (опублікований)]. Цей стандарт надає посібник з менеджменту ризиків інформаційної безпеки і розглядає принципи менеджменту ризиків інформаційної безпеки, методи оцінки ризиків, аналіз ризиків, моніторинг і перегляд ризиків, надаючи додаткові рекомендації щодо виконання стандарту ISO/IEC 27001.

ISO/IEC 27007:2014 – Guidelines for information security management systems auditing (published) [Настанова з аудиту систем менеджменту інформаційної безпеки (опублікований)]. ISO/IEC 27007 запропонований з метою надання настанов з проведення аудитів ISMS, а також настанов з компетентності аудиторів систем менеджменту інформаційної безпеки в доповнення до настанов, які містяться в ISO 19011. Цей стандарт розглядає окрему настанову, що необхідна для аудитів ISMS в підтримку стандарту ISO/IEC 27006 і загальної настанови для аудиторів, що міститься в ISO 19011.

ISO/IEC TR 27008:2011 – Guidance for auditors on ISMS controls (published) [Настанова для аудиторів заходів ISMS (опублікований)]. Цей технічний звіт 2-го типу націлений на надання настанови з того, як перевірити доказ і якість заходів, що були реалізовані в ISMS, завдяки чому підтримати планування і виконання оцінки заходів ISMS.

ISO/IEC 27013:2017 – Guidance on the integrated implementation of 20000-1 and 27001 (published) [Настанова з інтегрованої реалізації стандартів ISO/IEC 20000-1 і ISO/IEC 27001 (опублікований)]. Цей стандарт надає настанови зі впровадження інтегрованої системи менеджменту інформаційної безпеки та менеджменту IT-послуг.

ISO/IEC 27014:2013 – Information security governance framework (published) [Основні положення управління інформаційною безпекою (опублікований)]. Цей стандарт надає основні положення (framework) управління інформаційною безпекою в підтримку вимог до управління корпорацією, які потребують від організації продемонструвати ефективні внутрішні заходи з управління.

ISO/IEC 27010:2015 – Information security management guidelines for inter-sector communications (published) [Настанови з менеджменту інформаційної безпеки для міжгалузевих зв'язків (опублікований)]. Цей стандарт надає настанови менеджменту інформаційної безпеки зв'язків і співробітництва між відкритими і/або закритими секторами.

ITU X.1051 | ISO/IEC 27011:2018 – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002 [Настанова з менеджменту інформаційної безпеки для телекомунікаційних організацій на основі ISO/IEC 27002]. Цей стандарт:

– встановлює настановні вказівки і загальні принципи для ініціювання, реалізації, підтримки і покращення менеджменту інформаційної безпеки в телекомунікаційних організаціях на основі ISO/IEC 27002;

– надає основу для реалізації менеджменту інформаційної безпеки в телекомунікаційних організаціях для забезпечення конфіденційності, цілісності і доступності телекомунікаційних засобів і послуг.

ISO/IEC 27015:2012 – Information security management guidelines for financial and insurance services (published) [Настанови з менеджменту інформаційної безпеки для фінансових послуг і послуг страхування (опублікований)]. Цей стандарт встановлює вимоги і вказівки для ініціювання, реалізації, підтримки і покращення менеджменту інформаційної безпеки, специфічні для організацій, які надають фінансові послуги і послуги страхування. Вимоги стандарту доповнюють вимоги стандарту ISO/IEC 27001, які також повинні виконуватись. Настанови доповнюють загальні настанови з реалізації менеджменту інформаційної безпеки, які надаються стандартом ISO/IEC 27002, у контексті надання фінансових послуг та страхування.

ISO/IEC 27031:2011 – Guidelines for ICT readiness for business continuity (published). Настанови щодо готовності ІКТ для підтримки неперервності бізнесу. Цей стандарт описує концепцію і принципи готовності ІКТ для підтримки безперервного бізнесу для будь-якої організації незалежно від її розміру, а також специфікації усіх аспектів покращення готовності ІКТ для забезпечення неперервності бізнесу. Область дії цього стандарту охоплює всі події і інциденти, котрі можуть мати вплив на системи і інфраструктуру ІКТ. Вона включає і розширює практичні правила поведінки з інцидентами безпеки і менеджмент планування підтримки готовності ІКТ.

ISO/IEC 27033 – Network security (all parts) [Безпека мереж (всі частини)]. Різні частини цього стандарту надають детальні настанови з аспектів безпеки, що належать до управління та використання мереж інформаційних систем і їх зв'язків.

ISO/IEC 27034 – Application security (all parts) [Безпека додатків (всі частини)]. Різні частини цього стандарту надають настановні вказівки для розробників програмного забезпечення, адміністраторів безпеки, користувачів програмного забезпечення, аудиторів, менеджерів з визначення, розробки у випадку необхідності, реалізації, підтримки і заміни додатків з погляду інформаційної безпеки.

ISO/IEC 27035:2018 – Information security incident management [Менеджмент інцидентів інформаційної безпеки]. Цей стандарт надає настанову з оцінки ризиків, що виникають від придбання і використання послуг аутсорсингу в підтримку стандарту ISO/IEC 27001 і заходів, пов'язаних з аутсорсингом, стандарту ISO/IEC 27002.

ISO/IEC 27037:2017 – Guidelines for identification, collection and/or acquisition and preservation of digital evidence) [Настановні вказівки для ідентифікації, збору і/або придбання і зберігання цифрових доказів]. Цей стандарт надає детальну настанову, яка описує процес виявлення, ідентифікації, збору і/або придбання і зберігання цифрових даних, які можуть містити інформацію, що має потенційне доказове значення.

Контрольні питання:

1. Що таке стандартизація?
2. Що є найважливішими результатами стандартизації?
3. Назвіть основні вимоги до стандартів, що розробляються.
4. Які типи стандартів ви знаєте?
5. З яких елементів складається стандарт?
6. Назвіть стандарти серії 27000.

ТЕМА 10
РОБОТИ СПЕЦІАЛІЗОВАНИХ МІЖНАРОДНИХ ОРГАНІЗАЦІЙ ТА ОБ'ЄДНАНЬ У ГАЛУЗІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У темі описано альянси великих технологічних компаній, організації, що займаються дослідницькою та інформаційною роботою в масштабі всієї спільноти фахівців у сфері інформаційної безпеки, як-от Координаційний центр CERT, Дослідницька група X-Force, Альянси великих технологічних компаній, Альянс за смарт-картками, Альянс з безпеки мережі Інтернет, Міжнародна асоціація компаній-виробників біометричного устаткування. Описано принципи побудови таких організацій, які вони вирішують завдання, їх напрями роботи.

Ключові слова: *управління інформаційною безпекою, об'єднання, CERT, computationally secure, incident, порушення інформаційної безпеки, загроза інформаційній безпеці, безпека розробки, аналіз вразливостей, група реагування, internet security, ISS, vulnerability, exposure, CVE, аналіз загроз.*

План

10.1. Вступ.

10.2. CERT Coordination Center (CERT/CC) – Координаційний центр CERT.

10.3. X-Force security intelligence team – Дослідницька група X-Force.

10.4. Альянси великих технологічних компаній.

10.5. Smart Card Alliance (SCA) – Альянс за смарт-картками.

10.6. Internet Security Alliance (ISA) – Альянс з безпеки мережі Інтернет.

10.7. The International Biometric Industry Association (IBIA) – Міжнародна асоціація компаній-виробників біометричного устаткування.

10.1. Вступ

Спеціалізовані організації, що мають глобальний вплив на управління інформаційною безпекою на різних рівнях і загальний стан інформаційної безпеки зазвичай можуть функціонувати на базі:

– приватних компаній, що займаються дослідженнями, розробками та консультаціями у сфері інформаційної безпеки;

– великих закладів вищої освіти, що спеціалізуються на інформаційних технологіях, а також мають значним авторитетом та фінансовими ресурсами;

– урядових установ, відповідальних за забезпечення інформаційної безпеки в певних сферах.

Основним напрямом організаційної роботи, що здійснюється в такій формі, стає формування та підтримка баз даних, що містять інформацію про вразливості різних програмних і апаратних засобів, що стали відомими, а також інші

форми та напрями інформаційної, консультативної й методичної роботи в цій сфері.

Важливими чинниками успішності функціонування таких організацій є об'єднання інформації з якомога більшої кількості джерел (зокрема від якомога більшої кількості фахівців і компаній, що займаються проблемами інформаційної безпеки) і якомога більш ефективне поширення відомостей (знань) в співтоваристві користувачів інформаційних систем.

Зважаючи на те, що така форма організаційної роботи заснована на приватних компаніях і відносно невеликих установах, підходи до організації та управління зазвичай не підпорядковуються будь-яким загальним правилам. Також склад таких організацій може з часом змінюватися: на зміну одним дослідницьким центрам можуть приходити інші – більш успішні та ефективні – з тими ж функціями. Наразі можна виділити такі найбільш значущі організації, що займають цю нішу:

– CERT Coordination Center – Координаційний центр CERT;
– Дослідницька група X-Force компанії IBM.

10.2. CERT Coordination Center (CERT/CC) – Координаційний центр CERT

CERT/CC, що створена в 1988 р. як Computer security incident response team (Група реагування на інциденти, пов'язані з комп'ютерною безпекою), функціонує на базі Інституту розробки програмного забезпечення при Університеті Карнегі-Мелон (Software Engineering Institute, Carnegie Mellon University) і фінансується Міністерством оборони та Міністерством національної безпеки США. Разом із проведенням незалежних досліджень та виконанням різних завдань із забезпечення безпеки глобальної інформаційної інфраструктури ця організація забезпечує централізований збір відомостей про всі вразливості в різних інформаційних системах і підтримує актуальну базу знань про інформаційні системи. Відомості про знову виявлені вразливості, шкідливі програми і способи порушення інформаційної безпеки розсилаються по електронній пошті: передплатниками цього бюлетеня є більш ніж 161 000 фахівців у всьому світі.

У межах цієї діяльності CERT/CC здійснює постійну дослідницьку роботу:

– визначення характеру можливих наслідків використання виявлених вразливостей і вірусів;

– аналіз наявних засобів використання вразливостей;

– аналіз того, наскільки активно використовуються вразливості і наскільки поширені віруси;

– взаємодія з постачальниками інформаційних систем з метою більш глибокого аналізу виявлених вразливостей.

На основі проведеного аналізу CERT/CC розробляє заходи щодо усунення вразливостей і рекомендації щодо зменшення негативних наслідків. За результатами цієї роботи всім передплатникам розсилається інформація про загрози інформаційній безпеці та можливі способи їх усунення. Також на основі цих даних формується спеціальна довідкова та технічна документація, проводиться подальша дослідницька та методична робота. Зокрема, CERT/CC підтримує програму безпечної розробки ПЗ («secure coding»), що ґрунтується на тому, що більша частина вразливостей виникає внаслідок відносно кількості помилок у програмному коді інформаційних систем. Отже, CERT/CC на основі накопичених результатів аналізу вразливостей проводить цілеспрямовану роботу з виявлення типових програмних помилок, вироблення стандартів безпечного програмування та поширення цієї інформації серед розробників ПЗ.

Крім основної інформаційної роботи з вразливостями CERT також займається супутніми видами діяльності:

– організація навчальних курсів з різними напрямами (мережева безпека, управління інформаційними ризиками, організація роботи груп реагування);

– сертифікація спеціалістів з реагування на інциденти у сфері інформаційної безпеки;

– підтримка фундаментальних наукових досліджень у різних галузях інформаційної безпеки, як-от методи розробки безпечних додатків, виявлення вразливостей, аналіз шпигунського ПЗ, вирішення питань безпеки як складової частини процесу розробки і тощо;

– сприяння розвитку локальних (національних і корпоративних) груп реагування на інциденти.

10.3. X-Force security intelligence team – Дослідницька група X-Force

Діяльність цієї групи є одним з напрямів бізнесу компанії Internet Security Systems (ISS) – найбільш авторитетного постачальника комплексних рішень у сфері інформаційної безпеки, клієнтами якого є всі без винятку найбільші компанії США, а також урядові організації. Наприкінці 2006 р. ISS була куплена компанією IBM і інтегрована до неї в якості самостійного підрозділу. Одним із завдань групи X-Force є підтримка в актуальному стані бази даних відомих вразливостей різних програмних і апаратних платформ. База даних, підтримувана цією групою, доступна по мережі Інтернет і постійно поповнюється відомостями про нові вразливості (нині їх налічується понад 40 000).

Основні причини, через які ця організація є провідною у цій галузі, такі:

– велика кількість крупних компаній-клієнтів, від яких постійно надходить інформація про атаки, вразливості та ін.;

– наявність власної науково-дослідної бази, на основі якої постійно здійснюється виявлення нових вразливостей і узагальнення відомостей про вразливості, отриманих з різних джерел;

– використання спеціально розроблених універсальних класифікацій (зокрема, загального словника найменувань вразливостей – Common Vulnerabilities and Exposures, CVE) для зберігання і обробки інформації в базах даних відомих вразливостей.

Також одним з напрямів довідково-інформаційної діяльності цієї дослідницької групи є надання послуг з індивідуального аналізу загроз і інформування (X-Force Threat Analysis Service (XFTAS)). Цей комплекс послуг дає змогу замовникам щодня отримувати адаптовану актуальну інформацію про загрози і вразливості з урахуванням особливостей побудови їх інформаційних систем (платформ, додатків, сфери ведення бізнесу, географічного положення) і включає в себе:

– інформацію про загрози;
– експертний аналіз загроз;
– опис поточного і прогнозного стану загроз;
– рекомендовані способи усунення загроз;
– кількісний аналіз атак за останні 30 днів.

Ще одним із завдань групи є випуск періодичних (щоквартальних, щорічних) інформаційних бюлетенів з оглядами найбільш значимих подій у сфері інформаційної безпеки.

10.4. Альянси великих технологічних компаній

Спільні альянси (асоціації, коаліції, групи) великих (іноді середніх) технологічних і консультаційно-дослідницьких компаній являють собою тимчасові (укладаються на короткострокову або середньострокову перспективу) або довгострокові угоди між декількома фірмами, спрямовані на спільне, скоординоване, цілеспрямоване вирішення визначених масштабних і ресурсоємних завдань розвитку технології, формування ринкового попиту на певні продукти та організації інфраструктури інформаційної безпеки. Висока значимість форми організаційної роботи у сфері інформаційної безпеки, як-от формування альянсів великими і середніми компаніями, що спеціалізуються на інформаційних технологіях, обумовлена тим, що:

– такі альянси здатні здійснити значні інвестиції в розробку нових технологій і проведення досліджень, які можуть вплинути на весь розвиток інформаційних технологій і стан справ у сфері інформаційної безпеки;

– компанії, що входять до складу таких альянсів, займають значну частку ринку, тому визначають загальний напрям розвитку інформаційних технологій взагалі та засобів захисту інформації зокрема;

– такі альянси компаній здатні створити комплексні технології, продукти і рішення, що охоплюють різні аспекти функціонування інформаційних систем і засобів захисту інформації, і в такий спосіб досягти нового рівня захищеності інформації, що практично неможливо під час роботи компаній (навіть найбільших) окремо.

Зазвичай кожен такий альянс є унікальним, і учасники в кожному конкретному випадку визначають умови роботи в межах такої організаційної форми. На конкретний підхід до організації альянсу можуть впливати такі фактори:

– характер цілей і завдань, які ставляться перед альянсом;

– поточний стан справ у тій галузі, для роботи в якій створюється альянс;

– склад учасників альянсу, їх роль і місце на ринку інформаційних технологій;

– наявність можливих конкурентів (наприклад, аналогічних альянсів паралельно до створюваних іншими групами компаній);

– раніше сформовані взаємини між компаніями – учасниками альянсу та ін.

Завданнями формування альянсів можуть бути:

– розробка нових продуктів і послуг, а також базових технологій, протоколів, алгоритмів і угод, на основі яких такі продукти та послуги в майбутньому могли б розроблятися;

– формування нових ринків збуту та підтримка наявних;

– вплив на державні та громадські організації, а також на співтовариство користувачів інформаційних систем з метою забезпечення розвитку та більш широкого використання інформаційних технологій і засобів інформаційної безпеки;

– вплив на систему професійної підготовки фахівців з метою забезпечення якості їх навчання.

Основними типовими прийомами організаційної роботи на цьому рівні є:

– скоординований вибір та уніфікація технічних рішень (апаратних пристроїв, програмних алгоритмів), що використовуються в системах передачі та обробки інформації та/або системах захисту інформації;

– інформаційна підтримка як виробників інформаційних систем і постачальників рішень (які входять в альянс і не входять до нього), так і споживачів і користувачів (потенційних і справжніх);

– скоординоване розділення функцій з розробки окремих елементів інформаційної технології в межах спільної узгодженої стратегії розвитку;

– скоординована маркетингова і інформаційна політика, спрямована на забезпечення використання (підтримки, сумісності) створюваних рішень (технологій, протоколів тощо) якомога більшою кількістю споживачів і незалежних виробників, а також її визнання урядовими структурами;

– спільний вплив на органи державної влади (лобіювання) з метою забезпечення державної підтримки певних продуктів, проєктів, технологій та архітектур інформаційних систем і систем захисту інформації.

10.5. Smart Card Alliance (SCA) – Альянс за смарт-картками

SCA займається питаннями розвитку технології смарт-карт – однієї з ключових технологій у сфері інформаційної безпеки, використовуваної для ідентифікації користувачів різних сервісів і інформаційних систем (як-от мобільні телефонні мережі, банківські «електронні гаманці» тощо). Цей довгостроковий (стратегічний) альянс був утворений на початку 2001 р. шляхом злиття двох організацій: Smart Card Industry Association і Smart Card Forum. До складу альянсу входить приблизно сотня різних компаній і урядових організацій водночас серед учасників альянсу виділяється кілька груп:

– Керівна Рада (Leadership Council) – провідні компанії, що визначають основну політику Альянсу: Visa USA, Bank of America, IBM, Lockheed Martin, Intel, Mastercard International і деякі інші (всього більше двадцяти компаній);

– основна група членів Альянсу – різні фірми, так чи інакше пов'язані з питаннями інформаційної безпеки, постачанням відповідних продуктів і послуг (Texas Instruments Incorporated, Sun Microsystems та інші) – всього приблизно 70 компаній;

– члени – урядові організації. У цю групу входять як федеральні урядові установи США (Державний департамент, Міністерство національної безпеки та інші), так і місцеві органи влади (Портова адміністрація Нью-Йорка, Транспортна адміністрація Вашингтона та інші) – близько 30 членів.

Також до складу Альянсу входить один університет і кілька асоційованих членів.

Роботу альянсу очолюють Рада директорів на чолі з головою та Виконавчий директор. Діяльність альянсу розділена на членські ради (Member Council) з окремих сфер інтересів:

– Рада з безконтактних і мобільних платежів;

– Рада з охорони здоров'я (спеціалізується на питаннях використання смарт-карт у сфері охорони здоров'я);

– Рада з ідентифікації;

– Рада з систем контролю за фізичним допуском;

– Рада з транспорту (спеціалізується на питаннях просування та адаптації смарт-карт у транспортній сфері).

Кожна рада керується головою, віцеголовами і керуючим комітетом.

Напрями роботи Альянсу включають:

– організацію спеціалізованих щорічних конференцій;

– організацію освітніх програм і системи сертифікації фахівців;

– видання різних інформаційних та довідкових матеріалів як технічного, так і управлінського характеру;

– ведення централізованої бази даних постачальників обладнання та послуг у сфері смарт-карт.

10.6. Internet Security Alliance (ISA) – Альянс з безпеки мережі Інтернет

ISA був створений у квітні 2001 р. з ініціативи двох великих авторитетних організацій: CERT/CC Університету Карнегі-Меллон та Асоціації електронної промисловості (Electronic Industries Alliance, EIA). Вже до середини 2004 р. до альянсу входило приблизно тридцять членів, серед яких великі компанії, як-от Boeing, NEC, Mitsubishi, Federal Express, AIG, Sony, Symantec та інші.

Роботою Альянсу керує Рада директорів, до якої входять авторитетні представники найбільш відомих компаній-членів. До того ж до складу альянсу входять приблизно тридцять асоційованих членів. На початковому етапі становлення альянсу його основним завданням було підвищення ефективності обміну інформацією про вразливості, поширюваної CERT/CC. Надалі коло завдань альянсу розширювалося, і тепер робота ведеться за такими напрямами:

– створення ефективних механізмів обміну інформацією про вразливість у мережі Інтернет і знайдення рішення проблем безпеки;

– дослідження фундаментальних проблем безпеки;

– розвиток програм професійної підготовки та сертифікації фахівців з інформаційної безпеки;

– взаємодія з державними органами законодавчої і виконавчої влади.

10.7. The International Biometric Industry Association (IBIA) – Міжнародна асоціація компаній-виробників біометричного устаткування

Асоціацію було створено в 1998 р. з метою колективної підтримки інтересів компаній, пов’язаних з виробництвом біометричного устаткування. Основним завданням альянсу є взаємодія з потенційними замовниками їх продукції (як серед комерційних компаній, так і в громадському секторі) з метою просування засобів біометричної ідентифікації. Членами асоціації є приблизно 30 компаній і організацій, серед яких Hitachi, LG Electronics, Panasonic, NEC та інші.

Управління поточними справами здійснює Рада директорів, що складається з одинадцяти осіб, а також виконавчий директор. Діяльність Асоціації розділена на шість робочих груп, серед яких:

– Робоча група зі стандартів та технологій. Її основна мета – захищати базові інтереси членів альянсу у сфері стандартизації біометричних технологій і систем, що використовують біометрію;

– Робоча група зі споживчих додатків. Займається орієнтацією ринку споживчих систем на більш широке використання біометричних технологій;

– Робоча група з міжнародних ринків. Здійснює контакти з іншими біометричними організаціями в усьому світі;

– Робоча група з освіти, маркетингу та інформування. Забезпечує інформаційну присутність компаній-членів асоціації в різних сферах через реалізацію маркетингових заходів і освітніх програм;

– Робоча група з глобальної політики. Проводить інформаційну роботу з представниками урядових структур в усьому світі.

Контрольні питання:

1. Які існують альянси великих технологічних компаній, організації, що займаються дослідницькою та інформаційною роботою у сфері інформаційної безпеки?

2. Назвіть основні напрями організаційної роботи у сфері інформаційної безпеки Координаційного центру CERT.

3. Назвіть напрями діяльності Альянсу за смарт-картками.

4. Перерахуйте основні напрями діяльності Альянсу з безпеки мережі Інтернет.

ТЕМА 11
УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ НА РІВНІ ВЕЛИКИХ ПОСТАЧАЛЬНИКІВ ІНФОРМАЦІЙНИХ СИСТЕМ

У темі розглядається роль великих постачальників інформаційних систем, що роблять найбільш серйозний вплив на розвиток інформаційних технологій та інфраструктуру інформаційних систем. Описується специфічна для них організаційна робота, спрямована на забезпечення безпечного функціонування інформаційних систем та вдосконалення власних продуктів і послуг, пропонованих на ринку. Розглянуто організаційне забезпечення інформаційної безпеки на рівні окремих великих компаній, а саме на рівні Корпорації Microsoft, яка є найбільшим у світі виробником програмного забезпечення та Компанії Cisco Systems, що є світовим лідером у виробництві обладнання для мереж передачі даних.

Ключові слова: *об'єднання, мережа, значення, управління інформаційною безпекою, контроль, аналіз, вразливість, PDA, Windows CE, Pocket, безпека розробки, secure programming.*

План

11.1. Загальна методологія організаційного забезпечення інформаційної безпеки на рівні великих постачальників інформаційних систем.

11.2. Організаційне забезпечення інформаційної безпеки на рівні окремих великих компаній.

11.2.1. Корпорація Microsoft.

11.2.2. Корпорація Cisco Systems.

11.1. Загальна методологія організаційного забезпечення інформаційної безпеки на рівні великих постачальників інформаційних систем

В останнє десятиліття – період, коли відбулося значне поширення автоматизованих інформаційних систем, їх об'єднання в єдину глобальну мережу і масове використання мільйонами користувачів одних і тих же компонентів інформаційних систем (операційних систем, апаратних платформ, протоколів обміну інформацією), – великого значення набуло те, як постачальники подібних універсальних платформ і компонентів (які є іноді практично монополістами на певних сегментах ринку) організовують роботу з підвищення рівня інформаційної безпеки за різними напрямами. Рівень впливу таких компаній на стан справ у сфері інформаційної безпеки іноді може бути дуже значним – навіть більшим, ніж міжнародних організацій і деяких урядових структур.

Основні завдання організаційної роботи великих (тобто тих, що займають велику частку ринку) постачальників інформаційних систем, що широко використовуються у сфері інформаційної безпеки:

– закріпити свої ринкові позиції шляхом створення позитивного іміджу в очах покупців і всієї спільноти користувачів інформаційних систем;

– зайняти нові ринкові ніші, що ставлять більш суворі вимоги до рівня інформаційної безпеки, порівняно з масовим ринком (банківський сектор, урядові структури та ін.);

– забезпечити ефективну інтеграцію продуктів, що поставляються в різні інформаційні системи і бізнес-процеси;

– уникнути звинувачень (зокрема і судових позовів) з боку споживачів, чиї інформаційні системи могли б піддатися атакам.

Прийоми і методи управління інформаційною безпекою на цьому рівні в кожному випадку можуть бути різними і визначаються для кожної компанії-постачальника такими основними факторами:

– характеристиками продуктів, що поставляються на ринок;

– станом (кон'юнктурою) ринку інформаційно-технологічних продуктів такого типу і поведінкою конкурентів;

– політикою державних структур як щодо питань інформаційної безпеки взагалі, так і щодо окремих компаній-постачальників інформаційних систем;

– завданнями, цілями та основними способами використання користувачами продуктів, що поставляються;

– загальним станом справ у сфері інформаційної безпеки, інформаційної культури, розвитком і поширенням злочинності;

– формованою громадською думкою щодо питань інформаційної безпеки та окремих компаній-постачальників.

Організаційна робота у сфері інформаційної безпеки на рівні таких компаній розділяється на два основні піднапрями:

– організація роботи всередині компаній, спеціально спрямованої на забезпечення інформаційної безпеки продуктів, що випускаються;

– організація зовнішньої взаємодії зі споживачами, партнерами, державними структурами та іншими учасниками.

Внутрішня організаційна робота щодо забезпечення інформаційної безпеки продуктів, що виробляються і продаються, є невід'ємною частиною процесу проєктування, виробництва і маркетингової підтримки цих продуктів. Однак виділяються додаткові спеціальні заходи, здійснювані окремо від основних виробничо-збутових процесів у компаніях – великих виробниках інформаційних систем. Прикладами таких спеціальних організаційних заходів є створення спеціальних підрозділів, основним завданням яких є контроль за усуненням

наявних вразливостей і виконання супутніх функцій, а також навчання розробників спеціальним методам розробки програмного забезпечення та апаратних засобів, що не містять вразливостей.

Основні прийоми і методи зовнішньої організаційної роботи у сфері інформаційної безпеки на рівні великих компаній-постачальників інформаційних систем можуть бути такі:

– організація інформаційного обміну з користувачами продуктів, що випускаються – програмних і апаратних засобів (інформування про виявлені вразливості і способи їх усунення, отримання інформації про вразливості, виявлені користувачами, а також про інші проблеми, що виникають);

– організація діяльності у сфері підготовки фахівців (система підготовки кваліфікованого інженерно-технічного персоналу, що спеціалізується на певних програмних продуктах, зокрема на адмініструванні засобів захисту інформації, мережевих операційних систем тощо);

– організація професійних конференцій, які сприяють обміну досвідом та інформацією, пов'язаною з підвищенням рівня інформаційної безпеки під час використання певних програмних і апаратних платформ;

– організація взаємодії з урядовими організаціями (зокрема з питань сертифікації програмних і апаратних засобів на відповідність вимогам національних стандартів і правил);

– створення і підтримка системи сертифікації фахівців, орієнтованої на певні програмні продукти та апаратні системи (у тому числі, організація взаємодії зі спеціалізованими компаніями, що займаються професійним тестуванням фахівців та ін.).

Організація інформаційного обміну з користувачами продуктів є одним з найбільш важливих напрямів діяльності компаній у цій сфері. Ця робота передбачає збір інформації, її аналіз, а також прийняття рішень про те, чи необхідно інформувати все співтовариство користувачів, яких може торкнутися виявлена уразливість, чи тільки обмежене коло довірених фахівців, що мають необхідні повноваження і авторитет. Подальші дії зазвичай пов'язані з повідомленням користувачів про можливі способи вирішення проблем (потенційних або тих, що вже виникли) та інформуванням про можливі наслідки реалізації загроз.

11.2. Організаційне забезпечення інформаційної безпеки на рівні окремих великих компаній

11.2.1. Корпорація Microsoft

Корпорація Microsoft є одним з найбільших у світі виробників програмного забезпечення. Її програмні продукти використовуються в усьому світі. Зокрема, Microsoft виробляє і постачає такі основні програмні засоби:

– операційні системи для робочих станцій (користувацьких персональних комп'ютерів) – молодші версії операційних систем Windows 2000, Windows XP, Windows Vista, Windows 7 і наступних;

– операційні системи для мережевих серверів (вебсерверів, серверів баз даних, файл-серверів та ін.) – Старші версії операційних систем Windows 2000, Windows XP і наступних;

– операційні системи для мінікомп'ютерів (PDA) – сімейства Windows CE, Windows Pocket PC, Windows Phone;

– спеціалізовані функціональні сервери: сервери реляційних баз даних (Microsoft SQL Server), вебсервери (IIS – Internet Information Server), системи побудови сховищ даних (Analysis Services) та деяких інших;

– засоби розробки додатків;

– користувацькі програмні продукти для платформи Windows: веббраузери, поштові клієнти, програми верстки у форматі HTML, офісні додатки, мультимедійні додатки та інші.

Також корпорацією Microsoft була придбана компанія, що займається поставками систем управління підприємствами (систем класу ERP – Enterprise Resource Planning).

Через те, що програмними продуктами Microsoft користується більшість користувачів персональних комп'ютерів (як приватних, так і в комерційних та урядових організаціях), а на основі серверних програмних платформ Microsoft функціонує більшість інформаційних систем, що забезпечують обробку, зберігання та передачу інформації (зокрема і в мережі Інтернет), організаційна робота цієї корпорації у сфері інформаційної безпеки має глобальне значення.

Внутрішня організаційна робота у сфері інформаційної безпеки продуктів корпорації Microsoft передбачає:

– проведення спеціальних тренінгів та додаткового навчання розробників програмного забезпечення спеціальним методам, що забезпечує надійність і безпеку виробленого програмного забезпечення (включно із впровадженням і використанням для розробки власних продуктів методології Життєвого циклу безпечної розробки);

– організацію спеціального Центру вирішення питань безпеки (Microsoft Security Response Center, MSRC), основними завданнями якого є постійний збір інформації та пошук нових вразливостей, вжиття заходів для усунення виявлених вразливостей, координація роботи розробників та недопущення появи раніше виявлених вразливостей у нових продуктах у майбутньому.

В організаційній структурі Microsoft, крім MSRC, існує ще один підрозділ, що спеціалізується на вирішенні питань безпеки – Центр захисту від шкідливих програм (Microsoft Malware Protection Center, MMPC). Він включає кілька лабо-

раторій, розташованих в усьому світі, і займається дослідженням шкідливих програм, забезпечує методичну підтримку розробки різних засобів захисту (Windows Live OneCare, Windows Defender, Malicious Software Removal Tool), а також бере участь у процедурах реагування на виникнення нових загроз безпеці.

Основними напрямами зовнішньої організаційної роботи корпорації Microsoft у сфері інформаційної безпеки є:

– систематичне інформування користувачів операційних систем Windows (а також інших програмних продуктів) про виявлені вразливості та поширення інформації про те, як ці уразливості можуть бути ними усунені;

– реалізація програми попереджувальних захисних дій – Microsoft Active Protections Program (MAPP);

– підтримка навчання користувачів програмних продуктів (в основному адміністраторів серверних платформ);

– розробка та підтримка методології Життєвого циклу безпечної розробки – Microsoft Security Development Lifecycle (SDL);

– партнерська програма Microsoft Security Partners – Партнери Microsoft в сфері безпеки;

– Government Security Program (GSP) – Програма забезпечення безпеки урядів;

– організація конференцій з різних аспектів використання програмних продуктів Microsoft;

– організація спеціального фонду для боротьби з хакерами;

– організація централізованої сертифікації своїх продуктів у державних органах;

– проведення власної конференції з безпеки.

Перший напрям – **організація інформування користувачів про виявлені вразливості** – будується на основі т. зв. Бюлетенів Безпеки («Security Bulletin»), що випускаються з певною періодичністю, а також після виходу спеціальних оновлень, що усувають виявлені вразливості (так званих «латок», patches). Порядок випуску цих бюлетенів, їх зміст та інші питання регулюються спеціальним організаційним документом – процедурою випуску Бюлетенів Безпеки (Security Bulletin Release Process). Також у межах цієї роботи організовано збір інформації про уразливості, що виявляються користувачами: на інтернет-сайті компанії розміщена спеціальна форма, заповнивши яку, кожен охочий може повідомити про нові самостійно виявлені вразливості в програмних продуктах.

Програма попереджувальних захисних дій – Microsoft Active Protections Program (MAPP) – являє собою систему прискореного інформування розробників систем безпеки (антивірусів, систем виявлення і запобігання вторгнень) про нововиявлені вразливості. Ця програма реалізується для того, щоб сторонні

розробники систем безпеки могли не чекати виходу чергового Бюлетеня Безпеки і якомога раніше почали розробляти механізми нейтралізації нових вразливостей на основі своїх програмних рішень. До участі у цій програмі допускаються розробники систем захисту на основі програмних платформ Microsoft, клієнтська база яких становить не менше 10 тисяч користувачів.

Підтримка системи навчання користувачів та адміністраторів реалізується декількома основними способами:

– цілеспрямована підготовка та опублікування навчальних посібників, довідників, статей та інших навчальних матеріалів, які містять пояснення, покрокові інструкції, приклади конфігурації і сценарії для установки програмних продуктів, зокрема і такі, які повинні забезпечити вирішення питань інформаційної безпеки;

– організація та методична підтримка системи професійного навчання та сертифікації фахівців з різних програмних продуктів (зокрема і адміністраторів мережевих операційних систем, баз даних та інших серверних продуктів, як-от Internet Security and Acceleration Server). Така підтримка включає в себе сертифікацію викладачів навчальних центрів, сертифікацію самих навчальних центрів, а також встановлення партнерських відносин з організаціями, що займаються професійним навчанням і професійним тестуванням адміністраторів і розробників інформаційних систем;

– проведення безкоштовних семінарів для адміністраторів операційних систем, присвячених питанням забезпечення інформаційної безпеки (зокрема функціональним можливостям тих чи інших програмних продуктів, що забезпечує вирішення певних питань захисту інформації).

Одним із напрямів інформаційної та методичної підтримки спільноти фахівців є просування і популяризація серед розробників інформаційних систем методології **Життєвого циклу безпечної розробки – Microsoft Security Development Lifecycle (SDL).** Ця методологія являє собою набір універсальних методичних, технічних і організаційних рекомендацій і прийомів, що у сукупності забезпечують істотне підвищення рівня безпеки розроблюваного ПЗ. Так, за твердженням Microsoft, після впровадження цієї методології вдалося знизити загальна кількість вразливостей, виявлених в SQL Server протягом трьох років після випуску продукту на ринок, на 91 % (якщо в MS SQL 2000 було виявлено 34 вразливості, то в MS SQL 2005 – всього 3 вразливості).

Просування цієї методології в середовищі розробників інформаційних систем включає в себе:

– опублікування і постійний розвиток самої методології;

– організацію професійного співтовариства (SDL Pro Network), яке об’єднує консалтингові компанії та навчальні центри, що спеціалізуються на питаннях безпеки;

– розробку та розповсюдження шаблонів для середовища розробки Visual Studio, що підтримують виконання положень методології.

Microsoft Security Partners – програма побудови партнерських відносин з різними незалежними компаніями, що працюють у сфері інформаційної безпеки. Ця програма розвивається за кількома самостійним напрямами:

– Antivirus Partners – партнерство у створенні антивірусних і захисних програм, а також в обміні актуальною інформацією про нові віруси, які впливають на різні продукти Microsoft. У цій програмі беруть участь такі фірми Symantec, ДіалогНаука, Лабораторія Касперського, Panda Software та інші (всього приблизно 20 різних компаній);

– Альянс SecureIT – партнерство з розробниками рішень у сфері безпеки (VeriSign, Trend Micro, Symantec та ін.) щодо спільної розробки нових засобів в цій галузі. Члени альянсу отримують від Microsoft і один від одного закриту інформацію про нові розробки, що дає змогу створювати інтегровані і взаємодіючі рішення;

– ISA Server Partners – партнерство з розробниками програмних і апаратних рішень, адаптованих для платформи Internet Security and Acceleration Server;

– Microsoft Windows Rights Management Services Partners – Партнерство з компаніями-розробниками програмних продуктів, розробниками апаратних засобів ідентифікації та системними інтеграторами у питаннях більш повного використання функціональних можливостей ОС Windows, пов'язаних з управлінням правами користувачів і доступом до інформаційних ресурсів. Ця програма включає в себе три категорії партнерів: Незалежних постачальників ПЗ, Розробників інфраструктурних рішень і Системних інтеграторів.

Government Security Program (GSP) – програма забезпечення безпеки урядів – являє собою ініціативу з передачі урядовим структурам різних країн вихідних кодів програмних продуктів (в основному операційних систем) для того, щоб у фахівців та експертів була можливість переконатися у відсутності істотних вад у цьому програмному забезпеченні. Такий аналіз повинен дати підстави для визнання цих програмних продуктів надійними з погляду інформаційної безпеки, а отже, – розширити можливості їх застосування різними організаціями (як урядовими, так і приватними). Також передбачається, що ця програма повинна допомогти усунути наявні недоробки в програмному забезпеченні і розширити партнерство між Microsoft і урядами різних країн у сфері захисту інформації. У межах програми експертам, що беруть у ній участь, також надається доступ до документації, довідкові матеріали, спеціальні засоби для роботи з вихідними кодами і підтримка з боку фахівців Microsoft. В цю програму включено приблизно 60 країн, що відповідають певним вимогам щодо захисту прав на інтелектуальну власність.

Однією з можливих причин початку реалізації цієї програми стало те, що деякі уряди (наприклад, Німеччини) заявили про можливий перехід урядових і муніципальних установ на альтернативні операційні системи (наприклад, Linux), для яких доступні вихідні коди. Розвиток цієї тенденції в перспективі міг призвести (і частково вже призвів) до певної втрати ринків збуту продукції Microsoft.

Централізована сертифікація програмних продуктів у державних органах є для корпорації Microsoft одним з напрямів реалізації концепції розвитку захищених інформаційних систем і передбачає можливість використання програмного забезпечення цієї компанії в інформаційних системах, до яких ставляться особливі вимоги з погляду надійності та інформаційної безпеки.

Також Microsoft проводить роботу з сертифікації деяких своїх продуктів на відповідність стандарту Common Criteria for Information Technology Security Evaluation – універсального стандарту забезпечення інформаційної безпеки, офіційно визнаному багатьма державами. Останні покоління операційних систем пройшли сертифікацію за цим стандартом у грудні 2005 р.

Конференція з безпеки BlueHat проводиться з 2005 р. двічі на рік для обміну думками та ідеями з різних питань інформаційної безпеки. У ній беруть участь тільки фахівці, запрошені компанією Microsoft.

11.2.2. Корпорація Cisco Systems

Компанія Cisco Systems, заснована в 1984 р. групою фахівців Стенфордського університету, наразі є світовим лідером у виробництві обладнання для мереж передачі даних. На основі обладнання, виробленого цією компанією, функціонують глобальні мережі передачі даних, а також мережі багатьох урядових організацій і великих компаній.

Через те, що обладнання цієї компанії забезпечує функціонування більшості найбільш значимих і відповідальних мереж передачі даних, її організаційна підтримка вирішення питань інформаційної безпеки має глобальне значення.

До основних напрямів організаційної роботи компанії Cisco входять:

– підтримка мережі освітніх центрів – Мережева Академія Cisco – при різних навчальних закладах і підприємствах. Робота Мережевих академій в усьому світі забезпечує підготовку фахівців з адміністрування мереж та забезпечення мережевої безпеки і централізовано підтримується головним офісом, який здійснює підготовку викладачів, надає навчальні матеріали, веде облік слухачів, здійснює екзаменаційне тестування випускників, виписує міжнародні сертифікати тощо;

– організація та координація роботи постачальників різних компонентів інформаційної інфраструктури на основі програми Network Admission Control (NAC) – Управління Доступом в Мережу. В межах цієї програми, ініційованої

в 2003 р. спільно з провідними постачальниками антивірусів (Network Associates, Symantec і Trend Micro) і націленої на вирішення різних проблем інформаційної безпеки, Cisco планує реалізувати нові технічні рішення і підходи до забезпечення інформаційної безпеки, що ґрунтуються на власному мережевому обладнанні. Зокрема, кооперація з постачальниками програмних продуктів в межах цієї програми повинна дати змогу автоматично управляти підключенням комп'ютерів, що не відповідають певним вимогам (політикам) інформаційної безпеки;

– організація роботи Cisco Product Security Incident Response Team (PSIRT) – Групи реагування на інциденти, пов'язані з безпекою продуктів Cisco. Основним завданням цього підрозділу є збір інформації про виявлені вразливості, їх аналіз, а також координація робіт щодо їх усунення та запобігання негативним наслідкам;

– поширення інформації про виявлені вразливості і проблеми з безпекою.

Контрольні питання:

1. Назвіть основні прийоми зовнішньої організаційної роботи у сфері інформаційної безпеки на рівні великих компаній-постачальників інформаційних систем.

2. Назвіть основні прийоми внутрішньої організаційної роботи у сфері інформаційної безпеки на рівні великих компаній-постачальників інформаційних систем.

3. Організаційне забезпечення інформаційної безпеки на рівні Корпорації Cisco Systems.

4. Організаційне забезпечення інформаційної безпеки на рівні Microsoft.

ТЕМА 12
ОРГАНІЗАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ДЕРЖАВНОМУ РІВНІ: ПРАКТИКА США

Відповідно до загальної політики, а також наявної базової інфраструктури і сформованої практики державного управління в США протягом декількох років була організована і постійно вдосконалюється система державних органів, що здійснюють діяльність у сфері інформаційної безпеки: були створені спеціальні відомства та розширені завдання і повноваження наявних. Отже, в темі викладаються основні положення державної політики США у сфері інформаційної безпеки, а також описується структура і принципи діяльності основних державних органів, які працюють у цій сфері.

Ключові слова: *загроза інформаційній безпеці, обмін інформацією, оцінка вразливостей, інформаційні система, безпека персоналу.*

План

12.1. Загальна політика США у сфері інформаційної безпеки.

12.2. Структура органів державної влади, що забезпечують інформаційну безпеку в США.

12.3. Федеральні програми та ініціативи, підтримувані державою.

12.1. Загальна політика США у сфері інформаційної безпеки

Через те, що США володіють значним фінансовим, технологічним, науково-технічним і військовим потенціалом, а також приділяють велике значення посиленню національної безпеки, захисту цивільних прав та інтересів бізнесу, досвід цієї країни у сфері управління інформаційною безпекою є найбільш важливим для вивчення. Значимість управління інформаційною безпекою в США на державному рівні визначається також тим, що в цій країні сконцентровані найбільші фінансові компанії, дослідницькі установи та корпорації, які суттєво впливають на розвиток технологій, фінансову стабільність та економічний розвиток усього світового співтовариства.

Одним sз ключових напрямів розвитку інформаційної безпеки, як і в багатьох інших країнах, є забезпечення національної (державної) безпеки, зокрема безпеки інформаційних систем так званих «силових» відомств: збройних сил, зовнішньої розвідки та ін. Приблизно з 1992 р. основні зусилля з організації заходів у сфері інформаційної безпеки робилися Міністерством оборони США в межах концепції «Інформаційного протиборства», орієнтованої на вирішення завдань боротьби з системами управління збройними силами противника на різних рівнях та забезпечення безпеки і ефективності власних інформаційних

систем армії США. Подальший розвиток ця концепція отримала в 1996 р. у вигляді нового польового статуту армії США «Інформаційні операції».

Загалом початком сучасної цілеспрямованої систематичної організаційної діяльності у сфері інформаційної безпеки на національному рівні можна вважати видання директиви адміністрації Президента Білла Клінтона Presidential Decision Directive 63 (PDD 63) «Захист критично важливої інфраструктури» від 22 травня 1998 р. На цьому документі базується підписаний Біллом Клінтоном на початку 2000 р. «Загальнонаціональний план захисту інформаційних систем», який визначає основні напрями діяльності держави і всього суспільства у сфері забезпечення інформаційної безпеки.

Також у лютому 2003 р. адміністрацією президента Джорджа Буша-молодшого була опублікована «Національна стратегія досягнення безпеки в кіберпросторі» («National Strategy to Secure Cyberspace»), що описує п'ять пріоритетів у діяльності США щодо забезпечення інформаційної безпеки та основні завдання в межах цих пріоритетів на середньострокову і довгострокову перспективу.

Фактично ці документи можуть вважатися офіційною загальнонаціональною політикою США у сфері інформаційної безпеки, на основі якої будується вся система діяльності державної влади в цій області і структура державних органів, що забезпечують інформаційну безпеку в країні.

Відповідно до стратегії інформаційної безпеки основними державними пріоритетами в цій галузі є:

– становлення і розвиток національної системи реагування на події у сфері інформаційної безпеки;

– реалізація комплексної системи заходів щодо зменшення загроз інформаційній безпеці;

– забезпечення підготовки фахівців у сфері комп'ютерної безпеки та забезпечення відповідального ставлення всього населення країни до питань захисту інформації;

– забезпечення захисту інформаційних систем, що стосуються державних органів;

– розвиток різних форм кооперації (зокрема і міжнародної) у сфері забезпечення інформаційної безпеки.

Пріоритет 1. Розвиток системи реагування на події у сфері інформаційної безпеки передбачає, що швидке виявлення атак і своєчасний обмін інформацією про них у багатьох випадках можуть значно знизити збитки. Для реалізації цього пріоритету Стратегія передбачає такі основні заходи:

– розробку архітектури взаємодії як урядових, так і неурядових структур, яка забезпечила б реагування на інциденти;

– забезпечення як тактичного, так і стратегічного аналізу атак на інформаційні ресурси, а також оцінки їх вразливості;

– заохочення поширення приватними компаніями наявної у них інформації про загальний стан справ у сфері інформаційної безпеки.

Пріоритет 2. Реалізація програми усунення загроз для інформаційної безпеки і вразливостей в інформаційних системах передбачає, що наявність вразливостей у різних інформаційних системах сама по собі певною мірою обумовлює можливість атак на них, і відповідно є джерелом небезпек для елементів критично важливих об'єктів інфраструктури країни. Отже, усунення вразливостей є одним з найбільш важливих напрямів роботи щодо забезпечення інформаційної безпеки. Для забезпечення безпеки Стратегія передбачає реалізацію таких основних заходів:

– розширення можливостей проведення розслідувань комп'ютерних злочинів для подальшого запобігання можливим атакам;

– створення загальнонаціонального механізму для оцінки вразливостей з метою забезпечення більш повного розуміння негативних наслідків реалізації загроз та використання вразливостей;

– підвищення безпеки мережі Інтернет шляхом вдосконалення використовуваних протоколів і механізмів маршрутизації.

Пріоритет 3. Розвиток відповідального ставлення до питань інформаційної безпеки та підготовка кадрів у цій сфері передбачає, що джерелом багатьох вразливостей є недостатньо відповідальне ставлення деяких користувачів, системних адміністраторів і розробників інформаційних систем до питань захисту, їх недостатня обізнаність і інформованість у цій сфері. Для забезпечення безпеки Стратегія передбачає реалізацію таких чотирьох основних заходів:

– просування багатосторонньої загальнонаціональної програми з інформування та розвитку відповідального ставлення громадян країни до забезпечення безпеки тих інформаційних систем, до яких вони мають будь-який доступ;

– заохочення створення програм підготовки фахівців, які забезпечили б задоволення потреби в персоналі;

– підвищення ефективності наявних програм підготовки фахівців у сфері інформаційної безпеки;

– підтримка зусиль приватних компаній зі створення, розповсюдження і забезпечення загального визнання сертифікаційних програм у сфері інформаційної безпеки.

Пріоритет 4. Охорона державних інформаційних ресурсів. Для вирішення завдань у цій сфері Стратегія передбачає реалізацію таких основних заходів:

– забезпечення безперервного оцінювання загроз для державних інформаційних систем та наявних у них вразливостей;

– забезпечення безпеки локальних урядових бездротових мереж;

– забезпечення безпеки під час передачі процесів на аутсорсинг і проведення закупівель для урядових потреб.

Пріоритет 5. Розвиток кооперації між різними відомствами та компаніями, а також міжнародної кооперації у сфері забезпечення інформаційної безпеки обумовлено тим, що практично всі інформаційні системи (і в країні, і у світі) є взаємопов'язаними і вимагають глобального системного підходу до питань захисту інформації. Для вирішення завдань у цій сфері Стратегія передбачає реалізацію таких основних заходів:

– посилення контррозвідувальної діяльності у сферах, які стосуються інформаційних систем і технологій;

– заохочення створення національних і міжнародних мереж спостереження і попередження («watch-and-warning networks»), що забезпечують виявлення і попередження атак на інформаційні ресурси;

– заохочення приєднання інших країн до Конвенції Ради Європи з кіберзлочинів або вдосконалення національних законодавств.

12.2. Структура органів державної влади, що забезпечують інформаційну безпеку в США

Відповідно до загальної політики, а також наявної базової інфраструктури і сформованої практики державного управління в США протягом декількох років була організована і постійно вдосконалюється система державних органів, що здійснюють діяльність у сфері інформаційної безпеки. Одним з основних підрозділів президентської адміністрації, спеціально створених для вирішення завдань інформаційної безпеки, є Комітет з національних систем безпеки (Committee on National Security Systems, CNSS).

Також у системі виконавчої влади були створені нові окремі федеральні установи, пріоритетними завданнями яких є вирішення завдань безпеки держави і вирішення проблем інформаційної безпеки на федеральному рівні:

– Міністерство національної безпеки (Department of Homeland Security, DHS);

– Управління внутрішньої безпеки (Office of Homeland Security);

– Рада з внутрішньої безпеки (Homeland Security Council).

Включення функцій із забезпечення інформаційної безпеки до складу функцій Міністерства національної безпеки та інших аналогічних установ пояснюється тим, що атаки на інформаційну інфраструктуру потенційно можуть спричинити негативні наслідки для різних життєво важливих галузей економіки США: фінансового сектору, енергетики, транспорту.

До того ж у межах окремих федеральних міністерств і відомств були створені спеціальні підрозділи, що вирішують окремі завдання в межах загальної стратегії забезпечення інформаційної безпеки США:

– Група готовності до надзвичайних ситуацій в інформаційних системах – United States Computer Emergency Readiness Team, US-CERT (підрозділ, що функціонує в складі DHS);

– Армійський центр безпеки і підтримки роботи глобальних мереж – Army Global Network Operations and Security Center, AGNOSC (підрозділ, що функціонує в складі Міністерства оборони США);

– Агентство оборонних інформаційних систем Міністерства оборони США (DISA), під управлінням якого перебуває Об'єднаний центр забезпечення роботи комп'ютерних мереж – Joint Task Force for Computer Network Operations, JTF-CNO;

– Центральна служба безпеки (Central Security Service, CSS) Агентства національної безпеки, National Security Agency-NSA.

Отже, загальна організаційна структура державного управління у сфері інформаційної безпеки в США є складною й утворюється з безлічі самостійних і водночас взаємопов'язаних елементів, основні з яких представлені на рис. 12.1.

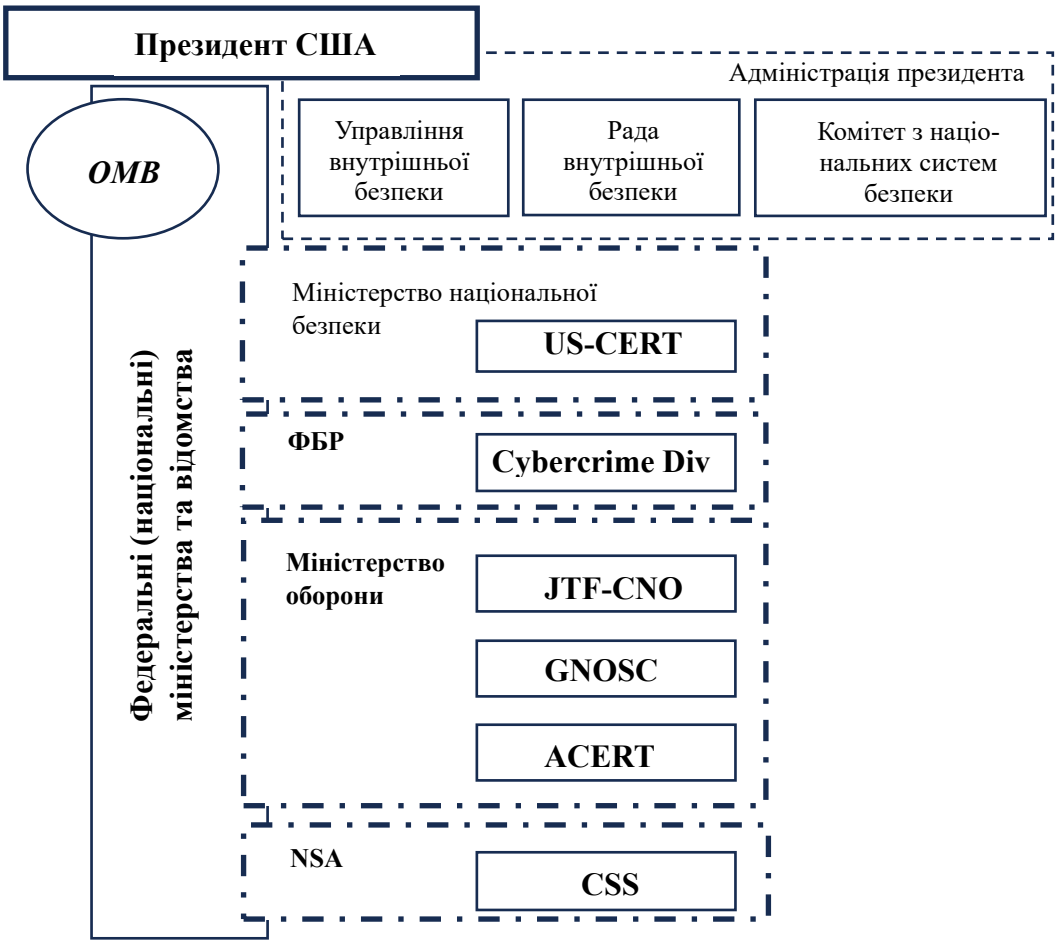

Рисунок 12.1. Структура органів управління виконавчої влади, що вирішують завдання щодо забезпечення інформаційної безпеки США

Комітет з національних систем безпеки (Committee on National Security Systems, CNSS) складається з 21 члена і 11 спостерігачів з-поміж фахівців різних федеральних відомств. Робота Комітету проводиться в рамках декількох робочих груп. Цей комітет формує централізовану державну політику щодо окремих технологій і методів, важливих для захисту інформаційної інфраструктури на загальнонаціональному рівні. Зокрема, робота ведеться за такими напрямами:

– управління ризиками;

– засоби ідентифікації користувачів і пристроїв;

– стійкість мережевої інфраструктури;

– розвиток системи підготовки кадрів у сфері інформаційної безпеки;

– забезпечення надійності розширення спільного доступу до інформаційних ресурсів.

Основними інструментами досягнення цілей у цих напрямах є:

– розвиток національної політики у сфері інформаційної безпеки, а також розробка стандартів;

– оцінка рівня розвиненості наявних і використовуваних засобів захисту інформації;

– випуск директив, інструкцій і технічних бюлетенів з певних проблем інформаційної безпеки;

– встановлення нових урядових структур для вирішення спеціалізованих завдань;

– участь у регулюванні експорту засобів захисту інформації.

Міністерство національної безпеки (Department of Homeland Security, DHS), створене в процесі найбільшої реорганізації державного апарату як самостійний постійно діючий орган федеральної влади, разом з вирішенням різних завдань, пов'язаних з безпекою США (як-от протидія тероризму та зовнішнім загрозам, а також запобігання наслідків стихійних лих), покликане виконувати такі основні функції у сфері інформаційної безпеки:

– розробка і вдосконалення загальнонаціонального плану щодо забезпечення безпеки ключових ресурсів та елементів інфраструктури Сполучених Штатів;

– здійснення управління кризовими ситуаціями під час атак на найбільш важливі інформаційні системи;

– надання технічної підтримки приватним компаніям і різним урядовим організаціям для усунення наслідків збоїв під час порушень роботи критично важливих інформаційних систем;

– координація дій з федеральними структурами з метою своєчасного оповіщення різних підприємств і організацій про загрози, що виникають, та заходи, які необхідно вжити;

– виконання, а також фінансування науково-дослідних робіт, необхідних для вирішення завдань внутрішньої безпеки.

Функції забезпечення інформаційної безпеки належать Управлінню кібербезпеки і комунікацій (Office of Cyber Security and Communications). У складі цього управління функціонує підрозділ, безпосередньою функцією якого є вирішення проблем, пов'язаних з інформаційною безпекою, – National Cyber Security Division, в який, включений USCERT.

Група готовності до надзвичайних ситуацій в інформаційних системах (United States Computer Emergency ReadinessTeam, US – CERT) є центральним цілодобово функціонуючим органом, що відповідає за взаємодію з урядовими структурами (як федеральними, так і місцевими), а також іншими суб'єктами з питань захисту інформації. Її основним завданням є збір та поширення інформації з метою реагування на інциденти, підвищення рівня скоординованості дій, зниження рівня вразливості.

Група включає в себе п'ять підрозділів:

– Відділ поточної діяльності (Operations branch). Відповідає за обробку одержуваної інформації про інциденти, забезпечує реагування на інциденти, поширює необхідну інформацію, а також забезпечує аналіз різних даних з метою підвищення якості оцінки відомих або нових загроз для критично важливих елементів національної інфраструктури (включно з аналізом мережевої інфраструктури, шкідливого ПЗ тощо).

– Відділ ситуаційної поінформованості (Situational Awareness branch). Відповідає за комплексний аналіз мережевої активності (тенденцій і характеру змін завантаження магістральних мереж) та інформування федеральних структур з метою підвищення рівня їх захищеності. Також забезпечує підтримку у вирішенні інцидентів.

– Слідчий відділ (Law Enforcement and Intelligence branch). Забезпечує взаємодію з правоохоронними органами за умов виявлення і розслідування протизаконних дій.

– Відділ перспективного розвитку (Future Operation branch). Відповідає за розробку перспективних планів, процедур, регламентів, що забезпечують роботу US-CERT з реагування на інциденти.

– Відділ підтримки (Mission Support branch). Забезпечує підтримку засобів комунікації, необхідних для роботи USCERT, включно підтримку вебсайта, а також відповідає за адміністративну підтримку, безпеку персоналу, постачання та інші допоміжні функції.

Крім забезпечення роботи US-CERT, Міністерство національної безпеки також виконує роботу за такими напрямами:

– проводить періодичні (раз на два роки) навчання **Cyber Storm** з метою перевірки готовності до надзвичайних ситуацій у сфері інформаційної безпеки;

– проводить щорічний інформаційно-освітній місячник з кібербезпеки;

– координує роботу групи з 13 федеральних відомств (включно з розвідкою, правоохоронними структурами і US-CERT) на випадок виникнення інцидентів загальнонаціонального масштабу;

– підтримує систему інформаційного обміну між працівниками правоохоронних органів з метою виявлення та розшуку злочинців, які вчинили кіберзлочини **(Cyber Cop Portal).**

Агентство оборонних інформаційних систем (Defense Information Systems Agency, DISA) Міністерства оборони США виконує безліч функцій, пов'язаних з підтримкою військових інформаційних систем, зокрема функції, пов'язані із забезпеченням їх надійності і безпеки.

Директору DISA підпорядковується **Об'єднаний центр забезпечення роботи комп'ютерних мереж** (Joint Task Force for Computer Network Operations, JTF-CNO1) Міністерства оборони США, створений як єдиний центр координації дій із захисту Оборонної інформаційної інфраструктури.

Основними завданнями JTF-CNO є:

– виявлення вторгнень в інформаційні системи підрозділів Міністерства оборони та інших відомств;

– аналіз виявлених вторгнень у контексті поточної військової обстановки з урахуванням наявної розвідувальної інформації;

– оцінка впливу вторгнень у функціонування інформаційних мереж і військові операції;

– підготовка плану дій з відновлення роботи комп'ютерних мереж;

– координація необхідних дій з різними підрозділами Міністерства оборони та іншими відомствами;

– самостійне здійснення конкретних заходів щодо забезпечення безпеки інформаційних систем.

До складу сил, відповідальних за інформаційну безпеку армії США, також входять:

– Перше командування інформаційними операціями американської армії (US Army's 1st Information Operations Command (LAND) (1ST IOC [L])), раніше відоме як Підрозділ з наземних військових інформаційних операцій (Land Information Warfare Activity, LIWA);

– Морське командування оборонними операціями в кіберпросторі (Navy Cyber Defense Operations Command);

– Армійський центр реагування на загрози інформаційній безпеці (ACERT).

Крім перерахованих функцій органів федеральної влади, державна політика інформаційної безпеки також наказує іншим установам надавати необхідне сприяння вирішенню проблем інформаційної безпеки:

– Національному науковому фонду – надавати фінансову підтримку наукових досліджень у сфері інформаційної безпеки;

– Державному департаменту – надавати різним органам необхідне сприяння під час здійснення міжнародного співробітництва у сфері інформаційної безпеки;

– Центральному розвідувальному управлінню – протистояти проникненням в інформаційні системи з-за кордону;

– Національному інституту стандартів (NIST), в особі Управління з комп'ютерної безпеки, що складається з чотирьох груп, – розробляти необхідні стандарти в сфері інформаційної безпеки;

– Міністерству оборони – надавати технічне сприяння під час розробки та впровадження систем захисту інформації;

– Міністерству юстиції та Федеральному бюро розслідувань – забезпечувати ефективне розслідування і припинення кіберзлочинів, а також здійснювати юридичну підтримку органів федеральної влади під час вирішення різних питань, пов'язаних з інформаційною безпекою.

Також Адміністративно-бюджетне управління (Office of Management and Budget, OMB) уповноважене здійснювати нагляд за впровадженням заходів інформаційної безпеки (застосуванням політик безпеки, відповідністю чинним стандартам, виконанням різних вимог тощо) у всіх федеральних органах влади за винятком органів державної безпеки.

Отже, з опису функцій різних відомств, що входять у систему виконавчої влади США, зрозуміло, що частина з них формує загальну політику і координує дії на рівні міністерств, частина – вирішує питання методичної та технічної підтримки процесів захисту інформації, а частина – виконує повсякденну роботу, пов'язану з розв'язанням окремих інцидентів і вдосконаленням окремих систем захисту інформації.

У складі **законодавчої гілки влади – Конгресу США** – основним структурним підрозділом, відповідальним за вирішення проблем інформаційної безпеки, є один із 22 постійних комітетів Палати представників – Особливий комітет з національної безпеки (Select Committee on Homeland Security). Основним профільним підкомітетом є Підкомітет нових загроз, кібербезпеки і науки (Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology). У сферу його інтересів входять питання, пов'язані з безпекою комп'ютерних систем, телекомунікацій, інформаційних технологій, систем автоматичного управління в промисловості, а також питання запобігання внутрішніх і зовнішніх атак на урядові та приватні мережі, збитку, нанесеного цивільному населенню внаслідок атак на інформаційні системи.

Деякі слухання з питань інформаційної безпеки також може проводити Комітет з енергетики і торгівлі (Committee on Energy and Commerce). Зокрема, цими проблемами може займатися Підкомітет з телекомунікацій і мережі Інтернет (Subcommittee on Communications, Technologies, and the Internet).

До складу завдань Конгресу у сфері управління інформаційною безпекою, у всіх інших сферах державного управління, відповідно до Конституції країни входять:

– прийняття законодавства;
– прийняття бюджету та управління фінансами;
– контроль за діяльністю урядових установ;
– виконання квазісудових функцій;
– формування структури виконавчої та судової влади.

Однією з основних форм роботи Конгресу, зокрема Комітету з національної безпеки та Комітету з енергетики і торгівлі, є проведення спеціальних слухань і розслідувань. Слухання проводяться з метою визначення напрямів удосконалення законодавства, виявлення і припинення недоробок і порушень у роботі органів виконавчої гілки влади тощо. Конгрес може розглядати як питання, пов'язані з національною безпекою і інформаційною безпекою державних структур, так і проблеми інформаційної безпеки приватного сектора і громадян країни. Для участі в слуханнях із різних питань, пов'язаних з інформаційною безпекою, в Конгрес зазвичай запрошуються керівники та експерти, що представляють різні галузі діяльності:

– представники урядових установ, у чию компетенцію входить забезпечення інформаційної безпеки (як-от NSA та ін.);
– керівники великих приватних компаній, які є лідерами у виробництві інформаційних систем та наданні інформаційних послуг (Microsoft, ISS та інших);
– представники авторитетних науково-дослідних установ, консалтингових компаній, професійних та галузевих об'єднань (як-от Electronic Industries Alliance).

Діяльність комітетів і підкомітетів Конгресу підтримується Головним контрольним управлінням Конгресу (Government Accountability Office, GAO), до функціональних підрозділів якого входить спеціальна група, що займається питаннями інформаційних технологій та інформаційної безпеки (Information Technology Team). У список завдань цього підрозділу включені:

– вивчення стану інформаційної інфраструктури та інформаційної безпеки на різних рівнях і в різних урядових організаціях з метою усунення ризиків у їх діяльності;
– вивчення та просування передового досвіду («кращих практик») у сфері побудови надійних і безпечних інформаційних систем, а також сучасних інформаційних технологій, на основі яких такі системи можуть будуватися;

– оцінка окремих технологій захисту інформації з погляду їх можливого застосування в тих чи інших урядових структурах;

– контроль за обґрунтованістю бюджетних витрат на забезпечення інформаційної безпеки;

– вивчення можливостей практичного розвитку концепції так званого «Електронного уряду» (e-government).

На основі результатів своєї аналітичної роботи GAO може робити висновки, представляти аналітичні матеріали зацікавленим конгресменам, формулювати рекомендації тощо.

12.3. Федеральні програми та ініціативи, підтримувані державою

Крім організації роботи окремих відомств, одним з важливих напрямів діяльності держави є підтримка програм спільної діяльності у сфері інформаційної безпеки всіх державних установ, а також приватних компаній.

Однією з основних таких ініціатив є **Міжрегіональний Центр обміну та аналізу інформації (Multi-State Information sharing and analysis center, MS-ISAC),** який об'єднує структури, відповідальні за інформаційну безпеку, в урядах практично всіх штатів. Завдання цього об'єднання:

– обмін інформацією про інциденти;

– поширення практично випробуваних методів і прийомів забезпечення безпеки;

– поширення попереджень про нові загрози інформаційної безпеки.

До того ж однією з федеральних ініціатив є Національне партнерство з підвищення надійності інформації – **National Information Assurance Partnership, NIAP,** створене для підтримки розробки надійних IT-продуктів та перевірки інформаційних систем на відповідність міжнародним стандартам у сфері інформаційної безпеки. Завдання цієї структури:

– оптимізація витрат урядових і приватних структур на оцінку інформаційних систем;

– заохочення створення приватних структур, що займаються перевіркою безпеки інформаційних продуктів;

– підвищення доступності інформаційних систем, які пройшли належну перевірку на відповідність сучасним стандартам.

Також до загальнофедеральних програм належить **Інформаційна мережа для попереджень про загрози критичній інфраструктурі (Critical infrastructure Warning Information Network, CWIN),** основним завданням якої є надання можливості обміну попередженнями та передачі сигналів тривоги між урядовими організаціями, а також приватними компаніями і деякими зарубіжними партнерами. За задумом Міністерства національної безпеки, ця

мережа повинна забезпечити надійний зв’язок з різними суб’єктами, участь яких принципово необхідна для відновлення критично важливих об’єктів інфраструктури в разі надзвичайних подій національного масштабу.

Контрольні питання:

1. Назвіть ключові напрями розвитку інформаційної безпеки США.
2. Яка структура органів державної влади, що забезпечують інформаційну безпеку в США?
3. Який структурний підрозділ у складі законодавчої гілки влади США займається питаннями інформаційної безпеки?

ТЕМА 13
ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ДЕРЖАВНОМУ РІВНІ: ПРАКТИКА УКРАЇНИ

Державна політика національної безпеки в інформаційній сфері має створювати умови для реалізації конституційного права громадян своєї держави вільно отримувати і використовувати інформацію для вирішення важливих завдань формування національного інформаційного простору, включення його до світового інформаційного простору на засадах забезпечення інформаційного суверенітету та інформаційної безпеки і формування демократично орієнтованої свідомості. Головною метою державної політики національної безпеки в інформаційній сфері є створення необхідних економічних і соціокультурних умов, правових і організаційних механізмів формування, розвитку і забезпечення ефективного використання національних інформаційних ресурсів у всіх сферах життєдіяльності особи, суспільства і держави як організму. В темі розглянуто основні положення державної політики України у сфері інформаційної безпеки, а також описані структура і принципи діяльності основних державних органів, що працюють у цій сфері.

Ключові слова: *інформаційна безпека, об'єкт, суб'єкт, загроза, захист інформації, Держспецзв'язку.*

План

13.1. Визначення інформаційної безпеки, об'єкти, суб'єкти, основні складники.

13.2. Система забезпечення інформаційної безпеки.

13.3. Загрози інформаційній безпеці України у контексті діяльності Держспецзв'язку.

13.4. Історія створення Держспецзв'язку.

13.5. Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язку).

13.6. Організаційна структура Держспецзв'язку.

13.1. Визначення інформаційної безпеки, об'єкти, суб'єкти, основні складові

Під інформаційною безпекою розуміють складову частину національної безпеки, що характеризує стан захищеності національних інтересів в інформаційній сфері від зовнішніх та внутрішніх загроз. Суть інформаційної безпеки полягає у захисті інформаційного простору України від небажаного інформаційного впливу, захисті національних інформаційних ресурсів, забезпеченні безпечного функціонування інформаційних та телекомунікаційних систем, а також у захисті інформації, що циркулює в них.

До *об'єктів інформаційної безпеки* належать: свідомість, психіка людей або різноманітні інформаційні системи, які складають інформаційну інфраструктуру держави.

До *соціальних об'єктів інформаційної безпеки* належать: особистість, колектив, суспільство та держава – її конституційний лад.

До *суб'єктів інформаційної безпеки* належать:

– держава, що здійснює свої функції через відповідні органи державної влади шляхом створення системи забезпечення інформаційної безпеки;

– громадяни, суспільні або інші організації і об'єднання, що володіють повноваженнями із забезпечення інформаційної безпеки відповідно до законодавства.

На рис. 13.1 наведено основні складники інформаційної безпеки.

Основні цілі забезпечення інформаційної безпеки визначаються пріоритетами національної безпеки, що відповідають інтересам суспільного розвитку. Такими цілями є:

– забезпечення інформаційного суверенітету України в умовах глобалізації інформаційних відносин і прагнення інших країн до інформаційного домінування;

– формування інформаційного середовища, орієнтованого на духовний та інтелектуальний розвиток особи і суспільства загалом;

– підтримка необхідної достатності інформаційних ресурсів України, які забезпечують розвиток особи та стійке функціонування суспільства і держави;

– забезпечення захисту інформації фізичних, юридичних осіб та держави від зовнішніх і внутрішніх інформаційних загроз, зокрема боротьба з комп'ютерними злочинами;

– забезпечення законності і реалізація прав суб'єктів інформаційних відносин у галузі створення і використання національних інформаційних ресурсів, інформаційних технологій та інформаційної інфраструктури.

Як **основні системоутворюючі складники** інформаційної безпеки можна виділити:

– захист інформаційного простору;

– захист інформаційних ресурсів;

– захист інформації з обмеженим доступом.

Інформаційну безпеку можна класифікувати за її видами, відповідно до загроз, а саме:

– забезпечення безпеки діяльності, пов'язаної із забезпеченням свободи слова та доступу громадян до інформації;

– протидія поширенню засобами масової інформації культу насильства, жорстокості, порнографії;

Складники інформаційної безпеки

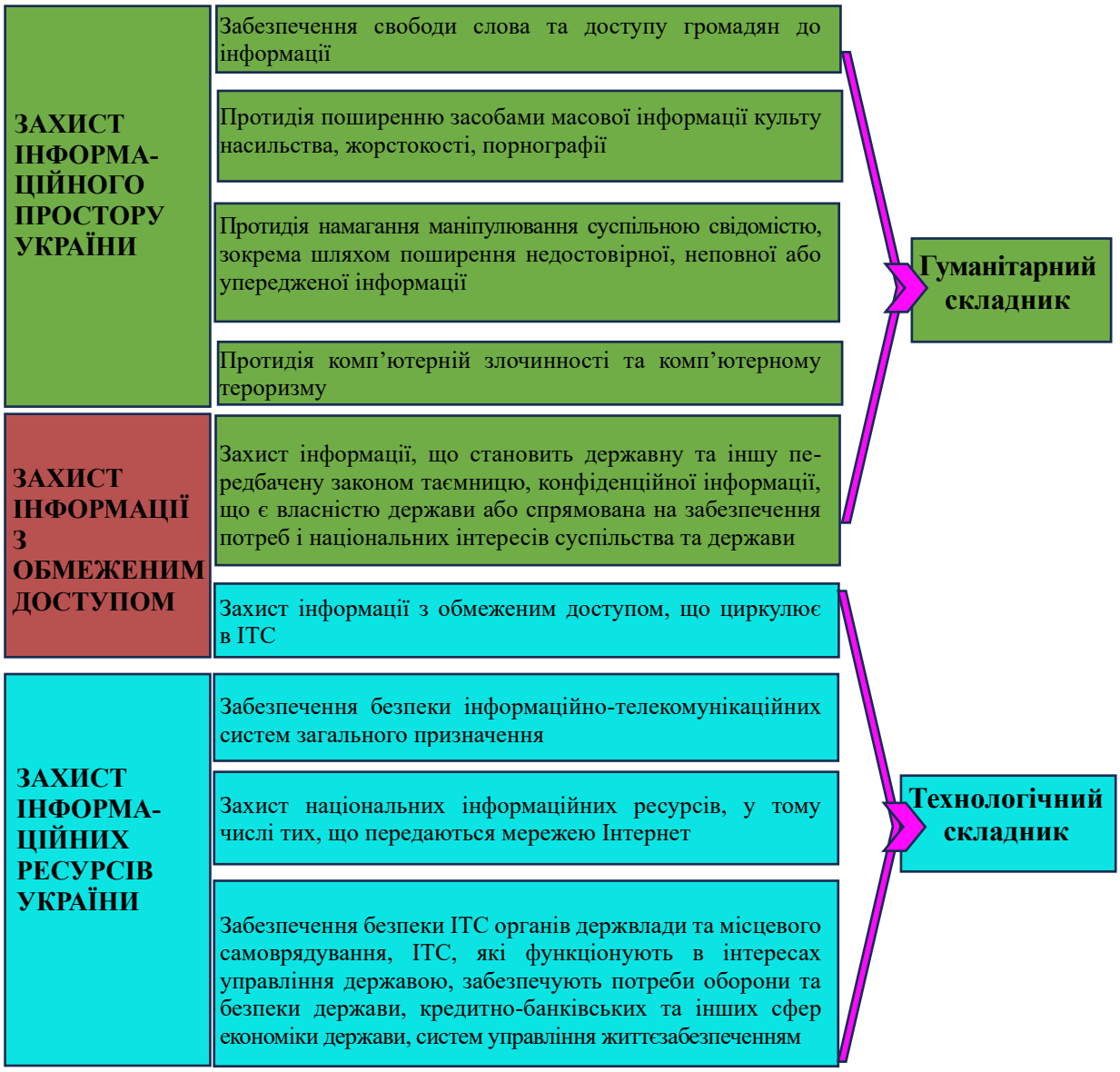

Рисунок 13.1. Складники інформаційної безпеки

– протидія намаганням маніпулювання суспільною свідомістю, зокрема шляхом поширення недостовірної, неповної або упередженої інформації;

– протидія комп'ютерній злочинності та комп'ютерному тероризму;

– забезпечення безпеки інформаційно-телекомунікаційних систем загального призначення;

– захист національних інформаційних ресурсів, у тому числі тих, доступ до яких здійснюється з використанням мережі Інтернет;

– забезпечення безпеки інформаційно-телекомунікаційних систем органів державної влади та місцевого самоврядування, інформаційно-телекомунікацій-

них систем, які функціонують в інтересах управління державою, забезпечують потреби оборони та безпеки держави, кредитно-банківських та інших сфер економіки держави, систем управління життєзабезпеченням;

– захист інформації, що становить державну та іншу передбачену законом таємницю, конфіденційної інформації, що є власністю держави або спрямованої на забезпечення потреб та національних інтересів суспільства та держави.

Державна політика у сфері інформаційної безпеки спрямована на накопичення та захист національних інформаційних ресурсів, розробку та впровадження сучасних безпечних інформаційних технологій, побудову захищеної національної інформаційної інфраструктури, формування і розвиток інформаційних відносини тощо. Вона повинна реалізовуватися шляхом створення і забезпечення ефективного функціонування в Україні цілісної системи інформаційної безпеки, а також вдосконалення наявної і розробки нової нормативно-правової бази, яка регулює відносини в сфері інформаційної безпеки, встановлює вимоги і правила провадження діяльності у цій сфері.

13.2. Система забезпечення інформаційної безпеки

Система забезпечення інформаційної безпеки – організована державою сукупність державних органів, посадових осіб, громадських організацій, окремих громадян, об'єднаних цілями та завданнями захисту національних інтересів України в інформаційній сфері, які реалізують державну політику та здійснюють узгоджену діяльність у межах законодавства України. Основними функціями системи забезпечення інформаційної діяльності є:

– створення та забезпечення діяльності державних органів – елементів системи;

– управління діяльністю системи;

– міжнародне співробітництво в сфері інформаційної безпеки.

Основними елементами системи забезпечення інформаційної безпеки України є:

– громадяни України;

– Верховна Рада України;

– Комітет Верховної Ради України з питань національної безпеки і оборони;

– Комітет Верховної Ради України з питань свободи слова та інформації;

– Комітет Верховної Ради України з питань транспорту і зв'язку;

– Президент України;

– Національний інститут стратегічних досліджень;

– Рада Національної безпеки і оборони України.

Безпосередньо РНБО України підпорядковуються:

– Інститут проблем національної безпеки та Національний інститут проблем міжнародної безпеки;

– Апарат Ради національної безпеки і оборони України;

– Кабінет Міністрів України. У складі Секретаріату Кабінету Міністрів України діє Управління стратегії розвитку інформаційних ресурсів та технологій;

– Урядова комісія з питань інформаційно-аналітичного забезпечення діяльності органів виконавчої влади;

– Національна комісія з питань регулювання зв'язку України;

– Міністерство освіти та науки України. У складі Міністерства освіти та науки України діє Державний департамент інтелектуальної власності;

– Державний комітет інформаційної політики, телебачення та радіомовлення;

– Державний комітет архівів;

– Державний комітет статистики України;

– Служба безпеки України;

– Державна служба спеціального зв'язку та захисту інформації України;

– Міністерство внутрішніх справ України. У складі – відділ боротьби з правопорушеннями у сфері високих технологій Державної служби боротьби з економічною злочинністю;

– Національна Рада України з питань телебачення та радіомовлення;

– Конституційний Суд України;

– суди загальної юрисдикції;

– генеральна прокуратура України;

– органи місцевого самоврядування;

– інші державні органи та організації;

– засоби масової інформації;

– політичні партії та рухи;

– громадські організації та професійні спілки;

– неурядові дослідницькі організації;

– організації та установи, що здійснюють діяльність в інформаційній сфері.

Загалом, в Україні створена й функціонує структурно повна система забезпечення інформаційної безпеки. Функції та повноваження відповідних державних органів закріплені в нормативно-правових актах різного рівня – у Конституції України, законах України, указах Президента України, постановах Кабінету Міністрів України, інших, зокрема відомчих, нормативних актах. Водночас розподіл функцій між окремими суб'єктами системи та схема їх взаємодії потребують вдосконалення.

Інформаційна безпека є невід'ємним напрямом розбудови інформаційного суспільства, розвиток якого повинен іти не тільки через нарощування технологічних можливостей здійснення інформаційного обміну, але й через глибоке усвідомлення усіма суб'єктами інформаційних відносин – власниками інформації та її користувачами, виробниками інформаційних технологій і засобів,

постачальниками послуг, державою – необхідності здійснення всіх заходів щодо захисту інформаційних ресурсів та забезпечення інформаційної безпеки держави.

Актуальність вирішення проблеми захисту інформаційних ресурсів обумовлюється зростанням доступу до мереж загального користування окремих категорій протиправно налаштованих категорій громадян, певною вразливістю окремих мереж, зростання попиту з боку злочинних елементів на здобування або руйнування інформації, що циркулює в спеціальних мережах зв'язку, системах управління військами та озброєнням, на блокування публічних державних інформаційних ресурсів у мережі Інтернет, інформаційних ресурсів об'єктів критичної інфраструктури, а також вразливістю загальних ефірних теле- та радіоканалів громадського мовлення. Все це свідчить про необхідність надійного захисту вказаних об'єктів та потребує подальшого розвитку системи криптографічного та технічного захисту інформації в державі, розробки та вдосконалення нормативно-правового підґрунтя діяльності у сфері забезпечення безпеки інформації.

В Україні захист інформації розглядається як система правових, організаційних, технічних та інших заходів, спрямованих на забезпечення збереження не тільки інформації з обмеженим доступом, а й відкритої інформації, необхідність захисту якої визначається законом. Ці заходи поширюються також на інформаційні ресурси, системи та технології, на засоби їх забезпечення. Вони призначені для підтримки інформації у такому стані, за якого вона зберігає свою фізичну та логічну цілісність, доступність (неможливість блокування) і використовується відповідно до встановленого регламенту.

Як свідчить досвід, ефективно вирішувати завдання щодо захисту інформації, що циркулює в інформаційних та телекомунікаційних системах, а також забезпечити надійний захист інформаційно-телекомунікаційних систем державних органів від злочинних посягань (зокрема і з-за меж України) можна лише шляхом створення в їх складі комплексних систем захисту інформації, що поєднують правові, організаційні, інженерні заходи, а також технічні і програмні засоби захисту. Тобто одним, чи не найголовнішим чинником процесу створення системи забезпечення безпеки інформації в Україні стає розробка та вдосконалення правового підґрунтя діяльності у цій сфері, і зокрема такої нормативної бази, яка б, враховуючи вимоги сучасності, регламентувала суспільні відносини у сфері захисту інформації та забезпечення безпеки її під час інформаційного обміну. Причому процеси формування та вдосконалення нормативно-правової бази системи захисту інформації проходять як шляхом внесення змін до наявних, так і шляхом розробки нових нормативно-правових актів. Водночас вони повинні відповідати вимогам щодо гармонізації українського законодавства з міжнародним законодавством і законодавством ЄС, вони мають створити для України можливість стати рівноправним учасником міжнародного інформаційного обміну за умов збереження інформаційного суверенітету нашої країни.

13.3. Загрози інформаційній безпеці України у контексті діяльності Держспецзв'язку

Сьогодні законодавством України визначено основні загрози національній безпеці України, зокрема в інформаційній сфері. До **загроз національній безпеці** в інформаційній сфері, серед інших, віднесено:

– прояви обмеження свободи слова та доступу громадян до інформації;

– комп'ютерна злочинність та комп'ютерний тероризм;

– розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави, або спрямованої на забезпечення потреб та національних інтересів суспільства і держави;

– намагання маніпулювати суспільною свідомістю, зокрема шляхом поширення недостовірної, неповної або упередженої інформації.

До зовнішніх факторів, які формують пріоритети і стратегічні цілі політики національної безпеки з урахуванням ролі та важливості інформаційного складника, необхідно віднести:

– посилення загроз національній безпеці, серед яких – прагнення низки країн та транснаціональних об'єднань до домінування у світовому інформаційному просторі, що призводить до обмеження інтересів України;

– витіснення України із зовнішнього та внутрішнього інформаційних ринків;

– формування негативного іміджу України у світі шляхом поширення інформації, яка не відповідає дійсності;

– діяльність міжнародних терористичних організацій, а також окремих осіб і груп, схильних до деструктивної інформаційної діяльності;

– діяльність іноземних політичних, економічних, військових, розвідувальних й інформаційних структур, яка має спрямування до інтересів України в інформаційній сфері.

До того ж суттєвим зовнішнім фактором, що характеризує середовище формування пріоритетів національної безпеки, є глобалізація інформаційного обміну та невідповідність інформаційної інфраструктури України та рівня її розвитку та захищеності вимогам сучасності.

Серед внутрішніх факторів, які стають внутрішніми загрозами національній безпеці держави з позиції формування стратегічних напрямів діяльності щодо забезпечення її інформаційної безпеки, є:

– Помітне відставання України від провідних держав світу в галузі створення і впровадження сучасних інформаційних технологій, у сфері розвитку індустрії інформаційних послуг та, як наслідок, вимушене широке використання закордонних програмно-технічних засобів обміну інформацією та її захисту під час розбудови національної інформаційної інфраструктури.

Наслідком такого відставання може стати реалізація стратегій інформаційного протиборства проти України, поява реальної можливості несанкціонованого проникнення в інформаційні системи та бази даних, блокування систем та мереж, особливо тих, що функціонують в інтересах управління державою.

– Недостатній рівень захищеності державних інформаційних ресурсів, розповсюдження комп'ютерних вірусів, програмних та апаратних закладок спричиняють появу реальної можливості втрати стратегічно важливої інформації, порушення її цілісності та блокування доступу до неї. До того ж це може призвести до порушення нормального функціонування систем управління об'єктами критичної інфраструктури.

Протягом останніх років спостерігається стійка тенденція до різкого збільшення загроз із погляду кількості спроб несанкціонованого втручання в роботу інформаційних та телекомунікаційних систем і несанкціонованого доступу до інформації, яка в них циркулює, а також появи нових методів та алгоритмів щодо їх здійснення. Зазначене являє собою реальну загрозу національному інформаційному простору України і в разі неприйняття необхідних заходів може призвести у найближчому майбутньому до втрати державою контролю над частиною її інформаційного простору та, відповідно, неможливості забезпечення прав громадян у цій сфері.

– Недостатня узгодженість діяльності державних органів України щодо формування і реалізації єдиної державної політики забезпечення інформаційної безпеки, порушення встановлених режимів функціонування інформаційно-телекомунікаційних систем органів державної влади та місцевого самоврядування, інформаційно-телекомунікаційних систем, які забезпечують потреби оборони і безпеки держави, кредитно-банківської та інших сфер економіки держави, систем управління життєзабезпеченням;

– Об'єктивна неспроможність промисловості України задовольнити попит на сучасне комп'ютерне обладнання та обладнання зв'язку сприяє широкому застосуванню закордонних засобів обчислювальної і комунікаційної техніки.

Ці загрози як фактори формування державної політики у безпековому секторі держави необхідно врахувати під час підготовки стратегій та концепції забезпечення національної безпеки Україні, моделі сектору безпеки України, що сприятиме гармонічному розвитку безпекового сектору, та приведенню його до європейських стандартів.

Як свідчить досвід провідних країн світу, ефективна діяльність у сфері забезпечення інформаційної безпеки повинна проходити шляхом нарощування потужностей тих структур, на які покладено реалізацію державної політики за основними, технологічними її складниками: заходів щодо захисту інформаційних ресурсів, захисту інформації, забезпечення безпеки інформаційного обміну. Це

дає змогу не тільки створити додаткові важелі впливу на процеси реалізації державної політики у сфері інформаційної безпеки, але й забезпечити в умовах подальшої демократизації суспільства відкритість заходів, що впроваджуються для підтримання та забезпечення інформаційної безпеки особи, суспільства і держави.

13.4. Історія створення Держспецзв'язку

Проблемам забезпечення безпеки інформації, захисту інформаційного простору України від небажаного інформаційного впливу, забезпеченню безпечного функціонування інформаційно-телекомунікаційних систем та захисту інформації, що циркулює в них, приділялась серйозна увага з перших днів існування української держави. Вже наступного дня після проголошення Декларації про незалежність України було прийнято рішення щодо прийняття під юрисдикцію України захищених видів зв'язку. Прийнятим у березні 1992 р. Законом України «Про Службу безпеки України» було законодавчо визначено порядок забезпечення засекреченим і шифрованим зв'язком державних органів України та відповідних посадових осіб.

Політичні, економічні та соціальні зміни, які проходили у нашому суспільстві, вимагали розробки нових підходів до розвитку та удосконалення спеціальних систем зв'язку та захисту інформації. З метою найшвидшого і якісного вирішення цього завдання діюче на той час Управління урядового зв'язку, яке забезпечувало лише експлуатацію регіональної частини союзної системи спеціального зв'язку, було реорганізовано в Головне управління урядового зв'язку СБ України (ГУУЗ СБУ), основним завданням якого стало створення власної системи урядового зв'язку суверенної держави.

Протягом порівняно короткого періоду ГУУЗ поступово було перетворено успадкований фрагмент системи урядового зв'язку в цілісну Державну систему урядового зв'язку – систему спеціального зв'язку, яка забезпечує передачу інформації, що містить державну таємницю та функціонує в інтересах управління державою як у мирний, так і у воєнний час. Необхідно зазначити, що і на цей час державна система урядового зв'язку залишається тією єдиною телекомунікаційною системою, яка за своїми характеристиками та організацією здатна на належному рівні виконувати головне своє призначення: забезпечувати надійним, безперебійним, захищеним зв'язком Верховного Головнокомандувача Збройних Сил України з командуванням Збройних Сил України у мирний та воєнний час, забезпечувати спеціальними видами зв'язку вищих посадових осіб держави, посадових осіб органів державної влади та місцевого самоврядування.

Розуміючи, що реалізація загроз і нанесення шкоди системі управління та зв'язку, а також взагалі інформаційним ресурсам держави, можуть обернутися для країни важкими наслідками – від втрати керованості до майже повного

руйнування системи управління державою, особливу увагу було приділено проблемам забезпечення безпечного інформаційного обміну та захисту її інформаційних ресурсів.

Одним з найважливіших напрямів діяльності у сфері забезпечення безпеки інформації є захист інформації криптографічними методами. Президентом України у лютому 1998 р. на ГУУЗ СБУ було покладено здійснення заходів щодо криптографічного захисту інформації в телекомунікаційних та інформаційних системах, а вже у травні того ж року – реалізацію державної політики у цій сфері.

Як відомо, інформацію тільки тоді можна вважати надійно захищеною, коли для її захисту комплексно використовуються та органічно поєднується усі види захисту: криптографічний, технічний, організаційний. З метою концентрації зусиль у сфері захисту інформації за рішенням Президента України у серпні 1998 р. на базі ГУУЗ СБУ із залученням фахівців Головного управління технічного захисту інформації Держкомсекретів та МО України було створено Департамент спеціальних телекомунікаційних систем та захисту інформації СБ України (ДСТСЗІ СБ України), який став головною структурою в державі з питань криптографічного та технічного захисту інформації.

Як довела практика, об’єднання функцій криптографічного та технічного захисту інформації в одному підрозділі дало можливість комплексно вирішувати питання захисту інформації, знаходити більш ефективні рішення, заощаджувати державні кошти та суттєво скоротити терміни розробки і реалізації проєктів. З метою реалізації державної політики в галузях криптографічного та технічного захисту інформації, захисту інформаційних ресурсів в мережах передачі даних Указом Президента України в квітні 2000 р. ДСТСЗІ було визначено органом державного управління. Надання йому цього статусу було зумовлено тим, що низка його функцій мали загальнодержавне значення, а рішення Департаменту, прийняті в межах його компетенції, стали обов’язковими для виконання.

За останні роки у напрямі створення цілісної системи захисту інформації в державі та забезпечення надійного функціонування спеціальних телекомунікаційних систем зроблено немало. За результатами діяльності Департаменту створено нормативно-правове, організаційне та технологічне підґрунтя для комплексного вирішення питань щодо забезпечення технічного складника інформаційної безпеки держави. В Україні Департамент виступав як суб’єкт державної системи інформаційної безпеки, який забезпечує реалізацію технічного складника державної політики у сфері безпеки інформації.

Подальша ефективна діяльність, як свідчить досвід провідних країн світу, повинна проходити шляхом нарощування потужностей тих структур, на які покладено реалізацію цих завдань, шляхом збільшення їх ваги в системі органів державного управління, створення додаткових важелів впливу на процеси реалі-

зації державної політики у сфері інформаційної безпеки, особливо з позиції її важливості для безпечного та стабільного розвитку суспільства в умовах глобалізації процесів інформаційного обміну.

Указом Президента України «Про додержання прав людини під час проведення оперативно-технічних заходів» від 07.11.2005 № 1556/2005 було визначено необхідність створення в державі служби спеціального зв'язку та захисту інформації України як центрального органу виконавчої влади із спеціальним статусом, визначивши її основними завданнями реалізацію державної політики у сфері захисту державних інформаційних ресурсів у мережах передачі даних, забезпечення функціонування Державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, криптографічного та технічного захисту інформації.

Необхідність існування такого державного органу також визначена в Законах України «Про захист інформації в інформаційно-телекомунікаційних системах», «Про електронний цифровий підпис», «Про електронні документи та електронний документообіг» тощо.

На рис. 13.2 представлено історію створення Державної служби спеціального зв'язку та захисту інформації України.

Рисунок 13.2. Історія створення Держспецзв'язку

13.5. Державна служба спеціального зв'язку та захисту інформації України (Держспецзв'язку)

Держспецзв'язку створена на виконання прийнятого 23 лютого 2006 р. Закону України «Про Державну службу спеціального зв'язку та захисту інформації України» на базі Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України, що ліквідується.

Держспецзв'язку створено як державний орган, діяльність якого спрямовується Кабінетом Міністрів України, який здійснює заходи щодо забезпечення її функціонування. Держспецзв'язку підконтрольна Верховній Раді України, а з питань, пов'язаних із забезпеченням національної безпеки України – підпорядковується і підконтрольна Президенту України.

Держспецзв'язку, відповідно до своїх повноважень та функцій, забезпечує:

– функціонування та розвиток державної системи урядового зв'язку та Національної системи конфіденційного зв'язку як спеціальних телекомунікаційних систем, що функціонують в інтересах управління державою;

– реалізацію державної політики у специфічній сфері криптографічного та технічного захисту інформації;

– комплексний захист інформаційних ресурсів держави в інформаційно-телекомунікаційних системах;

– контроль стану безпеки спеціальних видів зв'язку та захисту інформації в Україні.

Завдання та повноваження Держспецзв'язку визначені в Законі України «Про Державну службу спеціального зв'язку та захисту інформації України».

Основними завданнями Держспецзв'язку є:

– участь у формуванні та реалізація державної політики у сфері захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах, криптографічного та технічного захисту інформації;

– забезпечення в установленому порядку урядовим зв'язком Президента України, Голови Верховної Ради України, Прем'єр-міністра України, інших посадових осіб органів державної влади, органів місцевого самоврядування, органів військового управління, керівників підприємств, установ і організацій у мирний час, в умовах надзвичайного та воєнного стану, а також у разі виникнення надзвичайної ситуації;

– забезпечення функціонування, безпеки та розвитку державної системи урядового зв'язку і Національної системи конфіденційного зв'язку;

– визначення вимог і порядку створення та розвитку систем технічного й криптографічного захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;

– здійснення державного контролю за станом криптографічного та технічного захисту інформації, яка є власністю держави, або інформації з обмеженим

доступом, вимога щодо захисту якої встановлена законом, а також за додержанням вимог законодавства у сфері надання послуг електронного цифрового підпису;

– охорона об'єктів, приміщень, систем, мереж, комплексів, засобів урядового і спеціального зв'язку, ключових документів до засобів криптографічного захисту інформації Державної служби спеціального зв'язку та захисту інформації України.

Основні завдання Держспецзв'язку

- забезпечення функціонування й розвитку державної системи урядового зв'язку
- створення й розвиток Національної системи конфіденційного зв'язку
- криптографічний захист інформації
- технічний захист інформації
- захист державних інформаційних ресурсів
- державний контроль стану захисту інформації

Рисунок 13.3. Основні завдання Держспецзв'язку

Згідно з Законом, Держспецзв'язку утворено у складі спеціально уповноваженого центрального органу виконавчої влади з питань організації спеціального зв'язку та захисту інформації й підпорядкованих йому регіональних органів та територіальних підрозділів. У Держспецзв'язку створюються навчальні, медичні, санаторно-курортні та інші заклади, науково-дослідні та науково-виробничі установи. До сфери управління Держспецзв'язку входять держпідприємства, діяльність яких пов'язана із забезпеченням виконання покладених на Держспецзв'язку завдань.

13.6. Організаційна структура Держспецзв'язку

Для організації діяльності, спрямованої на забезпечення захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах, криптографічного та технічного захисту інформації, безпеки спеціального зв'язку в Держспецзв'язку України, як спеціально уповноважений орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації, створено Адміністрацію Держспецзв'язку. Адміністрація Держспецзв'язку є управлінською структурою, побудованою на базі основних підрозділів ДСТСЗІ СБ України та з покладанням на неї їх основних функцій.

Організаційна структура Адміністрації:

– Адміністрація Держспецзв'язку;

– регіональні підрозділи;

– територіальні підрозділи.

На Адміністрацію Держспецзв'язку покладається здійснення управління Державною службою спеціального зв'язку та захисту інформації України, організація забезпечення функціонування, безпеки та розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку, здійснення державного контролю за станом криптографічного та технічного захисту інформації. Функції, пов'язані безпосередньо з реалізацією завдань, що стоять перед Держспецзв'язку, покладаються на окремі підрозділи, що входять до складу Держспецзв'язку:

– *Центр забезпечення урядовим зв'язком Держспецзв'язку у м. Києві та Київській області,* що забезпечує функціонування державної системи урядового зв'язку та безпеку інформації в ній безпосередньо у місті Києві;

– *Державний науково-дослідний інститут спеціального зв'язку та захисту інформації,* основними завданнями якого є підготовка пропозицій щодо загальної стратегії розвитку спеціальних інформаційно-телекомунікаційних систем, розробка нормативно-правових актів у цій сфері, розробки проєктів створення спеціальних інформаційно-телекомунікаційних систем;

– *Інститут спеціального зв'язку та захисту інформації Національного технічного університету «КПІ»* для підготовки висококваліфікованих фахівців у галузі спеціального зв'язку та захисту інформації для Держспецзв'язку та інших органів виконавчої влади, наукових кадрів, перепідготовки і підвищення кваліфікації інженерних кадрів;

– *регіональні органи та територіальні підрозділи* для вирішення покладених на Держспецзв'язку завдань в регіонах України.

Контрольні питання:

1. Що таке інформаційна безпека?

2. Назвіть об'єкти і суб'єкти інформаційної безпеки.

3. Назвіть основні складники інформаційної безпеки.

4. Перерахуйте основні функції системи забезпечення інформаційної діяльності.

5. Назвіть основні загрози національній безпеці України.

6. Яка державна структура є головною з питань криптографічного та технічного захисту інформації?

7. Основні завдання Держспецзв'язку.

ТЕМА 14
ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ДЕРЖАВНОМУ РІВНІ: ПРАКТИКА УКРАЇНИ (криптографічні методи захисту)

Серед усього спектру методів захисту даних від небажаного доступу особливе місце займають криптографічні методи. Криптографія – наука про математичні методи забезпечення конфіденційності і автентичності інформації. Для сучасної криптографії характерне використання відкритих алгоритмів шифрування, що припускають використання обчислювальних засобів. Криптографічний захист інформації – вид захисту інформації, що реалізується шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховування / відновлення змісту інформації, підтвердження її справжності, цілісності, авторства. У темі розглядаються основні положення державної політики України у сфері інформаційної безпеки, а саме розглядається один з найважливіших напрямів діяльності у сфері забезпечення безпеки інформації – захист інформації криптографічними методами.

Ключові слова: *інформаційна безпека, захист інформації, інформаційно-телекомунікаційні системи, криптографічний захист, шифрування, криптосистема.*

План

14.1. Захист державних інформаційних ресурсів в інформаційно-телекомунікаційних системах.

14.2. Криптографічний захист інформації.

14.3. Науково-технічна діяльність.

14.1. Захист державних інформаційних ресурсів в інформаційно-телекомунікаційних системах

Реалізація державної політики щодо захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах полягає у (рис. 14.1):

– підготовці пропозицій до визначення загальної стратегії та пріоритетних напрямів діяльності у сфері захисту державних інформаційних ресурсів в ІТС;

– виконанні обов’язків уповноваженого органу у сфері захисту інформації в інформаційно-телекомунікаційних системах;

– розробленні порядку та вимог до захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах, а також погодження проектів нормативно-правових актів з цих питань;

– розробленні критеріїв та порядку оцінювання стану захищеності державних інформаційних ресурсів в інформаційно-телекомунікаційних системах тощо.

Рисунок 14.1. Схема реалізації державної політики в інформаційно-телекомунікаційних системах перенабрати

Реалізація державної політики забезпечується шляхом виконання низки заходів відповідно до визначених завдань, а саме:

– методичного керівництва та координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форми власності з питань, пов'язаних із запобіганням вчиненню порушень безпеки інформації в інформаційно-телекомунікаційних системах, виявленням та усуненням наслідків інших несанкціонованих дій щодо державних інформаційних ресурсів в інформаційно-телекомунікаційних системах;

– накопичення та аналізу даних про вчинення та/або спроби вчинення несанкціонованих дій щодо державних інформаційних ресурсів в інформаційно-телекомунікаційних системах, а також про їх наслідки;

– організації та здійснення оцінювання стану захищеності державних інформаційних ресурсів в інформаційно-телекомунікаційних системах, надання відповідних рекомендацій.

Сьогодні підключення органів державної влади до мережі Інтернет здійснюється через захищений вузол інтернет-доступу Держспецзв'язку. Подальше підключення органів державної влади до мережі Інтернет має здійснюватися виключно через захищений вузол інтернет-доступу НСКЗ.

На виконання завдань Національної програми інформатизації у межах виконання проєкту «Забезпечити антивірусний захист державних інформаційних ресурсів» створено Центр антивірусного захисту інформації (ЦАЗІ). Одним із основних завдань ЦАЗІ є впровадження єдиної технологічної політики щодо антивірусного захисту інформації в ІТС органів державної влади, а також централізованого забезпечення їх антивірусними програмними продуктами, сертифікованими у встановленому законодавством України порядку.

Також із використанням ресурсів ЦАЗІ проводяться державні експертизи антивірусних програмних засобів з метою визначення можливості їх застосування в Україні та експрес-експертизи антивірусних оновлень до них.

З метою проведення оцінки стану захищеності державних інформаційних ресурсів в інформаційно-телекомунікаційних системах відповідно до затвердженого постановою Кабінету Міністрів України від 03.08.2005 № 688 Положення утворено Реєстр інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління. Забезпечення функціонування цього Реєстру покладено на Департамент безпеки інформаційно-телекомунікаційних систем.

Реалізація вимог Положення створює передумови для:

– запровадження єдиної системи обліку відомостей про ІТС органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління;

– проведення аналізу стану захисту державних електронних інформаційних ресурсів в ІТС;

– надання методичної допомоги і координування діяльності міністерств та інших центральних органів виконавчої влади, пов'язаної із захистом державних електронних інформаційних ресурсів в ІТС.

З метою оптимізації дій щодо недопущення реалізації загроз інформаційним ресурсам держави необхідно здійснювати проведення оцінювання (аудиту) стану захищеності державних інформаційних ресурсів в ІТС, зокрема тих, що мають доступ до мережі Інтернет.

Наступним кроком у напрямі організації та здійснення оцінювання стану захищеності державних інформаційних ресурсів в інформаційно-телекомуні-

каційних системах має стати розроблення й видання відповідних нормативно-правових актів та нормативних документів, які б, з урахуванням міжнародного досвіду, дали змогу оптимізувати вироблення єдиних критеріїв та порядку такого оцінювання.

Сьогодні з метою вжиття упереджувальних заходів та розвитку методології запобігання порушенню цілісності, доступності та конфіденційності державних інформаційних ресурсів здійснюються заходи, спрямовані на підготовку до ліквідації наслідків несанкціонованих дій, що порушили безперебійне функціонування інформаційно-телекомунікаційних систем органів державної влади, поширюється інформація щодо наявних та ймовірних загроз, інструментів і засобів забезпечення безпеки інформації тощо.

В Адміністрації Держспецзв'язку функціонує підрозділ, діяльність якого спрямована саме на вирішення таких завдань. Надання відповідних повноважень та реєстрація встановленим порядком українського аналога CSIRT (Computer Security Incident Response Teams – структури швидкого реагування на інциденти, що загрожують безпеці інформаційних ресурсів) сприятиме ефективній реалізації державної політики у сфері захисту державних інформаційних ресурсів в ІТС та підвищенню загального стану захисту національного інформаційного простору.

14.2. Криптографічний захист інформації

Одним із найважливіших напрямів діяльності у сфері забезпечення безпеки інформації був і залишається **захист інформації криптографічними методами.**

Сьогодні у сфері криптографічного захисту інформації реалізовуються такі основні завдання:

– участь у формуванні та реалізація державної політики у сфері криптографічного захисту інформації;

– розробка нормативно-правових актів, організація та проведення ліцензування, сертифікації та державної експертизи у сфері криптографічного захисту інформації;

– здійснення контролю за додержанням вимог законодавства у сфері надання послуг електронного цифрового підпису (ЕЦП).

Формування та реалізація державної політики у сфері криптографічного захисту інформації (КЗІ) здійснюється за такими напрямами:

– нормативно-правове забезпечення функціонування та розвитку системи криптографічного захисту інформації;

– організація та супроводження заходів у межах державних цільових програм;

– ліцензування господарської діяльності у сфері КЗІ;

– координація робіт з проведення сертифікації засобів КЗІ, державної експертизи у сфері КЗІ, тематичних досліджень та допуску до експлуатації засобів КЗІ;

– організація робіт з проведення сертифікації засобів КЗІ;

– організація та проведення робіт з державної експертизи у сфері КЗІ, тематичних досліджень та допуску до експлуатації засобів КЗІ;

– участь у заходах щодо державного контролю за міжнародними передачами товарів подвійного використання;

– розроблення криптографічних алгоритмів та криптографічних протоколів;

– централізований облік спеціальних виробів.

На рис. 14.2 представлено реалізацію державної політики у галузі криптографічного захисту інформації.

Рисунок 14.2. Схема реалізації державної політики у галузі КЗІ

Пріоритетними напрямами діяльності, спрямованими на формування пропозицій та ефективну реалізацію державної політики у сфері криптографічного захисту інформації, є:

– удосконалення нормативно-правової бази у сфері КЗІ;

– розробка та введення в дію гармонізованих з міжнародними стандартів у галузі КЗІ;

– удосконалення механізму та збільшення напрямків прикладних та фундаментальних досліджень у галузі КЗІ.

Системність опрацювання наукоємних та складних завдань цієї сфери забезпечує безпечне функціонування та поступовий розвиток системи криптографічного захисту інформації, застосування шифрувальних засобів, створення на базі сучасних технологій криптографічних систем та засобів криптографічного захисту інформації. Створення таких систем можна порівняти із ракетобудуванням або розробкою «космічних» технологій (див. рис. 14.3).

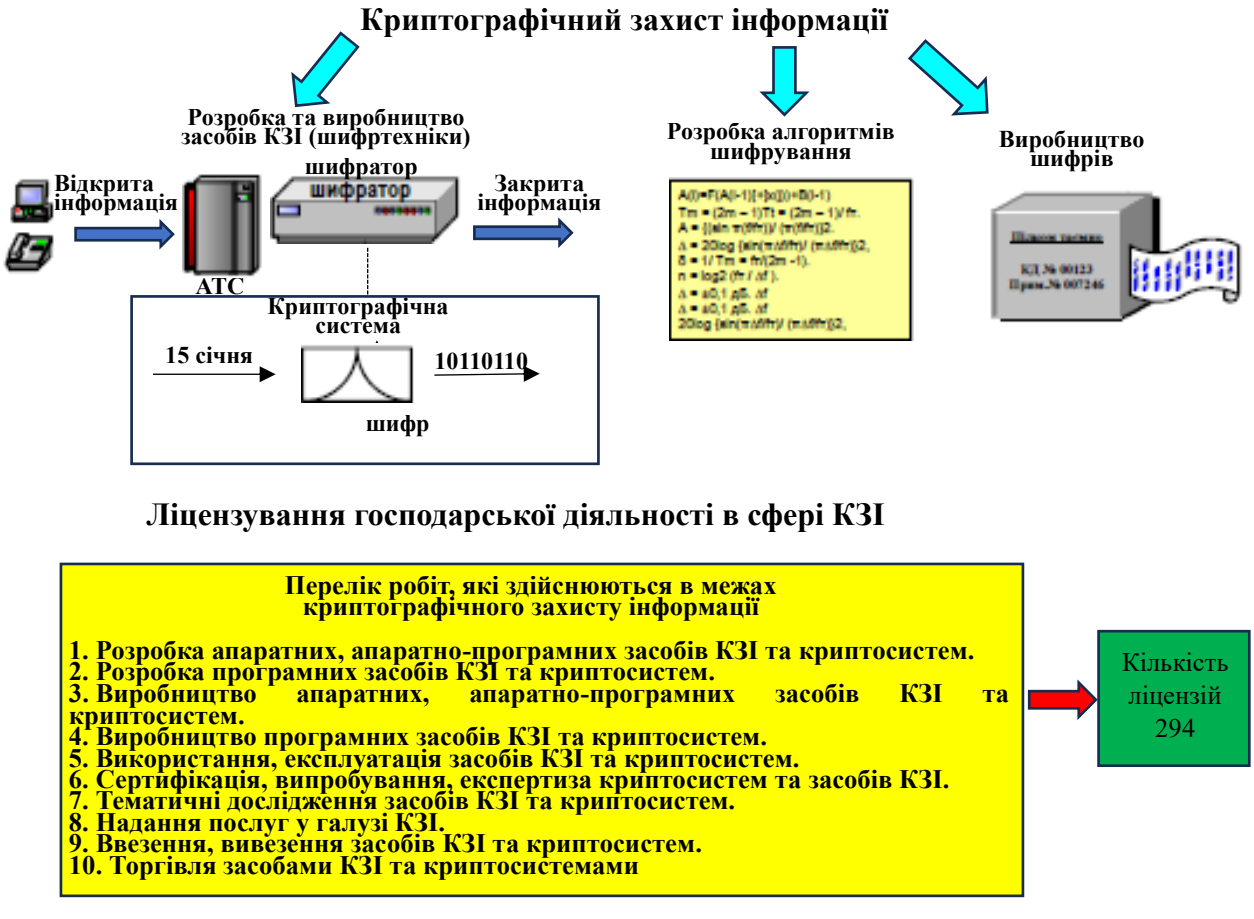

Рисунок 14.3. Схема криптографічного захисту інформації

Основою для виконання зазначених завдань є нормативно-правові акти України, якими визначено запровадження ефективного механізму ліцензування, сертифікації та експертизи в галузі захисту інформації, вимоги до порядку

розробки, дослідження, виготовлення, експлуатації засобів криптографічного захисту інформації та криптосистем, формування вимог до них та контроль за безпекою на всіх стадіях життєвого циклу засобів, а також впровадження електронного документообігу та електронного цифрового підпису.

У розвиток принципів, покладених в основу системи нормативно-правових актів цієї сфери, основні завдання виконуються консолідованими зусиллями високопрофесійних фахівців у сфері захисту інформації. Застосування сучасних технологій управління об'єднало зусилля широкого кола науковців. Це дало змогу забезпечувати розвиток нормативно-правової бази цієї сфери, а саме введення в дію низки нормативних документів технічного характеру, національних стандартів, зокрема гармонізованих із міжнародними. Проведена робота створила передумови для побудови в Україні системи криптографічного захисту інформації.

Згідно з Положенням про порядок здійснення криптографічного захисту інформації в Україні система криптографічного захисту інформації (система КЗІ) являє собою сукупність органів, підрозділів та груп, діяльність яких направлена на забезпечення КЗІ, а також підприємств, установ та організацій, що розробляють, виробляють, експлуатують та (або) розповсюджують криптосистеми та засоби КЗІ.

Розвиток системи криптографічного захисту інформації, організація і налагодження виробництва вітчизняних захищених засобів і технологій для оброблення інформації – це необхідні напрями діяльності у сфері забезпечення національної безпеки України. Сьогодні розвиток системи КЗІ здійснюється в межах відповідної Державної цільової програми. Вимоги, а також порядок створення, функціонування та розвитку системи КЗІ визначено в нормативно-правових актах, що регулюють діяльність у цій сфері. Результат діяльності у сфері КЗІ такий:

– розгорнуто виробництво національних ключових документів (шифрів) для використання у системах спеціального зв'язку України;

– розроблено сімейство національних криптографічних алгоритмів та криптографічних протоколів, на основі яких можуть створюватись найсучасніші засоби захисту інформації;

– розроблено типові рішення, які дають змогу забезпечити створення уніфікованої низки засобів шифрування і засекречування та розгорнути їх серійне виробництво;

– розроблені та серійно виготовляються вітчизняні конкурентноспроможні засоби захисту інформації, які за своїми властивостями не поступаються кращим світовим зразкам; створена нормативно-правова база та побудована організаційно-технічна інфраструктура для організації та застосування електронного цифрового підпису як аналога власноручного підпису.

За останні роки в державі забезпечено сталий розвиток інфраструктури електронного цифрового підпису відповідно до положень Закону України «Про електронний цифровий підпис». У практичному аспекті це стосується створення організатора національної системи електронного цифрового підпису кореневого центру сертифікації ключів, запровадження інституту добровільної акредитації, а також початку функціонування та надання відповідних послуг центрами сертифікації ключів, розвитку нормативної бази в цій сфері, поступовою консолідацією зусиль заінтересованих суб'єктів ЕЦП у спільному вирішенні проблем організаційного та технічного характеру. Зі свого боку Держспецзв'язку, виконуючи функції контролюючого органу у сфері ЕЦП та уповноваженого органу виконавчої влади у сфері захисту інформації, спрямовує свої зусилля на забезпечення послідовного вирішення нормативних, організаційно-технічних та інших питань, пов'язаних із розбудовою та безпечним функціонуванням інфраструктури ЕЦП в державі.

Подальше удосконалення нормативно-правової бази у сфері КЗІ, її гармонізація з міжнародними нормативними документами буде сприяти зміцненню національної безпеки України та підвищенню міжнародного авторитету України як демократичної і правової держави.

Одним зі складників реалізації державної політики у сфері криптографічного захисту інформації є проведення ліцензування та сертифікації засобів КЗІ. Регулярно здійснюється перевірка дотримання суб'єктами господарської діяльності ліцензійних умов і правил провадження діяльності у сфері КЗІ. Створені системи сертифікації й експертизи систем та засобів КЗІ та забезпечується їх діяльність. Виконуються роботи, пов'язані з проведенням досліджень та підтвердженням якісних характеристик засобів, комплексів і систем криптографічного захисту інформації.

14.3. Науково-технічна діяльність

Важливим напрямом діяльності у сфері криптографічного й технічного захисту є наукова та науково-технічна діяльність, що зумовлено необхідністю:

– постійного вдосконалення та розвитку наявних мереж і комплексів спеціальних інформаційно-телекомунікаційних систем, розроблення сучасних вітчизняних засобів криптографічного та технічного захисту інформації, забезпечення безпеки державних інформаційних ресурсів в інформаційно-телекомунікаційних системах;

– визначення загроз інформації, формування вихідних даних для оцінки можливостей технічних засобів розвідки і їх небезпеки, виявлення потенційних каналів витоку інформації;

– проведення фундаментальних та прикладних наукових досліджень різних факторів і фізичних полів, технічних рішень і технологій, що можуть бути використані для ведення розвідувальної діяльності і несанкціонованого збору інформації, особливо відомостей, що становлять державну таємницю.

Розвиток спеціальних інформаційно-телекомунікаційних систем

На сучасному етапі розвитку суспільства, який характеризується впровадженням новітніх технологій і систем, одним з важливих завдань є не лише забезпечення функціонування вже наявних, але і впровадження нових, які б не поступалися світовим стандартам та відповідали вимогам часу.

Для забезпечення зазначених завдань у складі Адміністрації Державної служби утворено Департамент стратегії розвитку спеціальних інформаційно-телекомунікаційних систем. Основними його завданнями є:

– підготовка пропозицій щодо загальної стратегії розвитку спеціальних інформаційно-телекомунікаційних систем;

– розробка нормативно-правових актів у цій сфері та розробки проєктів створення спеціальних інформаційно-телекомунікаційних систем;

– організація виконання робіт зі створення засобів криптографічного захисту інформації та погодження міжнародних передач засобів КЗІ та криптосистем.

Для виконання покладених функцій на Департамент було створено високопрофесійний колектив, результатами діяльності якого було сформовано основні концептуальні підходи, направлені на розвиток спеціальних інформаційно-телекомунікаційних систем, які знайшли своє відображення у Державних програмах.

Ці Державні програми були підтримані Урядовим комітетом та затверджені Урядом. З метою консолідації зусиль та об’єднання високофахового наукового потенціалу Урядом держави підтримано пропозицію Державної служби та було утворено Державний науково-дослідний інститут спеціального зв’язку та захисту інформації.

Сьогодні в Державній службі запроваджено систему організації та проведення наукових досліджень, які здійснюються в основному у формі науково-дослідних та дослідно-конструкторських робіт. Одним із ключових виконавців наукових робіт і є новостворений Державний інститут.

Роботи, які виконує Державний інститут, виконуються на високому професійному рівні та знаходять своє застосування у вигляді розробок сучасних вітчизняних засобів криптографічного та технічного захисту інформації, спеціалізованого комутаційного, прикінцевого та допоміжного обладнання. Інженерно-технічні рішення, які застосовуються у службовому процесі, дають змогу впроваджувати весь технологічний цикл розробки спеціальних розробок – від ескізно-технічного рішення до дослідного зразка.

Забезпечення технічного захисту інформації як складна та наукоємна проблема потребує науково-методичного та науково-технічного супроводу. Для визначення загроз інформації, формування вихідних даних для оцінки можливостей технічних засобів розвідки і їх небезпеки, виявлення потенційних каналів витоку інформації необхідно забезпечити проведення фундаментальних та прикладних наукових досліджень різних факторів і фізичних полів, технічних рішень і технологій, що можуть бути використані для ведення розвідувальної діяльності і несанкціонованого збору інформації, особливо відомостей, що становлять державну таємницю.

З метою розгляду наукових рекомендацій, інших пропозицій щодо головних напрямів розвитку науки і техніки в галузі спеціальних інформаційно-телекомунікаційних систем та захисту інформації, обговорення найважливіших програм у складі Державної служби працює Науково-технічна рада, яка виступає координуючим органом наукової діяльності у межах Державної служби. Активну участь підрозділи Державної служби беруть у проведенні спеціалізованих конференцій, виставок і семінарів, зокрема й міжнародних.

Контрольні питання:

1. Що таке криптографія?
2. Що таке криптографічний захист інформації?
3. Перерахуйте основні завдання криптографічного захисту інформації.

ТЕМА 15
ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ДЕРЖАВНОМУ РІВНІ: ПРАКТИКА УКРАЇНИ
(технічні методи захисту)

Серед загроз інформації за своїми небезпечними наслідками особливе місце займають:

а) здобування технічними розвідками відомостей у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку;

б) несанкціонований доступ до інформації, яка обробляється та циркулює в інформаційних та телекомунікаційних системах;

в) витік інформації з обмеженим доступом технічними каналами.

Для протидії зазначеним загрозам у державі створена, функціонує та розвивається система технічного захисту інформації, яка є сукупністю організаційних структур, поєднаних цілями і завданнями захисту інформації, нормативно-правової та матеріально-технічної бази.

У темі розглядається реалізація державної політики України в сфері технічного захисту інформації (ТЗІ), а саме організаційна структура ТЗІ, ліцензування, сертифікація і державна експертиза в галузі ТЗІ.

Ключові слова: *інформаційна безпека, захист інформації, технічний захист, ліцензування, сертифікація, експертиза, державний контроль, державна політика, науково-технічна діяльність.*

План

15.1. Технічний захист інформації в Україні, основні аспекти.

15.2. Побудова і організаційна структура системи ТЗІ в Україні.

15.3. Ліцензування діяльності у галузі ТЗІ.

15.4. Сертифікація засобів ТЗІ.

15.5. Державна експертиза у сфері ТЗІ.

15.6. Система підготовки та перепідготовки фахівців у галузі ТЗІ.

15.7. Державний контроль стану КТЗІ.

15.1. Технічний захист інформації в Україні, основні аспекти

У загальному комплексі заходів щодо забезпечення національної безпеки держави важливе місце займають заходи, пов’язані з безпосереднім захистом інформації від загроз, реалізація яких може нанести особі, суспільству, державі політичних, економічних, фінансових та інших збитків. Серед загроз інформації за своїми небезпечними наслідками особливе місце займають:

1. Здобування технічними розвідками відомостей у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку.

Незважаючи на позитивні зміни в міжнародній обстановці навколо України, діяльність технічних розвідок іноземних держав із здобування інформації продовжується. Проти України безперервно ведеться розвідка багатофункціональними космічними, повітряними, наземними, морськими системами та комплексами технічної розвідки. Провідні країни світу продовжують модернізувати свої розвідувальні служби, вдосконалюють технічну розвідку, нарощують її можливості.

Наявні можливості технічних розвідок практично дають змогу забезпечити безперервне спостереження за всією територією України, і надалі засоби технічної розвідки, зокрема космічної компоненти, будуть мати виключно високі характеристики, які дадуть змогу забезпечити постійне стеження за всією територією держави в реальному масштабі часу.

2. Несанкціонований доступ до інформації, яка обробляється та циркулює в інформаційних та телекомунікаційних системах, а також спеціальний вплив на інформацію з метою її спотворення, руйнування, знищення, порушення нормального функціонування систем обробки інформації.

За умови недостатньої номенклатури засобів обробки інформації та програмного забезпечення вітчизняної розробки в інформаційно-телекомунікаційних системах широко використовуються продукти іноземного виробництва, які здебільшого не мають об'єктивних оцінок механізмів захисту, а також створюють передумови впровадження в усі сфери життєдіяльності особи, суспільства та держави інформаційних технологій. Це зумовлено широким розгортанням інформаційно-телекомунікаційних систем, різким збільшенням обсягів інформації, яка обробляється, зберігається в цих системах, значним збільшенням кола користувачів, які мають безпосередній доступ до інформаційних ресурсів тощо.

Водночас за відсутності конкурентоспроможних вітчизняних зразків перевага надається інформаційним технологіям та технічним засобам обробки інформації іноземного виробництва, які здебільшого не забезпечують захисту інформації, а також створюють передумови неконтрольованого використання спеціальних програмних та апаратних засобів («закладних пристроїв»).

У світі зберігається тенденція поширення масштабів комп'ютерної злочинності, розповсюдження комп'ютерних вірусів, насамперед з використанням інтернету, істотно зростає небезпека наслідків неправомірних дій, технічних і технологічних помилок та збоїв під час застосування інформаційно-телекомунікаційних систем, що є особливо актуально в умовах широкого входження вітчизняних інформаційно-телекомунікаційних систем до глобальних.

Окремими державами реалізується «концепція інформаційного протиборства», яка полягає в реалізації заходів щодо спеціального впливу на інформаційну інфраструктуру з метою ураження (знищення) інформаційних ресурсів та руйнування системи управління у сферах оборони, економіки, безпеки, фінансів тощо.

3. Витік інформації з обмеженим доступом технічними каналами внаслідок виникнення побічних електромагнітних випромінювань і наводів, ведення акустичної та оптико-електронної розвідки в безпосередній близькості від об'єкта інформаційної діяльності.

У процесі здійснення інформаційної діяльності для зберігання, обробки та передавання інформації, зокрема й інформації з обмеженим доступом, широко використовуються технічні засоби різного призначення (засоби обчислювальної техніки, оргтехніка, засоби зв'язку, автоматизовані системи тощо). На об'єктах інформаційної діяльності здійснюється обговорення службових питань щодо захисту інформації, який визначено як складник забезпечення національної безпеки України.

Метою ***державної політики у сфері технічного захисту інформації*** є створення правових, організаційних, економічних засад функціонування системи технічного захисту інформації (див. рис. 15.1).

Рисунок 15.1. Схема реалізації державної політики в галузі ТЗІ

15.2. Побудова і організаційна структура системи ТЗІ в Україні

Державна політика у сфері ТЗІ визначається пріоритетністю національних інтересів, має на меті унеможливлення реалізації загроз для інформації та здійснюється у напрямах нормативно-правового і організаційного забезпечення науково-технічної та виробничої діяльності. Важливість для безпеки держави галузі ТЗІ, її наукоємність вимагає концентрації зусиль науково-технічного та виробничого потенціалу міністерств, інших центральних органів виконавчої влади, академій наук. Відповідно до цього визначено основні принципи і концептуальні засади організації забезпечення ТЗІ в Україні. До таких належать:

– додержання балансу інтересів особи, суспільства та держави, їх взаємна відповідальність;

– єдність підходів до забезпечення ТЗІ, які визначаються загрозами безпеці інформації та режимом доступу до неї;

– комплексність, повнота та безперервність заходів ТЗІ;

– гармонізованість нормативно-правових актів та нормативних документів щодо ТЗІ з відповідними міжнародними договорами України та міжнародними стандартами;

– обов'язковість захисту інженерно-технічними заходами інформації, яка становить державну та іншу передбачену законом таємницю, конфіденційної інформації, що є власністю держави, відкритої інформації, важливої для держави, незалежно від того, де зазначена інформація циркулює, а також відкритої інформації, важливої для особи та суспільства, якщо ця інформація циркулює в органах державної влади, інших державних органах та органах місцевого самоврядування, у допоміжних органах і службах Президента України, Національній академії наук, Збройних Силах, інших військових формуваннях, органах внутрішніх справ, на державних підприємствах, в державних установах і організаціях;

– виконання на власний розсуд суб'єктами інформаційних відносин вимог щодо технічного захисту інформації, що є їхньою власністю, та відкритої інформації, важливої для особи та суспільства, якщо остання циркулює поза межами державних організацій;

– покладання відповідальності за формування та реалізацію державної політики у сфері ТЗІ на спеціально уповноважений центральний орган виконавчої влади;

– ієрархічність побудови організаційної структури системи ТЗІ, суб'єкти якої належать до сфери управління або підпорядковані відповідній державній організації, та її керівництво діяльністю цих суб'єктів у межах повноважень, наданих нормативно-правовими актами;

– методичне керівництво спеціально уповноваженим центральним органом виконавчої влади у сфері ТЗІ діяльністю організаційних структур системи ТЗІ;

– фінансова забезпеченість системи ТЗІ за рахунок державного бюджету, місцевих бюджетів та інших джерел.

Організаційна структура системи ТЗІ має ієрархічну деревовидну будову з підлеглістю і підзвітністю «знизу вгору» по вертикалі та незалежністю суб'єктів одного рівня ієрархії. Функції уповноваженого державного органу у сфері ТЗІ виконує Держспецзв'язку.

На відомчому рівні заходи із забезпечення ТЗІ здійснюються безпосередньо суб'єктами системи ТЗІ – міністерствами й іншими органами державної влади та підпорядкованими їм підприємствами, установами й організаціями, а відповідальність за організацію і стан захисту інформації покладається на їх керівників. Вони мають створювати або визначати підрозділи для оцінювання стану загроз інформації, розроблення та реалізації планів заходів щодо її захисту, координації діяльності інших суб'єктів у сфері підпорядкування, здійснення розрахунків та обґрунтувань потрібних для цього коштів.

Сьогодні нормативно-правовими актами повністю визначена правова основа функціонування всіх елементів організаційної структури системи ТЗІ, завдання і функції суб'єктів ТЗІ, їх права і обов'язки, порядок їх взаємодії і здійснення ними діяльності, а також порядок функціонування основних елементів, як-от системи ліцензування і оцінювання продукції, підготовки і перепідготовки кадрів.

Одним із важливих напрямів діяльності в галузі ТЗІ є організація **протидії технічним розвідкам.** Організація протидії, своєчасне розроблення та впровадження необхідних заходів покладається на керівника органу державної влади, органу місцевого самоврядування, органу управління Збройних Сил України та інших військових формувань, утворених згідно з законодавством України (далі орган), підприємства, установи, організації (далі організація). Проведення заходів протидії покладається на створений або визначений наказом керівника органу (організації) штатний чи позаштатний підрозділ ТЗІ або призначену особу.

Протидія технічним розвідкам (ПДТР) є невід'ємним складником систем охорони державної таємниці та захисту інформації з обмеженим доступом, яка є власністю держави (ІОДД) і здійснюється шляхом впровадження заходів щодо запобігання порушенню конфіденційності ІОДД засобами технічної розвідки. Сукупність впроваджуваних організаційних та інженерно-технічних заходів, програмних і технічних засобів, які використовуються для забезпечення протидії, є складником комплексу ТЗІ, спрямованого на приховування ІОДД та дезінформування технічних розвідок.

Держспецзв'язку здійснює організацію та координацію робіт з протидії, надання суб'єктам системи ТЗІ консультативної допомоги щодо застосування нормативних документів, забезпечення виявлення і прогнозування загроз для ІОДД, формування та супроводження моделей технічних розвідок, визначення

напрямів робіт, розроблення нормативних документів системи ТЗІ, контроль за виконанням вимог нормативно-правових актів з питань протидії.

Треба зазначити, що сучасна система ПДТР була збудована на підґрунті, закладеному ще при СРСР. На час здобуття Україною самостійності в державі існувала система протидії іноземним технічним розвідкам (ПДІТР), організаційна структура якої базувалася на штатних підрозділах ПДІТР органів і організацій.

З проголошенням Україною незалежності система ПДІТР була трансформована в систему ТЗІ, а в більшості державних органів і організацій, діяльність яких пов'язана з ІОДД, на базі підрозділів ПДІТР були створені підрозділи ТЗІ, на які було покладено вирішення питань протидії, і діяльність яких повинна узгоджуватися з діяльністю режимно-секретних органів. Одночасно розпочався процес розроблення вітчизняних нормативних документів з питань ТЗІ та створення засобів захисту інформації і захищених технічних засобів. Накопичений досвід з протидії не було втрачено – нормативні документи системи ПДІТР були ретельно переглянуті, і деяким з них було надано чинності (в основному це стосується норм і методик).

Отже, сьогодні організаційна структура ПД ТР є частиною інфраструктури ТЗІ, а її діяльність повністю з нею узгоджується.

15.3. Ліцензування діяльності у галузі ТЗІ

Одним із суттєвих важелів регулювання діяльності у сфері ТЗІ є процедура ліцензування діяльності суб'єктів господарської діяльності. Механізм ліцензування діяльності у сфері ТЗІ провадиться в Україні з 1995 р. Метою провадження ліцензування є формування в Україні контрольованого ринку послуг із ТЗІ, виконання вимог нормативних документів з питань захисту інформації, розповсюдження систем та засобів технічного захисту інформації, що відповідають законодавству України, а також виключення:

– передумов до можливості застосування засобів ТЗІ в протизаконних та злочинних діях, внаслідок їх неконтрольованого обігу в країні;

– можливості компрометації інформації з обмеженим доступом через надання некваліфікованих послуг та використання неякісних засобів ТЗІ, що може призвести до реальних загроз безпеці особистості, суспільству та державі;

– розповсюдження засобів ТЗІ, що не відповідають вимогам нормативних документів чи засобів низької якості, зокрема засобів іноземного виробництва, що може призвести до знищення вітчизняної галузі розробки та виробництва надійних, конкурентоспроможних засобів ТЗІ.

Отже, крім безпосередньо регулятивних і контрольних функцій ліцензування діяльності спрямоване також на розвиток матеріально-технічної бази системи ТЗІ.

Всього в галузі ТЗІ підлягає ліцензуванню 7 видів робіт, а саме:

– розроблення, впровадження, дослідження ефективності, обслуговування на об'єктах інформаційної діяльності комплексів (систем) технічного захисту інформації, носіями якої є акустичні поля, надання консультативних послуг;

– розроблення, впровадження, дослідження ефективності, обслуговування на об'єктах інформаційної діяльності комплексів (систем) технічного захисту інформації, носіями якої є електромагнітні поля та електричні сигнали, надання консультативних послуг;

– розроблення, виробництво, впровадження, дослідження ефективності, супроводження засобів та комплексів технічного захисту інформації в інформаційних системах, інформаційних технологій із захистом інформації від несанкціонованого доступу, надання консультативних послуг;

– виявлення та блокування витоку мовної та видової інформації через закладні пристрої на об'єктах інформаційної діяльності, надання консультативних послуг;

– виробництво засобів забезпечення технічного захисту інформації, носіями якої є акустичні поля;

– виробництво засобів забезпечення технічного захисту інформації, носіями якої є електромагнітні поля та електричні сигнали;

– розроблення, впровадження, дослідження ефективності, обслуговування на об'єктах інформаційної діяльності комплексів (систем) технічного захисту інформації, носіями якої є хімічні речовини, надання консультативних послуг.

Система оцінювання продукції у сфері ТЗІ включає дві процедури – сертифікацію засобів ТЗІ та державну експертизу.

15.4. Сертифікація засобів ТЗІ

Об'єктом сертифікації в галузі ТЗІ є окремі засоби ТЗІ, які можуть вироблятися і серійно, і як одиничні зразки, зокрема сертифікації можуть підлягати і засоби імпортного виробництва. Процедура призначена надавати споживачу засобів ТЗІ гарантії відповідності цих засобів нормативним документам. Така гарантія може бути надана після проведення певних організаційно-технічних заходів. Результатом сертифікаційних робіт є спеціальний документ встановленого зразка – сертифікат відповідності.

Створення системи сертифікації засобів ТЗІ в Україні було розпочато ще в середині 90-х років, і складність його полягала в тому, що раніше ні в СРСР, ні в Україні не проводилася сертифікація засобів ТЗІ, до того ж на той час бракувало необхідної для досягнення цієї мети нормативно-правової та матеріально-технічної бази.

З березня 1999 р. система сертифікації засобів ТЗІ розпочала свою практичну діяльність. Порядок та вимоги щодо проведення сертифікації засобів ТЗІ визначаються Порядком проведення робіт із сертифікації засобів забезпечення технічного захисту інформації загального призначення, який є обов'язковим як для акредитованих у системі органів з сертифікації засобів ТЗІ та випробувальних лабораторій, так і для підприємств, установ й організацій, зокрема й іноземних, які виготовляють і (або) постачають засоби ТЗІ у державні і недержавні установи, де циркулює інформація, що підлягає захисту відповідно до законодавства.

15.5. Державна експертиза у сфері ТЗІ

Введення процедури експертного оцінювання комплексних систем захисту інформації в ІТС, технічних і програмно-апаратних засобів захисту інформації обумовлено логічною складністю сучасних програмно-апаратних комплексів, а також суттєвим впливом на безпеку інформації конкретних умов експлуатації ІТС. Інакше кажучи, такі об'єкти не повторюють один одного, і кожен з них має тільки йому притаманні особливості. У випадках оцінки програмно-апаратних засобів закордонного виробництва зазвичай відсутня необхідна для проведення їх сертифікації технічна документація, практично неможливою є оцінка умов виробництва, організація взаємодії органів сертифікації з закордонними виробниками засобів захисту.

Правову основу цієї процедури складає Закон України «Про наукову та науково-технічну експертизу». Методологічною основою є експертиза технічних рішень і організаційних заходів, які базуються на узагальненні висновків окремих експертів та результатах інструментальних вимірювань і випробувань комплексу програмно-апаратних і технічних засобів захисту інформації.

Порядок проведення державної експертизи у сфері ТЗІ, основні функції й права суб'єктів експертизи визначено Положенням про державну експертизу в сфері технічного захисту інформації.

Відповідно до законодавства у ньому визначені суб'єкти експертизи (Замовник, Організатор експертизи, Експерт), основні функції ДСТСЗІ СБ України та суб'єктів експертизи, порядок їх взаємодії, порядок документального оформлення результатів експертизи та видачі Експертного висновку (для окремих засобів захисту інформації) і Атестата відповідності на комплексні системи захисту інформації в ІТС.

Наявність позитивного рішення щодо засобу є підставою для його включення до Переліку засобів технічного захисту інформації загального призначення, які дозволені до використання з метою ТЗІ, а наявність атестата відповідності – підставою для одержання дозволу на обробку в ІТС інформації, що підлягає захисту.

Система державної експертизи функціонує з початку 2000 р., і за цей час стала одним з найбільш вагомих чинників реалізації державної політики у галузі, а її результати – розвитку матеріально-технічної бази системи ТЗІ та наповнення ринку ефективними конкурентоспроможними програмно-апаратними засобами захисту інформації.

15.6. Система підготовки та перепідготовки фахівців у галузі ТЗІ

Враховуючи, що завдання захисту інформації самі по собі є технологічно складними і науково ємними, потребують впровадження сучасних досягнень у сфері інформаційних технологій, проведення теоретичних і прикладних досліджень, необхідною умовою для їх ефективного вирішення є наявність висококваліфікованих спеціалістів. З метою підготовки таких спеціалістів в Україні вже впродовж 10-ти років у закладах вищої освіти існує система підготовки і перепідготовки спеціалістів у цій галузі.

Сьогодні система підготовки та перепідготовки фахівців із технічного захисту інформації переживає нову трансформацію і модернізацію з урахуванням сучасних вимог, що висуваються до захисту інформації і, як наслідок, до рівня підготовки фахівців. Сьогодні підготовку фахівців у галузі ТЗІ здійснюють 22 вищі навчальні заклади України.

Наказом Міністерства освіти і науки України № 246 від 9 квітня 2002 р. головним закладом освіти і науки України з інженерно-технічних напрямів галузі знань «Національна безпека» визначено НТУУ «КПІ». Важливим елементом фахової освіти є система перепідготовки та підвищення кваліфікації кадрів. Сьогодні підвищення кваліфікації фахівців з ТЗІ здійснюється за такими напрямами:

– захист інформації в інформаційно-телекомунікаційних системах, побудова комплексної системи захисту інформації;

– захист інформації на об’єктах інформаційної діяльності, виявлення закладних пристроїв;

– організація захисту мовної інформації та інформації в телекомунікаційних мережах і системах зв’язку;

– організація захисту інформації в комп’ютерних системах.

Базовим закладом є Навчальний центр перепідготовки та підвищення кваліфікації фахівців у галузі інформаційної безпеки у складі Фізико-технічного інституту КПІ ім. Ігоря Сікорського, який функціонує з 1999 р. За час створення системи підвищення кваліфікації перепідготовку пройшли більше 3 000 слухачів.

15.7. Державний контроль стану КТЗІ

Відбувається ***здійснення державного контролю за станом криптографічного та технічного захисту інформації,*** яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, а також за додержанням вимог законодавства у сфері надання послуг електронного цифрового підпису.

Діяльність щодо здійснення державного контролю за станом криптографічного та технічного захисту інформації в інформаційно-телекомунікаційних системах в органах державної влади, органах місцевого самоврядування, військових формуваннях, на підприємствах, в установах і організаціях незалежно від форми власності, у тому числі в закордонних дипломатичних установах України та миротворчих контингентах України за кордоном безпосередньо покладається на Департамент державного контролю за станом криптографічного та технічного захисту інформації.

За результатами цієї діяльності готуються та подаються на розгляд Президентові України, Голові Верховної Ради України і Прем'єр-міністрові України рекомендації щодо поліпшення стану захисту інформації в державі. Впровадження цих рекомендацій дає змогу підтримувати стан захищеності інформації та інформаційних ресурсів держави на належному рівні, попередити витік інформації, що є власністю держави, уникнути розголошення інформації, що становить державну таємницю.

Контрольні питання:

1. Що таке технічний захист інформації?
2. Назвіть основні аспекти технічного захисту інформації в Україні.
3. Організаційна структура системи технічного захисту інформації в Україні.
4. Підготовка та перепідготовки фахівців у галузі технічного захисту інформації.

ТЕМА 16
МЕНЕДЖМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА РІВНІ ПІДПРИЄМСТВА: ОСНОВНІ НАПРЯМИ І СТРУКТУРА ПОЛІТИКИ БЕЗПЕКИ

Забезпечення власної інформаційної безпеки на підприємствах зазвичай є невід'ємною частиною загальної системи управління, необхідної для досягнення статутних цілей та завдань та має велике значення не тільки для стратегічного розвитку підприємства і створення основного продукту, але і для окремих (іноді допоміжних) напрямів діяльності та бізнес-процесів, як-от комерційні переговори і умови контрактів, цінова політика тощо.

У темі перераховуються основні напрями управлінської (організаційної) роботи у сфері інформаційної безпеки на рівні окремого підприємства. Розкривається загальна структура політики інформаційної безпеки підприємства як основного організуючого документа в цій галузі.

Ключові слова: *управління інформаційної безпекою, CISO, джерело загрози, інформаційні системи, державна таємниця, державна стратегія, аналіз, контроль поведінки, розподіл функцій, доступ, зловмисник, ділова репутація, державна таємниця, банківська таємниця, управління інформаційною безпекою, ISO/IEC 27002.*

План

16.1. Передумови розвитку менеджменту у сфері інформаційної безпеки на рівні підприємств.

16.2. Загальна структура управлінської роботи щодо забезпечення інформаційної безпеки на рівні підприємства.

16.3. Формування політики інформаційної безпеки на підприємстві.

16.1. Передумови розвитку менеджменту у сфері інформаційної безпеки на рівні підприємств

Забезпечення власної інформаційної безпеки на підприємствах зазвичай є невід'ємною частиною загальної системи управління, необхідної для досягнення статутних цілей та завдань. Значимість систематичної цілеспрямованої діяльності щодо забезпечення інформаційної безпеки стає тим більш високою, чим вищий ступінь автоматизації бізнес-процесів підприємства, і чим більший «інтелектуальний складник» у його кінцевому продукті, тобто чим більшою мірою успішність діяльності залежить від наявності та збереження певної інформації (технологій, ноу-хау, комерційних баз даних, маркетингової інформації, результатів наукових досліджень тощо), забезпечення її конфіденційності та доступності для власників і користувачів. Роль інформації в діяльності під-

приємств зростає в міру лібералізації світових ринків, коли матеріальні активи меншою мірою є джерелами конкурентних переваг через значне зменшення торговельних бар'єрів. Нематеріальні активи, наявні зазвичай у вигляді інформації, в цих умовах починають відігравати роль однієї з провідних засад для підвищення конкурентоспроможності та розвитку бізнесу.

Забезпечення інформаційної безпеки також зазвичай має велике значення не тільки для стратегічного розвитку підприємства і створення основного продукту, але і для окремих (іноді допоміжних) напрямів діяльності та бізнес-процесів, як-от комерційні переговори і умови контрактів, цінова політика тощо. До того ж значимість забезпечення інформаційної безпеки в деяких випадках може визначатися наявністю в загальній системі інформаційних потоків підприємства відомостей, що становлять не тільки комерційну, а й державну таємницю, а також інші види конфіденційної інформації (відомості, що становлять банківську таємницю, лікарську таємницю, інтелектуальну власність компаній-партнерів тощо).

Так само, як і на державному рівні, управління інформаційною безпекою на рівні підприємств націлене на нейтралізацію різних видів загроз:

– зовнішніх, як-от неправомірні дії державних органів (зокрема і закордонних), протиправна діяльність злочинців і злочинних угруповань, незаконні дії компаній-конкурентів та інших суб'єктів господарювання, недобросовісні дії компаній-партнерів, невідповідність чинної нормативно-правової бази фактичному розвитку технологій і суспільних відносин, збої і порушення в роботі глобальних інформаційних і телекомунікаційних систем та інформаційних систем компаній-партнерів (контрагентів) та ін.;

– внутрішніх, як-от помилки і халатність персоналу підприємства, а також порушення, які навмисно допускаються, збої і порушення в роботі власних інформаційних систем та ін.

Отже, управління інформаційною безпекою на кожному окремому підприємстві має здійснюватися в контексті його загальної господарської діяльності: з урахуванням характеру діяльності компанії (технології виробництва, специфіки ринків збуту тощо), а також як фактично складається ситуація у ринковій конкурентній боротьбі, державній політиці, розвитку правової та правоохоронної системи, рівня розвитку окремих використовуваних інформаційних і телекомунікаційних технологій та інших факторів, що формують загальні умови поточної діяльності.

Формальною підставою (передумовою) для здійснення цілеспрямованої діяльності у сфері захисту інформації, крім загальнодержавних вимог до захисту інформації, що становить державну, військову, лікарську та банківську таємницю, також є перелік відомостей, що становлять комерційну таємницю підприємства,

який визначається підприємством самостійно з урахуванням вимог чинного законодавства.

До того ж необхідність розробки і впровадження політики інформаційної безпеки може бути обумовлена такими обставинами:

– необхідність зменшення вартості страхування інформаційних ризиків або певних бізнес-ризиків;

– необхідність впровадження міжнародних стандартів, як-от ISO/IEC 27002.

На рис. 16.1 представлено передумови розробки політики безпеки підприємства.

Рисунок 16.1. Передумови розробки політики безпеки підприємства

16.2. Загальна структура управлінської роботи щодо забезпечення інформаційної безпеки на рівні підприємства

Для нейтралізації наявних загроз і забезпечення інформаційної безпеки підприємства створюють систему менеджменту у сфері інформаційної безпеки, в межах якої проводять роботу за кількома напрямами (рис. 16.2):

– формування та практична реалізація комплексної багаторівневої політики інформаційної безпеки підприємства та системи внутрішніх вимог, норм і правил;

– організація департаменту (служби, відділу) інформаційної безпеки;

– розробка системи заходів і дій на випадок виникнення непередбачуваних ситуацій («Управління інцидентами»);

– проведення аудитів (комплексних перевірок) стану інформаційної безпеки на підприємстві.

Кожен із цих напрямів організаційної роботи має свої особливості і повинен реалізовуватися з використанням специфічних методів менеджменту та відповідно до своїх правил. Політики і правила інформаційної безпеки є організаційними документами, що регулюють діяльність усієї організації або окремих підрозділів (категорій співробітників) у роботі з інформаційними системами

та інформаційними потоками. Департамент інформаційної безпеки є вузькоспеціалізованим підрозділом, який вирішує специфічні питання захисту інформації. Система заходів з реагування на інциденти забезпечує готовність усієї організації (включно з Департаментом інформаційної безпеки) до осмислених цілеспрямованих дій у разі будь-яких подій, пов'язаних з інформаційною безпекою. Проведення внутрішніх аудитів інформаційної безпеки (періодичних або пов'язаних із певними подіями) має забезпечити контроль за поточним станом системи заходів щодо захисту інформації, зокрема незалежну перевірку відповідності реального стану справ встановленим правилам і вимогам.

Рисунок 16.2. Структура організаційної діяльності у сфері інформаційної безпеки на підприємстві

Водночас кожен із напрямів діяльності має постійно вдосконалюватися, а конкретні завдання повинні постійно уточнюватися відповідно до змін в організаційній структурі, виробничих процесах або зовнішньому середовищі.

16.3. Формування політики інформаційної безпеки на підприємстві. Структура політики інформаційної безпеки та процес її розробки

Політика інформаційної безпеки являє собою комплекс документів, що відображають усі основні вимоги до забезпечення захисту інформації та напрями роботи підприємства в цій сфері. Під час побудови політики безпеки можна умовно виділити три її основні рівні: верхній, середній і нижній.

Верхній рівень політики інформаційної безпеки підприємства слугує:

– для формулювання і демонстрації ставлення керівництва підприємства до питань інформаційної безпеки та відображення загальних цілей усього підприємства в цій галузі;

– основою для розробки індивідуальних політик безпеки (на більш низьких рівнях), правил та інструкцій, що регулюють окремі питання;

– засобом інформування персоналу підприємства про основні завдання та пріоритети підприємства у сфері інформаційної безпеки.

Політики інформаційної безпеки середнього рівня визначають ставлення підприємства (керівництва підприємства) до певних аспектів його діяльності та функціонування інформаційних систем:

– ставлення і вимоги (більш детально, порівняно з політикою верхнього рівня) підприємства до окремих інформаційних потоків та інформаційних систем, що обслуговують різні сфери діяльності, ступінь їх важливості та конфіденційності, а також вимоги до надійності (наприклад, щодо фінансової інформації, а також інформаційних систем і персоналу, які її стосуються);

– відношення і вимоги до певних інформаційних та телекомунікаційних технологій, методів і підходів до обробки інформації і побудови інформаційних систем;

– відношення і вимоги до співробітників підприємства як до учасників процесів обробки інформації, від яких безпосередньо залежить ефективність багатьох процесів і захищеність інформаційних ресурсів, а також основні напрями і методи впливу на персонал з метою підвищення інформаційної безпеки.

Політики безпеки на найнижчому рівні стосуються окремих елементів інформаційних систем і ділянок обробки та зберігання інформації і описують конкретні процедури і документи, пов’язані із забезпеченням інформаційної безпеки.

Розробка політики безпеки передбачає здійснення низки попередніх кроків:

– оцінку особистого (суб’єктивного) відношення до ризиків підприємства його власників і менеджерів, відповідальних за функціонування і результативність роботи підприємства загалом або окремі напрями його діяльності;

– аналіз потенційно вразливих інформаційних об’єктів;

– виявлення загроз для значимих інформаційних об’єктів (відомостей, інформаційних систем, процесів обробки інформації) і оцінку відповідних ризиків.

Здійснення попередніх кроків (аналізу) дає змогу визначити, наскільки інформаційна безпека загалом важлива для стійкого здійснення основної діяльності підприємства, його економічної безпеки. На основі цього аналізу з урахуванням оцінок менеджерів і власників визначаються конкретні напрями роботи щодо забезпечення інформаційної безпеки. Водночас у деяких випадках особиста думка окремих керівників може і не мати вирішального значення.

Отже, політика інформаційної безпеки (практично на всіх рівнях) у частині роботи з такими даними буде заснована на загальних строго формалізованих правилах, процедурах і вимогах (як-от використання сертифікованого обладнання та програмного забезпечення, проходження процедур допуску, обладнання спеціальних приміщень для зберігання інформації тощо).

Під час розробки політик безпеки всіх рівнів необхідно дотримуватися основних правил:

– Політики безпеки на більш низьких рівнях повинні повністю підпорядковуватися відповідній політиці верхнього рівня, а також чинному законодавству і вимогам державних органів.

– Текст політики безпеки повинен містити тільки чіткі і однозначні формулювання, що не допускають подвійного тлумачення.

– Текст політики безпеки повинен бути доступний для розуміння тих співробітників, яким він адресований.

Загалом політика інформаційної безпеки повинна давати чітке уявлення про необхідну поведінку користувачів, адміністраторів та інших фахівців під час впровадження та використання інформаційних систем і засобів захисту інформації, а також під час здійснення інформаційного обміну та виконання операцій з обробки інформації. До того ж із політики безпеки, якщо вона належить до певної технології та/або методології захисту інформації, повинні бути зрозумілі основні принципи роботи цієї технології. Важливою функцією політики безпеки є чітке розмежування відповідальностей у процедурах інформаційного обміну: всі зацікавлені особи повинні ясно усвідомлювати межу як своєї відповідальності, так і відповідальності інших учасників відповідних процедур і процесів. Також одним із завдань політики безпеки є захист не тільки інформації та інформаційних систем, а й захист самих користувачів (співробітників підприємства і його клієнтів і контрагентів).

Загальний життєвий цикл політики інформаційної безпеки включає в себе ряд основних кроків:

– проведення попереднього дослідження стану інформаційної безпеки;

– власне розробку політики безпеки;

– впровадження розроблених політик безпеки;

– аналіз дотримання вимог впровадженої політики безпеки та формулювання вимог щодо її подальшого вдосконалення (повернення до першого етапу, на новий цикл вдосконалення).

Цей цикл (рис. 16.3) може повторюватися кілька разів з метою вдосконалення організаційних заходів у сфері захисту інформації та усунення виявлених недоробок.

Політика інформаційної безпеки підприємства: верхній рівень

Політика інформаційної безпеки верхнього рівня фактично є декларацією керівників і/або власників підприємства про необхідність вести цілеспрямовану роботу із захисту інформаційних ресурсів, що має стати основою для більш успішного функціонування підприємства в основному напрямі його діяльності, а також усунути різні ризики, які можуть призвести до фінансових втрат, збитку

для репутації підприємства, адміністративного і кримінального переслідування керівників та інших негативних наслідків.

Політика інформаційної безпеки на цьому рівні може визначати й описувати:

– власне рішення про здійснення цілеспрямованої систематичної діяльності щодо забезпечення інформаційної безпеки підприємства;

– перелік основних інформаційних ресурсів, як-от інформаційні системи, масиви даних, інформація про окремі факти та явища (конструкторські розробки, комерційні угоди, результати НДДКР тощо), захист яких має найбільший пріоритет для всього підприємства;

– загальний підхід до розподілу відповідальності за забезпечення інформаційної безпеки всередині організації;

– необхідність для всього персоналу дотримуватися певних запобіжних заходів під час роботи з інформацією та інформаційними системами, підвищувати свою кваліфікацію в цій області і усвідомлювати міру відповідальності за можливі порушення;

– відношення керівництва підприємства до фактів порушення вимог щодо забезпечення інформаційної безпеки та осіб, що чинять такі порушення, а також загальний підхід до їх переслідування в разі виявлення таких фактів.

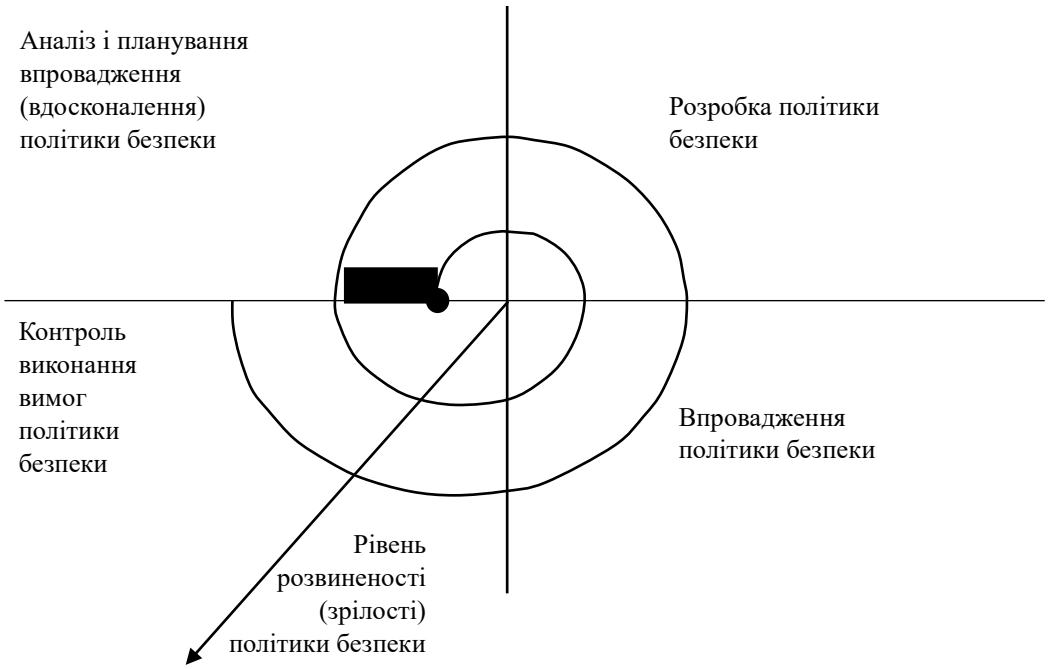

Рисунок 16.3. Цикли розвитку і вдосконалення політики перенабрати

Одним із завдань політики верхнього рівня є формулювання і демонстрація того, що захист інформації є одним із ключових механізмів забезпечення конкурентоспроможності підприємства та обумовлює як його здатність досягати поставлених цілей, так іноді і здатність виживання і збереження можливості продовжувати діяльність. Для цього можуть бути позначені пріоритетні

напрями господарської діяльності та відповідні їм інформаційні системи і потоки інформації, описаний причинно-наслідковий зв'язок між можливими порушеннями конфіденційності та/або порушеннями в стабільній роботі інформаційних систем, з одного боку, та порушеннями нормального перебігу поточних господарських операцій, з іншого боку. На основі цього можуть бути визначені пріоритетні напрями діяльності щодо забезпечення інформаційної безпеки. Найбільшою мірою залежність загальної ефективності діяльності від інформаційної безпеки характерна для компаній, які:

– займаються так званою електронною комерцією або працюють у суміжних сферах (електронні платежі, інтернет-реклама тощо);

– безпосередньо пов'язані з обігом (створенням, купівлею-продажем, охороною, оцінкою) об'єктів інтелектуальної власності, зокрема наукомістких технологій;

– безпосередньо пов'язані із обігом великих обсягів інформації, що становить таємницю інших осіб (банки, медичні установи, аудиторські компанії тощо).

Водночас робота над політикою інформаційної безпеки повинна включати в себе не тільки її початкову розробку, але й постійний моніторинг загроз, змін у зовнішньому середовищі для подальшого уточнення (або навіть повної переробки) політики відповідно до змінення умов роботи.

Політика інформаційної безпеки підприємства: середній рівень

Політики інформаційної безпеки середнього рівня безпосередньо деталізують вимоги, завдання та правила, позначені в політиці верхнього рівня, і окремо описують основні сфери, в яких необхідне системне здійснення тих чи інших організаційних і/або технічних заходів.

Політика інформаційної безпеки середнього рівня повинна містити такі основні розділи:

– Загальний опис тієї сфери діяльності (інформаційної технології, аспекту інформаційної системи, бізнес-процесів підприємства), на яку вона поширюється.

– Область застосування політики безпеки – перелік усіх осіб, організацій, інформаційних систем, до яких вона застосовується або які виключаються зі сфери її застосування.

– Безпосереднє відношення підприємства до цього аспекту інформаційних технологій та інформаційної безпеки – основна частина політики безпеки, що визначає конкретні правила, критерії та вимоги до процедур обігу інформації, елементів інформаційної інфраструктури, програмних і апаратних засобів тощо.

– Розподіл ролей і функцій, необхідних для вирішення конкретних питань – закріплення за певними співробітниками (фахівцями, керівниками) обов'язків з виконання необхідної роботи з метою вирішення завдань у межах цієї політики безпеки.

– Порядок вирішення питань, що виникають, – під час основних процедур вирішення з'являються труднощі у поточній роботі і прийнятті рішень про

можливі винятки з загальних правил, а також перелік осіб (підрозділів), відповідальних за безпосередню роботу з персоналом підприємства з питань, що належать до цієї політики безпеки.

Однією з основ для реалізації заходів у сфері інформаційної безпеки і детальної розробки політики безпеки є укрупнена класифікація інформаційних ресурсів, наявних на підприємстві. Усі наявні на підприємстві інформаційні об'єкти (і відповідні елементи інформаційної інфраструктури) зазвичай можуть бути розділені на п'ять або шість основних груп за рівнем своєї значимості і конфіденційності:

1. Критично важлива (абсолютно секретна) інформація – інформація, що вимагає особливих гарантій безпеки.

2. Важлива інформація (інформація, що становить комерційну таємницю) – інформація, яка використовується тільки всередині підприємства, порушення конфіденційності якої може завдати серйозної шкоди самому підприємству або його партнерам.

3. Значна (конфіденційна) інформація – інформація, призначена для використання обмеженим колом співробітників і керівників підприємства.

4. Персональна інформація – інформація про співробітників, що не підлягає розголошенню.

5. Інформація для внутрішнього використання – інформація для використання всередині підприємства, порушення конфіденційності якої не може завдати шкоди.

6. Інша інформація – відкрита інформація, конфіденційність якої не має особливого значення для діяльності підприємства.

У всьому обсязі політик середнього рівня необхідно виділити два їх основні види:

1. Політики, які належать до визначених сфер діяльності підприємства і відповідних інформаційних потоків (фінансів, комерційної діяльності тощо).

2. Політики, які належать до певних аспектів використання інформаційних технологій, організації інформаційних потоків та організації роботи персоналу на всьому підприємстві – незалежно від тієї сфери, де використовуються ці технології або зайнятий персонал.

До політик **першого типу** можуть належати:

– політики поводження з інформацією, що становить державну таємницю;

– політики поводження з результатами науково-дослідної, конструкторської та технологічної документації, що становить «ноу-хау» підприємства або його партнерів та інші.

Політики безпеки такого типу уточнюють і доповнюють загальні для всього підприємства правила, що поширюються на всі інші інформаційні системи та

об’єкти і відповідно мають найбільший пріоритет. Вони, наприклад, можуть містити:

– спеціальні вимоги до резервного копіювання інформації (як-от більш висока частота резервного копіювання та використання більш надійних носіїв для цього);

– спеціальні вимоги до ідентифікації і автентифікації користувачів (як-от комбінування біометричної ідентифікації та ідентифікації за допомогою паролів);

– спеціальні вимоги до копіювально-розмножувальної техніки, використовуваної для роботи з конфіденційною інформацією;

– спеціальні вимоги до приміщень, у яких проводяться наради з секретної тематики і обробляється відповідна інформація (товщина і матеріал стін, розташування приміщень у будівлях, захищеність вікон, надійність дверей і замків, а також охоронної та пожежної сигналізації, обстеження на предмет виявлення підслуховуючих пристроїв тощо) та інші.

До політик **другого типу** можуть належати:

– політика опублікування відкритих інформаційних матеріалів, зокрема політика організації вебсайта підприємства і його внутрішнього інформаційного порталу (в частині запобігання можливих витоків і спотворень інформації);

– політика використання мережі Інтернет (у частині запобігання можливих витоків інформації);

– політики використання окремих інформаційних і комунікаційних технологій, зокрема спільні для всього підприємства правила використання мобільних комп’ютерів і КПК, віддаленого доступу до корпоративної інформаційної системи, а також використання особистих комп’ютерів співробітників підприємства у службових цілях;

– класифікації інформаційних систем, інформаційних ресурсів та об’єктів інформації з погляду їх значимості і зусиль, які необхідно вживати для їх захисту;

– політика придбання, установки, модифікації та оновлення програмного забезпечення, а також аутсорсингу розробки і проєктування програмного забезпечення;

– політика закупівлі апаратних засобів інформаційних систем, систем інформаційної безпеки;

– політика використання користувачами власного програмного забезпечення (тобто ПЗ, яке самостійно розробляється підприємством);

– загальні для всього підприємства правила використання паролів та інших засобів персональної ідентифікації;

– політика використання електронно-цифрового підпису та інфраструктури відкритих ключів;

– політика (регламент) забезпечення внутрішньо-об’єктного режиму і фізичної захищеності інформаційних активів;

– політика доступу до внутрішніх інформаційних ресурсів сторонніх користувачів (організацій);

– загальний для всього підприємства порядок притягнення до відповідальності за порушення певних правил інформаційної безпеки.

Політика інформаційної безпеки підприємства: нижній рівень

Цей рівень включає в себе документи, які є інструкціями і методиками прямої дії, що використовуються в повсякденній діяльності співробітників підприємства. Ці документи належать до окремих сервісів, процедур та інформаційних систем. Основним завданням розробки організаційної документації на цьому рівні є забезпечення якомога більш детального і формалізованого опису всіх процедур і вимог, що належать до забезпечення безпеки окремих елементів інформаційних систем, інформаційних потоків і масивів інформації. Зокрема, для забезпечення повноти формування політики інформаційної безпеки підприємства необхідно сформувати якомога більш повний комплект організаційної документації, що включає в себе:

– бланки типових заявок на надання доступу окремих співробітників до певних інформаційних ресурсів та інформаційних систем, а також регламенти надання такого доступу;

– регламенти (процедури) роботи з певними інформаційними і телекомунікаційними системами, програмним забезпеченням і базами даних;

– посадові обов'язки окремих категорій співробітників щодо забезпечення інформаційної безпеки, а також вимоги, що пред'являються до персоналу;

– типові договори з зовнішніми контрагентами, пов'язані з передачею або отриманням інформації, або основні вимоги, що пред'являються до таких договорів.

Процедурні документи, які стосуються надання доступу до ресурсів (як-от мережа Інтернет, корпоративні інформаційні системи і бази даних, апаратні засоби, засоби передачі інформації тощо) можуть включати як типові бланки заявок на надання доступу, так і опис основних процедур (регламенту) прийняття рішень про надання такого доступу та надання конкретних прав під час роботи з інформаційними ресурсами, а також переліки критеріїв, необхідних для надання тих чи інших прав в інформаційних системах.

Процедури роботи з окремими інформаційними системами і/або модулями інформаційних систем (базами даних, модулями корпоративної ERP-системи, системами електронного документообігу тощо) можуть враховувати всі основні вимоги, правила і обмеження, наприклад, заборону використовувати дискети для копіювання та перенесення інформації або обмеження, що накладаються на можливість віддаленого доступу до тих чи інших інформаційних сервісів. Вимоги і правила, пов'язані із забезпеченням інформаційної безпеки, можуть бути включені як у загальні інструкції з використання інформаційних систем або регламенти здійснення бізнес-процесів, так і в оформлені у вигляді спе-

ціальних інструкцій і пам'яток, що містять виключно вимоги і правила інформаційної безпеки.

Посадові обов'язки персоналу підприємства, пов'язані із забезпеченням інформаційної безпеки, повинні входити до посадових інструкцій для кожного співробітника. До того ж політика безпеки може передбачати підписання (як під час вступу на роботу або переведення на певну посаду, так і під час звільнення з неї) окремими категоріями персоналу додаткових угод, зобов'язань і підписок про нерозголошення певної інформації. Також політика безпеки може вводити додаткові вимоги до персоналу, що працює з певними відомостями або інформаційними системами. Прикладами таких обмежень можуть бути відсутність судимості, наявність певних навичок або спеціальної кваліфікації, проходження професійної сертифікації або психологічної перевірки.

Політики безпеки, що стосуються роботи з зовнішніми контрагентами, можуть передбачати типові форми і окремі інструкції щодо складання комерційних контрактів (для кожного типу контрактів, а також для окремих груп контрагентів) і обміну інформацією з постачальниками, покупцями, консультантами, посередниками, субпідрядниками, постачальниками фінансових та інформаційних послуг та іншими учасниками господарської діяльності. Зокрема, в політиці для кожної з цих категорій може передбачатися специфічний порядок інформаційного обміну, взаємні вимоги щодо забезпечення конфіденційності і можливих заходів відповідальності в разі порушення узгоджених вимог будь-якої зі сторін.

У тих випадках, коли певна політика безпеки описує складну інформаційну систему і систему захисту інформації, призначену для виконання найбільш відповідальних операцій (наприклад, електронні грошові перекази), вона може бути поділена на два складники:

– внутрішній регламент роботи підрозділів (груп, адміністраторів), що відповідають за виконання найбільш важливих адміністративних функцій (наприклад, видача та обслуговування електронних сертифікатів Інфраструктури публічних ключів);

– політику, яка безпосередньо відображає вимоги до користувачів і процесів, а також опису процедур роботи та взаємодії всіх учасників інформаційного обміну.

Контрольні питання:

1. Основні етапи розробки політики безпеки підприємства.

2. Назвіть основні аспекти управлінської роботи щодо забезпечення інформаційної безпеки на рівні підприємства.

3. Назвіть основні кроки загального життєвого циклу політики інформаційної безпеки підприємства.

ТЕМА 17
ЗМІСТ ДЕТАЛІЗОВАНОЇ ПОЛІТИКИ БЕЗПЕКИ

Політика інформаційної безпеки – набір вимог, правил, обмежень, рекомендацій, які регламентують порядок інформаційної діяльності в організації і спрямовані на досягнення і підтримку стану інформаційної безпеки організації. Політика безпеки інформації є частиною загальної політики безпеки організації і повинна успадковувати основні її принципи. Головною причиною запровадження політики безпеки зазвичай є вимога наявності такого документа від регулятора – організації, що визначає правила роботи підприємств цієї галузі. У цьому випадку відсутність політики може спричинити репресивні дії щодо підприємства або навіть повне припинення його діяльності.

У темі описується основний зміст розділів політики безпеки за окремими напрямами захисту інформації.

Ключові слова: *порушення інформаційної безпеки, збиток, виявлення порушень, аналіз, програмні засоби, група реагування, інформаційний сервіс, ділова репутація, distributed, service, DDoS, інтернет, сервер, прийняття рішень, інформаційні системи, атака, ймовірність, загроза інформаційній безпеці, розмежування доступу, ідентифікація, політика безпеки, пошук, доступ, державна таємниця, інформація, мережа, ідентифікація і автентифікація, аутсорсинг, політика використання, передача даних, CDMA, PDA, бази даних, апаратні засоби, прийняття рішень.*

План

17.1. Організація внутрішньооб’єктного режиму і охорони приміщень.

17.2. Фізичний захист.

17.3. Організація режиму секретності в установах і на підприємствах.

17.1. Організація внутрішньооб’єктного режиму і охорони приміщень

Організація внутрішньооб’єктного режиму, охорони приміщень і територій є частиною загальної роботи підприємства щодо забезпечення збереження майна та безперервності поточної діяльності. Основним завданням забезпечення внутрішньооб’єктного режиму є недопущення сторонніх осіб до інформаційних активів і запобігання загрозам інформаційній безпеці. Основою внутрішньооб’єктного режиму є пропускний режим, у межах якого зазвичай встановлюються:

– документи, що дають право проходу на територію підприємства (пропуск і карта доступу, видані самим підприємством, і документи, видані сторонніми організаціями, – службові посвідчення посадових осіб деяких органів державної влади);

– категорії перепусток, які використовуються на підприємстві, відповідно до яких обмежується термін дії перепусток, час можливого проходу на територію підприємства (дні тижня, години доби) і деякі інші параметри;

– порядок видачі, обміну, продовження і вилучення перепусток, а також порядок дій співробітників і посадових осіб у разі втрати пропуску;

– порядок організації пропуску осіб, автотранспорту і проносу (провозу) майна: розміщення і порядок роботи контрольно-пропускних пунктів, можливість пропуску тих чи інших осіб, засобів автотранспорту і вантажів через ті чи інші КПП та ін.;

– основні положення документообігу, використовуваного для проходу відвідувачів на територію підприємства (вимоги до ведення журналу реєстрації проходу відвідувачів, вимоги до документів, на основі яких видаються разові перепустки, порядок видачі разових перепусток тощо);

– порядок огляду транспортних засобів, що допускаються на територію підприємства.

До того ж у межах організації внутрішньооб'єктного режиму може бути передбачено поділ приміщень і територій на окремі зони з обмеженням доступу (зокрема на основі поділу приміщень і територій на різні категорії), а також розмежування доступу окремих співробітників (категорій персоналу) і відвідувачів у різні зони; також можуть бути визначені основні вимоги до технічних засобів розмежування доступу і організації їх використання.

З технічного погляду заходи щодо забезпечення пропускного та внутрішньооб'єктного режимів можуть бути реалізовані тими ж засобами, які використовуються для забезпечення безпеки в інших сферах, крім інформаційної (захист майна та персоналу, забезпечення безперервності виробничого процесу), – засобами контролю доступу, відеоспостереження, сигналізації і фізичного захисту.

В основі засобів контролю доступу лежать механізми розпізнавання особистості і порівняння зі встановленими параметрами. Політика підприємства може встановлювати як спрощені підходи до розпізнання, коли охоронці підприємства перевіряють документи (підтвердження особи, підтвердження можливості проходу на територію у визначений час через визначений КПП), так і використання автоматизованих засобів, коли впізнання відвідувача і підтвердження (або заборона) можливості проходу на територію (виходу з території, з будівлі) проводиться автоматизованою системою контролю доступу на основі наявних у відвідувача машинозчитних засобів персональної ідентифікації (пластикових карт, жетонів тощо) або на основі зчитування і аналізу його фізичних особливостей (геометрії особи, відбитків пальців, малюнка райдужної оболонки ока, голосу та ін.).

Під час вибору конкретних засобів біометричної ідентифікації фахівцям і керівникам підприємства варто пам'ятати, що різні технології мають різний

ступінь надійності, а також можуть бути більш-менш зручними в повсякденному використанні великою кількістю людей. Так, наприклад, вважається, що одна з передових технологій біометричної ідентифікації – ідентифікація за кровоносними судинами пальця (коли інфрачервоний промінь просвічує палець і створює тривимірне зображення унікальної для кожної людини структури кровоносних судин).

17.2. Фізичний захист

Фізичний захист об'єктів зазвичай передбачає посилення конструкцій огорож, елементів будівель, споруд і окремих приміщень. До таких засобів належать захист віконних прорізів металевими ґратами і віконницями, спеціальне скління вікон, використання броньованих дверей, запірних пристроїв, сейфів для зберігання засобів обчислювальної техніки і носіїв інформації. Відповідно до особливостей використовуваних приміщень і територій політика безпеки підприємства також може передбачати розташування місць зберігання і обробки інформації (наприклад, архівів або серверних кімнат) у приміщеннях, найменш доступних для проникнення, найбільш віддалених від місць зберігання вибухонебезпечних і легкозаймистих речовин, найменш схильних до затоплення (для об'єктів, розташованих у долинах річок і на узбережжі), найбільш захищених від ударів блискавки та ін.

Із фізичним захистом безпосередньо пов'язано використання засобів сигналізації та відеоспостереження. Залежно від характеру об'єкта, що охороняється (територія, будівля, прохід, приміщення, окрема шафа або сейф) у засобах сигналізації можуть застосовуватися датчики, що працюють на різних фізичних принципах (фотоелектричні датчики, датчики об'єму, акустичні датчики тощо), що мають різні налаштування і використовують різні канали зв'язку.

На відміну від засобів сигналізації, засоби відеоспостереження дають змогу не тільки встановити факт порушення, а й у деталях відстежувати його, контролювати ситуацію, а також вести відеозапис, який можна буде використовувати для вжиття наступних заходів (пошук порушників, кримінальне переслідування та ін.).

Окремим завданням є забезпечення інформаційної безпеки під час транспортування носіїв інформації та інших об'єктів, що вимагає використання і спеціальних організаційних прийомів, і спеціальних технічних засобів. До організаційних методів належить залучення спеціально підготовлених кур'єрів, а також поділ носіїв інформації (об'єктів) на частини і їх окреме транспортування з метою мінімізації можливостей витоку інформації. До технічних засобів, що застосовуються під час транспортування об'єктів, належать захищені контейнери, спеціальні пакувальні матеріали, а також тонкоплівкові матеріали і голографічні мітки, що дають змогу ідентифікувати справжність об'єктів і контролювати несанкціонований доступ до них.

17.3. Організація режиму секретності в установах і на підприємствах

Організація режиму секретності в установах і на підприємствах ґрунтується на вимогах законодавства, що стосується питань державної таємниці, і відповідних підзаконних актів. Відповідно до чинних норм до державної таємниці може бути віднесена інформація, що стосується обороноздатності країни, її економіки, міжнародних відносин, державної безпеки та охорони правопорядку (зокрема і відомості про методи та засоби захисту секретної інформації, а також про державні програми і заходи в області захисту державної таємниці); в законодавстві також спеціально уточнюються сфери діяльності, інформація про які не може бути віднесена до державної таємниці. Віднесення конкретної інформації до державної таємниці здійснюється рішенням спеціально призначених посадових осіб, а загальний Перелік відомостей, віднесених до державної таємниці, затверджується Президентом і підлягає обов'язковому опублікуванню. Для відомостей, що становлять державну таємницю, встановлюються три ступені секретності: «особливої важливості», «цілком таємно» та «таємно», а носії таких відомостей (документи) повинні мати відповідні реквізити.

Основним елементом організації режиму секретності є допуск посадових осіб і громадян до відомостей, що становлять державну таємницю. Він передбачає виконання керівництвом підприємства і підрозділів із захисту державної таємниці (у взаємодії з уповноваженими правоохоронними органами) таких основних заходів:

– Ознайомлення посадових осіб і громадян з нормами законодавства, які передбачають відповідальність за порушення вимог.

– Отримання згоди на тимчасові обмеження їх прав відповідно до законодавства.

– Отримання згоди на проведення щодо них заходів перевірки.

– Прийняття рішення про допуск до відомостей, що становлять державну таємницю.

– Висновок щодо осіб, які отримали допуск, що відображає взаємні зобов'язання таких осіб і адміністрації підприємства (зокрема зобов'язання таких осіб перед державою з нерозповсюдження довірених їм відомостей, що становлять державну таємницю).

Крім віднесення відомостей до державної таємниці та допуску посадових осіб і громадян до засекречених відомостей, важливим елементом системи забезпечення режиму секретності є організація інформаційного обміну між підприємствами у разі спільного виконання робіт. Зокрема, передача засекречених відомостей від одного підприємства до іншого має проводитися з дозволу уповноваженого державного органу, договір на виконання робіт повинен передбачати зобов'язання сторін щодо забезпечення схоронності відомостей, а замовник

робіт повинен контролювати виконання нормативних вимог контрагентами за такими договорами (наявність ліцензій, оформлення допуску співробітників та ін.) і вживати необхідних заходів у разі виявлення порушень. Також важливим елементом забезпечення режиму секретності є організація передачі відомостей, що становлять державну таємницю, іншим державам (зокрема ознайомлення з такими відомостями і надання можливості доступу до них).

Політика опублікування матеріалів у відкритих джерелах (як-от газети, журнали, виставки, мережа Інтернет, радіо- і телепередачі, конференції, музейні експозиції тощо) має забезпечувати запобігання випадкових і організованих витоків конфіденційної інформації під час взаємодії підприємства із засобами масової інформації, громадськими та державними органами, науковими, академічними і бізнес-спільнотою. Для того, щоб уникнути шкоди інтересам підприємства, така політика має містити основні правила і процедури підготовки інформаційних матеріалів до відкритої публікації. Зокрема, в політиці безпеки треба передбачати створення спеціальної експертної ради, відповідальної за розгляд усіх інформаційних матеріалів, які передбачається опублікувати у відкритих джерелах (політика безпеки має містити конкретні обмеження на опублікування інформаційних матеріалів без їх розгляду експертною радою). Основним завданням такої ради є підготовка висновків про можливість або неможливість опублікування певних інформаційних матеріалів, а також підготовка конкретних пропозицій щодо вилучення певних відомостей з матеріалів, підготовлених до публікації. У разі відсутності єдиної думки у членів експертної комісії рішення про можливість опублікування може бути прийнято керівником підприємства з урахуванням рекомендацій експертів. Для ефективного вирішення завдань члени експертної ради повинні детально знати всі наявні обмеження (зокрема встановлені законодавством) і володіти ситуацією в тій сфері, в якій функціонує підприємство. Водночас зазвичай сам автор підготовлених до публікації матеріалів не може входити до експертної ради, а редактор або керівник, який відповідає за підготовку матеріалів, не може бути головою експертної ради.

Політика управління паролями (або, у більш загальному вигляді, політика ідентифікації і автентифікації) може визначати періодичність заміни паролів, дії, які необхідно здійснити під час компрометації паролів, основні вимоги до їх якості, процедур їх генерації, розподілу основних обов'язків, пов'язаних із генерацією паролів, їх зміною і доведенням до користувачів, а також основні заходи відповідальності за порушення встановлених правил і вимог. Політика на цьому рівні також може встановлювати заборону зберігання записаних паролів, заборона повідомляти будь-кому свій пароль (зокрема керівникам і адміністраторам інформаційних систем) та інші аналогічні обмеження.

Політика встановлення та оновлення версій програмного забезпечення може включати в себе деякі обмеження на самостійне придбання і установку

програмного забезпечення окремими підрозділами та користувачами, а також певні вимоги до кваліфікації фахівців, які здійснюють їх установку, налаштування і підтримку.

Політика придбання інформаційних систем та їх елементів (програмних і апаратних засобів) може включати в себе вимоги до ліцензування та сертифікації використовуваного програмного забезпечення і устаткування, а також певні вимоги до фірм, які здійснюють їх поставку та впровадження.

Політика доступу сторонніх користувачів (організацій) в інформаційні системи підприємства може містити перелік основних ситуацій, коли такий доступ можливий, а також основні критерії і процедури, відповідно до яких здійснюється доступ. Також політика може передбачати розподіл відповідальності співробітників самого підприємства за дії зовнішніх користувачів, які отримують такий доступ.

Політика щодо розробки ПЗ може містити вимоги як до питань безпеки і надійності програмних засобів, самостійно розроблених підприємством, так і щодо передачі розробки програмних засобів (модулів інформаційних систем, окремих програмних бібліотек і т. ін.) стороннім спеціалізованим організаціям (так званий «аутсорсинг»), а також щодо придбання та використання тиражованих програмних бібліотек (модулів), які розповсюджуються компаніями-виробниками. Зокрема, політика може містити вимоги до тестування самостійно розробленого ПЗ, аналізу його вихідних кодів, описувати основні критерії надійності і т. ін.

Політики використання окремих універсальних інформаційних технологій у масштабі всього підприємства можуть включати в себе:

– політику використання електронної пошти (e-mail);

– політику використання засобів шифрування даних;

– політику захисту від комп'ютерних вірусів і інших шкідливих програм;

– політику використання модемів і інших аналогічних комунікаційних засобів;

– політику використання інфраструктури публічних ключів;

– політику використання технології віртуальних приватних мереж (Virtual Private Network – VPN).

Політика використання електронної пошти може включати в себе як загальні обмеження на її використання певними категоріями співробітників, так і вимоги до управління доступом і збереження конфіденційності повідомлень, а також до адміністрування поштової системи і зберігання електронних повідомлень. До того ж політика може передбачати:

– заборону на використання електронної пошти в особистих цілях;

– спеціальні вимоги до відправлення та одержання приєднаних файлів, які потенційно можуть містити шкідливі програми;

– заборону на використання електронної пошти тимчасовими співробітниками;

– вимоги шифрування переданих повідомлень;

– спостереження за всіма переданими і одержуваними повідомленнями;

– обмеження на передачу конфіденційної інформації за допомогою електронної пошти та інші положення.

Політика використання комунікаційних засобів може визначати межі використання технологій, що дають змогу підключити комп'ютери та інформаційні системи підприємства до інформаційних систем і комунікаційних каналів за його межами. Зокрема, така політика може вводити певні обмеження на використання модемів для телефонних ліній, пристроїв, що використовують сучасні бездротові технології, як-от GSM (GPRS), Wi-Fi, передача даних у мережах стандарту CDMA і т. ін.

Політика використання мобільних апаратних засобів може ставитися до різних пристроїв, як-от мобільні ПК, КПК (PDA), переносні пристрої зберігання інформації (дискети, USB-flash, карти пам'яті, що підключаються, жорсткі диски тощо). Вона може відображати загальне ставлення підприємства до використання співробітниками таких пристроїв, визначати вимоги і встановлювати конкретні області, в яких їх використання допустимо. Також можуть встановлюватися додаткові загальні вимоги до стаціонарного обладнання з метою обмеження підключення до них мобільних комп'ютерів і засобів передачі даних.

Контрольні питання:

1. Організація внутрішньооб'єктного режиму.

2. Що ви можете сказати про фізичний захист забезпечення інформаційної безпеки?

3. Побудова політики інформаційної безпеки на підприємстві.

ТЕМА 18
ДЕПАРТАМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ І РОБОТА З ПЕРСОНАЛОМ

У темі описується робота департаменту інформаційної безпеки як основної структурної одиниці, що відповідає за комплексний захист інформації на підприємстві. Розкривається внутрішня структура департаменту, основні завдання та напрями його діяльності, методи роботи. Також розкриваються основні аспекти роботи з персоналом підприємства, спрямованої на захист інформаційних активів (як у частині підбору і розстановки співробітників, пов'язаних з обробкою інформації, так і в частині поточної роботи з персоналом).

Ключові слова: *управління інформаційної безпекою, CISO, джерело загрози, інформаційні системи, державна таємниця, державна стратегія, аналіз, контроль поведінки, розподіл функцій, доступ, зловмисник.*

План

18.1. Департамент інформаційної безпеки.

18.2. Організаційна структура та персонал департаменту інформаційної безпеки.

18.3. Робота з персоналом підприємства.

18.1. Департамент інформаційної безпеки

Департамент інформаційної безпеки (далі – департамент) підприємства є самостійним структурним підрозділом підприємства, безпосередньо виконує ключові функції захисту інформаційних ресурсів.

Його основними завданнями зазвичай є:

– організація та координація робіт із забезпечення комплексного захисту інформації на підприємстві;

– контроль за виконанням встановлених вимог та оцінка ефективності роботи підрозділів і персоналу підприємства щодо забезпечення інформаційної безпеки;

– виконання окремих адміністративних і технічних функцій щодо забезпечення інформаційної безпеки;

– формування, підтримка та документальне забезпечення політики інформаційної безпеки на всіх рівнях;

– впровадження різних засобів захисту інформації;

– адміністрування окремих інформаційних систем.

Склад завдань департаменту і його внутрішня організаційна структура в кожному конкретному випадку визначається такими особливостями функціонування підприємства:

– значимість інформаційних ресурсів у роботі підприємства і характер наявних загроз;

– ставлення керівництва і власників підприємства до питань інформаційної безпеки та їх управлінська кваліфікація;

– функціональність і характер використовуваних інформаційних систем, їх роль у бізнес-процесах;

– організація роботи та структура IT-служби;

– фінансовий стан підприємства.

Отже, рішення про склад і структуру департаменту в кожному випадку має бути індивідуальним і враховує всі основні умови.

Функції, пов'язані **з формуванням, підтримкою і документальним забезпеченням політики інформаційної безпеки підприємства,** можуть включати в себе:

– консультування керівників і власників підприємства з питань розробки та вдосконалення політики інформаційної безпеки;

– самостійну розробку політики безпеки, її узгодження і подання її керівництву підприємства для затвердження, а також внесення необхідних змін у міру зміни умов роботи підприємства;

– самостійну розробку політик безпеки, що стосуються окремих питань захисту інформації (правил застосування телекомунікаційних технологій, вимог, обов'язкових для всіх персональних комп'ютерів, що використовуються на підприємстві, тощо);

– формування вимог і регламенту процедур перегляду політики безпеки, окремих правил, типових форм та інших документів;

– аналіз окремих договорів і угод зі сторонніми організаціями (постачальниками, покупцями, партнерами з проведення науково-дослідних робіт тощо) на предмет відповідності вимогам політики інформаційної безпеки;

– аналіз та узагальнення передового досвіду та сучасних теорій у сфері управління інформаційною безпекою з метою їх практичного застосування на підприємстві;

– залучення сторонніх фахівців, дослідників, консультантів (консалтингових компаній) для розробки та вдосконалення політики безпеки підприємства та впровадження розвинених методів управління в цій сфері;

– управління навчанням персоналу компанії (контроль за повнотою та правильністю матеріалів навчальних програм, пов'язаних з інформаційною безпекою, забезпечення своєчасності проходження навчання тощо);

– консультування фахівців та керівників підрозділів підприємства з питань відповідності розроблюваних внутрішніх документів окремих підрозділів вимогам політики безпеки підприємства;

– контроль відповідності внутрішніх організаційних документів підприємства (правил внутрішнього розпорядку, посадових інструкцій, інструкцій з використання інформаційних систем, типових форм договорів тощо) вимогам політики інформаційної безпеки, а також узгодження таких документів під час їх затвердження.

Функції, пов'язані з **впровадженням засобів захисту інформації,** можуть включати в себе:

– аналіз сучасних програмних і апаратних засобів захисту інформації та пов'язаних з ними методик захисту, а також ринку доступних засобів захисту інформації, що застосовуються для різних цілей, і підготовка обґрунтованих пропозицій щодо придбання певних продуктів у певних постачальників;

– аналіз закуповуваних інформаційних систем (операційних систем, прикладних програм, телекомунікаційного устаткування, обчислювальної техніки тощо) на предмет їх потенційної надійності і наявності вразливостей;

– залучення сторонніх експертів і консультантів для аналізу закуповуваних і використовуваних засобів захисту інформації з погляду їх надійності, а також із погляду доцільності їх застосування (впровадження);

– формулювання вимог (пов'язаних із забезпеченням інформаційної безпеки) до самостійно розроблюваних програмних продуктів або програмного забезпечення, що створюється на замовлення сторонніх розробників;

– участь у проєктуванні нових інформаційних систем, а також тестуванні знову розроблених і впроваджуваних програмних продуктів;

– розробку техніко-економічного обґрунтування для проєктів впровадження засобів захисту інформації, а також залучення для цих цілей сторонніх аналітиків і консультантів, що спеціалізуються на питаннях аналізу засобів захисту інформації;

– підготовку обґрунтованих рішень про вибір між самостійною розробкою засобів захисту інформації (наприклад, програмних модулів, що здійснюють шифрування даних) і передачею їх розробки стороннім компаніям.

Функції, пов'язані з адмініструванням **інформаційних систем і систем захисту інформації,** можуть включати в себе:

– виконання деяких функцій з адміністрування окремих інформаційних систем (баз даних, систем колективної роботи з документами, поштових систем тощо), а також адміністрування та конфігурування систем захисту інформації (міжмережевих екранів, систем виявлення вторгнень тощо);

– визначення необхідних типових налаштувань і конфігурацій робочих станцій (персональних комп'ютерів), що стосуються інформаційних систем підприємства (зокрема підключених до його локальної мережі);

– залучення сторонніх організацій для здійснення поточного адміністрування інформаційних систем і систем захисту інформації, а також для консуль-

таційної та технічної підтримки у разі виникнення інцидентів, пов'язаних з інформаційною безпекою (зокрема під час здійснення нападів на інформаційні системи підприємства);

– установку (зокрема і спільно з фахівцями IT-підрозділу) програмних і апаратних засобів захисту інформації на робочі місця користувачів і в інші елементи інформаційних систем;

– консультування користувачів з питань, пов'язаних з інформаційною безпекою, і оперативне вирішення проблем;

– реагування на різні інциденти, пов'язані з порушенням інформаційної безпеки;

– прийняття активних зустрічних заходів у разі виявлення вторгнень в інформаційну систему (інформування правоохоронних органів, самостійний пошук нападників тощо);

– генерування паролів користувачів інформаційних систем та забезпечення їх збереження;

– участь у відновленні працездатності інформаційних систем після збоїв та порушень у роботі.

Функції, пов'язані з **контролем виконання вимог політики інформаційної безпеки та проведення аудитів,** можуть включати в себе:

– збір та аналіз відомостей про порушення різних вимог політики безпеки, що надходять з різних джерел (зокрема і від адміністраторів інформаційних систем) і визначення пріоритетних напрямів контрольної роботи;

– перевірку організаційної документації окремих підрозділів підприємства на предмет відповідності вимогам політики інформаційної безпеки (зокрема і своєчасності внесення всіх необхідних змін до чинних внутрішніх документів організації);

– перевірку стану (правильності ведення) поточної господарської та кадрової документації окремих підрозділів підприємства, пов'язаної із забезпеченням інформаційної безпеки (правильності і своєчасності заповнення журналів, своєчасність оформлення зобов'язань про нерозголошення відомостей співробітниками тощо);

– проведення комплексних аудитів інформаційної безпеки на підприємстві;

– організацію контрольних перевірок захищеності окремих елементів інформаційних систем (серверів, сегментів мережі тощо);

– залучення сторонніх організацій для проведення аудитів інформаційної безпеки на підприємстві, перевірок надійності інформаційних систем.

Крім перерахованих функцій, безпосередньо пов'язаних із захистом інформаційних ресурсів, також велике значення має виконання функцій, пов'язаних з охороною майна підприємства і вирішенням завдань, які пов'язані з забезпе-

ченням безпеки підприємства у більш широкому сенсі. Зокрема, для забезпечення інформаційної безпеки має значення виконання таких функцій:

– охорона території та майна підприємства, а також охорона персоналу;

– забезпечення дотримання пропускного режиму;

– спостереження за територією і приміщеннями (зокрема й із допомогою відеокамер);

– контроль за ввезенням на територію підприємства та вивезенням готової продукції, матеріалів, документів та іншого майна;

– організацію внутрішніх службових перевірок та розслідувань, а також взаємодію з правоохоронними органами;

– контроль за дотриманням тимчасового режиму роботи, а також за дотриманням правил внутрішнього розпорядку.

18.2. Організаційна структура та персонал департаменту інформаційної безпеки

На практиці департамент є підрозділом, або безпосередньо підпорядковується першій особі підприємства, або входить, як структурна одиниця, в службу безпеки підприємства. Співробітники департаменту знаходяться в адміністративному та функціональному підпорядкуванні у керівника департаменту, який несе відповідальність за забезпечення інформаційної безпеки на підприємстві. Висновок департаментів інформаційної безпеки зі структури IT-служб на підприємствах є однією з важливих сучасних тенденцій в управлінні бізнесом, інформаційними технологіями та інформаційною безпекою, тому, на думку деяких фахівців, у цих підрозділів є деякі частково взаємосуперечні інтереси, і тому деякі завдання не можуть бути ефективно вирішені в межах одного структурного підрозділу.

У складі департаменту для підвищення ефективності роботи можуть бути виділені самостійні групи (відділи), що спеціалізуються на виконанні певних функцій (рис. 18.1):

– відділ (група, бюро) нормативної (організаційної) документації;

– відділ (група, бюро) адміністрування інформаційних систем;

– відділ (група, бюро) аудиту інформаційної безпеки;

– відділ (група, бюро) впровадження інформаційних систем і систем захисту інформації.

Відділ нормативної документації вирішує завдання, пов’язані з формуванням, підтримкою і документальним забезпеченням політики інформаційної безпеки підприємства, і повинен насамперед включати в себе фахівців з менеджменту та бізнес-аналізу, що пройшли додаткову підготовку у сфері управління інформаційною безпекою. Також до складу такого відділу можуть входити юристи.

Рисунок 18.1. Приклад організаційної схеми Департаменту інформаційної безпеки підприємства

Аналогічний кадровий склад може бути і у **Відділу внутрішнього аудиту інформаційної безпеки.** Водночас до кваліфікації співробітників Відділу нормативної документації зазвичай повинні пред'являтися набагато більш високі професійні вимоги.

Відділ адміністрування інформаційних систем, а також **Відділ впровадження інформаційних систем і захисту систем інформації** зазвичай повинні включати в себе фахівців з інформаційних технологій та засобів захисту інформації, що мають значний досвід впровадження та експлуатації корпоративних інформаційних систем.

18.3. Робота з персоналом підприємства

Практична реалізація всіх положень сформованої політики інформаційної безпеки потребують від підприємства тривалих практичних зусиль. Одним з основних і найбільш складних напрямів роботи є робота з персоналом, цілі якої:

– відбір і попередня перевірка персоналу, прийнятого на роботу (на службу);

– навчання співробітників;

– досягнення взаєморозуміння керівників і співробітників у питаннях забезпечення інформаційної безпеки;

– психологічна підготовка з метою протистояння методам так званої «соціальної інженерії».

Основною причиною, що визначає значущість людського фактора в загальній системі захисту інформації, є те, що незважаючи на всю розвиненість сучасних засобів автоматизації, інформаційні системи, як і раніше, являють собою людино-машинні комплекси, і їх функціонування багато в чому залежить від роботи окремих людей. Саме через це неадекватне поводження службовців підприємства з компонентами інформаційної системи може завдати серйозної шкоди

інформаційній безпеці навіть за наявності детально опрацьованих політик безпеки і високоефективних програмних і апаратних засобів захисту інформації.

Початкова стадія роботи – підбір і розстановка кадрів – може мати кілька аспектів. Основним критерієм для призначення на певні посади, пов'язані з роботою з відомостями, які становлять державну таємницю, є отримання відповідної форми допуску. Відповідно до вимог чинних нормативно-правових актів Перелік посад, під час призначення на які необхідно оформляти спеціальний допуск, встановлюється керівником підприємства і може періодично переглядатися. Ця вимога пов'язана, з одного боку, з тим, що керівник підприємства несе відповідальність за забезпечення режиму секретності, а з іншого – з тим, що для виконання функціональних обов'язків співробітникам підприємства необхідно працювати з певними відомостями, і відповідно мати певний рівень допуску.

Також під час підбору і розстановки кадрів можуть застосовуватися і менш формалізовані методи. Це можуть бути різні методики психологічної оцінки, що включають у себе:

– аналіз мотиваційних аспектів особистості;

– оцінку психологічної стійкості особистості;

– оцінку рівня пізнавальних здібностей особистості (успішність придбання нових знань і навичок і здатність до їх практичного застосування);

– оцінку активності особистості в досягненні поставленої мети, уміння об'єктивно оцінювати ситуацію і людей, вміння виробляти оптимальну стратегію поведінки.

Такий аналіз може бути необхідний як щодо фахівців і керівників, які працюють з інформацією, що підлягає захисту, у зв'язку з виконанням своїх посадових обов'язків за основним профілем роботи підприємства, так і фахівців і керівників, чиїм основним завданням є забезпечення інформаційної безпеки підприємства (аудиторів ІБ, проєктувальників і адміністраторів інформаційних систем та систем захисту інформації тощо).

Крім ретельного підбору, однією з важливих основ роботи з персоналом є його навчання способам забезпечення інформаційної безпеки і безпечній роботі з інформаційними системами. Навчання і наступний контроль отриманих (наявних) знань може бути як первинним, так і повторним. У загальному випадку співробітник підприємства не може бути допущений до виконання своїх посадових обов'язків і роботі з інформаційними системами доти, поки він не пройде навчання з питань інформаційної безпеки і не буде:

– детально ознайомлений з усіма діючими на підприємстві вимогами і загальними правилами;

– повністю навчений методам і прийомам забезпечення інформаційної безпеки, необхідним для виконання його посадових обов'язків;

– ознайомлений з усіма можливими заходами відповідальності (дисциплінарної, адміністративної, кримінальної), які можуть бути до нього застосовані в разі порушення вимог, а також у випадку нанесення шкоди за його вини.

Після завершення всієї попередньої роботи співробітник повинен дати всі необхідні зобов'язання про нерозголошення конфіденційних відомостей, а також письмово засвідчити, що він повністю ознайомлений з основними положеннями політики безпеки. У процесі роботи підприємство також може проводити періодичний контроль знань і навичок, пов'язаний із забезпеченням інформаційної безпеки з тією метою, щоб засвідчити компетентність працівників у цій сфері.

Також одним з інструментів навчання може бути періодичне ознайомлення персоналу з реальними прикладами інцидентів, що недавно відбулися, пов'язаних з інформаційною безпекою. До того ж додаткове навчання персоналу підприємства може проводитись у випадках:

– впровадження нових автоматизованих інформаційних систем;

– зміни бізнес-процесів підприємства;

– зміни вимог політик безпеки (наприклад, через зміни вимог законодавства).

Необхідність додаткового навчання під час впровадження нових інформаційних систем, зокрема інтегрованих систем управління підприємством, зазвичай може бути обумовлена появою нових функціональних можливостей програмного забезпечення і зміною процедур обробки інформації. Також доступ до інтегрованих інформаційних систем потенційно може дати доступ до раніше недоступної інформації та надати раніше відсутні можливості впливати на різні інформаційні потоки. Через це може виникнути потреба в тому, щоб співробітники мали додаткові зобов'язання про дотримання заходів інформаційної безпеки. Аналогічні організаційні заходи щодо забезпечення захисту інформації можуть бути необхідні і під час зміни бізнес-процесів підприємства, коли змінюється його структура, розподіл функцій між підрозділами і обов'язків співробітників, і відповідно, вносяться зміни в організаційні схеми, штатні розписи і посадові інструкції персоналу. Зміни вимог політики безпеки можуть бути пов'язані з появою нових загроз, зміною законодавчих вимог, розширенням ринків, зміною ставлення керівництва і власників підприємства до питань інформаційної безпеки та іншими факторами, – всі ці уточнення і зміни також повинні своєчасно і в повному обсязі доводитися до персоналу.

У процесі навчання певну значимість може мати роз'яснення раціональних причин, з яких підприємство застосовує саме таку політику безпеки. Це може слугувати як для кращого розуміння та засвоєння положень політики безпеки, так і для певної розрядки психологічної напруженості.

Окремим напрямом навчання та підвищення кваліфікації може бути розвиток у персоналу компанії навичок протидії методам соціальної інженерії.

Використання для незаконного проникнення в інформаційні системи методів соціальної інженерії пов'язано з людським фактором, який являє собою сукупність певних психологічних схильностей і особливостей мислення і поведінки, властивих практично всім людям. До таких схильностей і особливостей можна віднести:

– нездатність адекватно оцінити небезпеку в деяких ситуаціях;

– специфічне ставлення до подій, що відбуваються рідко (притуплення уваги);

– зайва довіра і покладання на засоби автоматизації;

– схильність до маніпулювання, що ґрунтується, наприклад, на бажанні допомогти людям (зокрема і незнайомим) або на зайвій довірі людям, одягненим у спеціальну уніформу, тощо.

Саме з використанням деяких подібних психологічних особливостей здійснюється багато найбільш успішних (для нападників) проникнень у корпоративні інформаційні системи. Прикладами таких проникнень є ситуації, коли зловмисник:

– здійснює телефонний дзвінок, представляється адміністратором і, пославшись на певні обставини (наприклад, збій у системі), просить повідомити йому пароль;

– приходить в офіс у спеціальній уніформі (наприклад, у формі співробітника компанії, займається обслуговуванням і ремонтом комп'ютерів) і просить надати йому доступ до інформаційної системи;

– надсилає повідомлення електронною поштою від імені адміністратора інформаційної системи або керівництва підприємства і просить повідомити пароль або вчинити певні дії.

Велику значимість у системі заходів з подолання впливу людського фактора має повсякденна робота з персоналом. Крім навчання персоналу і застосування дисциплінарних заходів впливу, одним з основних завдань такої роботи є постійне нагадування всім співробітникам про необхідність дотримання правил інформаційної безпеки. Конкретні способи, за допомогою яких такі нагадування можуть бути зроблені, будуть залежати від уподобань керівників підприємства, сформованої корпоративної культури, специфіки бізнес-процесів та інших обставин. Характерними способами того, як підприємство може постійно нагадувати своїм співробітникам про необхідність дотримуватися обережності, є:

– розміщення та періодична зміна (оновлення дизайну та змісту) нагадувань про необхідність дотримуватися вимог політики інформаційної безпеки на предметах, які постійно перебувають у полі зору співробітників протягом робочого дня: настінних і настільних календарях, кавових чашках, обкладинках блокнотів, настільних експонатах, ручках, олівцях та іншому канцелярському приладді;

– періодична розсилка відповідних брошур, бюлетенів і буклетів, а також повідомлень по електронній пошті;

– використання скринсейверів, що містять відповідні нагадування;

– використання голосової пошти і гучного зв'язку для періодичної передачі повідомлень про необхідність дотримання правил інформаційної безпеки тощо.

Отже, комплекс всіх організаційних заходів з роботи з персоналом підприємства, що включає в себе систему навчання персоналу, систему притягнення порушників до відповідальності, і постійне підтримання атмосфери відповідального ставлення до питань безпеки, повинен певною мірою зменшити негативний вплив людського фактора на захищеність інформаційних систем і стан інформаційної безпеки.

Контрольні питання:

1. Назвіть основні завдання департаменту інформаційної безпеки на підприємстві.

2. Які підрозділи можуть входити до складу департаменту інформаційної безпеки на підприємстві?

3. Як підбирається персонал до департаменту інформаційної безпеки на підприємстві?

ТЕМА 19
ОРГАНІЗАЦІЯ РЕАГУВАННЯ НА НАДЗВИЧАЙНІ СИТУАЦІЇ (ІНЦИДЕНТИ)

Реагування на надзвичайні ситуації (інциденти), пов'язані з порушенням інформаційної безпеки, є таким самим важливим напрямом роботи, як і побудова системи захисту та запобігання порушенням. Під інцидентом зазвичай розуміють будь-яке відхилення від нормального процесу використання інформаційних ресурсів і функціонування інформаційних систем, що спричинило збитки для певних інформаційних активів підприємства або безпосередньо створює загрозу завдання такої шкоди. У темі описуються основні розділи регламентів реагування на інциденти (надзвичайні ситуації) у сфері інформаційної безпеки. Детально розкриваються типові дії, які повинні виконуватися персоналом підприємства у разі виникнення таких ситуацій.

Ключові слова: *порушення інформаційної безпеки, збиток, виявлення порушень, аналіз, програмні засоби, група реагування, інформаційний сервіс, ділова репутація, distributed, service, DDoS, інтернет, сервер, прийняття рішень, інформаційні системи, атака, ймовірність.*

План

19.1. Вступ.

19.2. Виявлення атак і розпізнавання вторгнень.

19.3. Локалізація та усунення наслідків.

19.4. Ідентифікація нападника (або джерела розповсюдження шкідливих програм).

19.5. Оцінка і подальший аналіз процесу нападу.

19.1. Вступ

Реагування на надзвичайні ситуації (інциденти), пов'язані з порушенням інформаційної безпеки, є таким самим важливим напрямом роботи, як і побудова системи захисту та запобігання порушенням. Під інцидентом зазвичай розуміють будь-яке відхилення від нормального процесу використання інформаційних ресурсів і функціонування інформаційних систем, що спричинило збитки для певних інформаційних активів підприємства або безпосередньо створює загрозу завдання такої шкоди.

Надзвичайна ситуація (інцидент), пов'язана з порушенням інформаційної безпеки, може бути обумовлена:

– руйнівним впливом на весь майновий комплекс підприємства у разі виникнення стихійних факторів (повінь, пожежа, землетрус тощо) або цілеспрямованим нападом (підрив, підпал, руйнування будівель та приміщень тощо);

– негативним впливом виключно на інформаційні ресурси підприємства (зазвичай здійснюваним віддалено, з використанням телекомунікаційних каналів).

У загальному випадку організаційні процедури (регламенти) реагування на надзвичайні ситуації повинні включати в себе:

– регламенти альтернативних процесів обробки інформації (зокрема, можливо, і без використання засобів автоматизації) на період виходу з ладу основних інформаційних ресурсів;

– визначення груп персоналу, відповідальних за виконання тих чи інших функцій у разі виникнення надзвичайної ситуації, а також визначення процедур взаємодії між групами і окремих груп з керівництвом підприємства;

– технічну та організаційну документацію, необхідну для відновлення інформаційних систем і даних після надзвичайної ситуації;

– порядок зберігання архівних (резервних) копій даних і програмних додатків обробки даних у місцях, захищених від механічних впливів, крадіжок, повеней, пожеж;

– угоди з постачальниками програмних і апаратних засобів, що входять в інформаційну інфраструктуру підприємства, про термінову поставку компонент, що вийшли з ладу і підлягають заміні в випадку надзвичайної ситуації.

Далі в цьому розділі докладно розглядаються інциденти, причиною яких є навмисно здійснювані напади на інформаційні ресурси підприємства. Процес реагування на такі інциденти включає в себе чотири основні етапи:

– виявлення нападу;
– локалізація нападу;
– ідентифікація нападників;
– оцінка і подальший аналіз процесу нападу і його обставин.

19.2. Виявлення атак і розпізнавання вторгнень

Виявлення атак і розпізнавання вторгнень зазвичай є інженерно-технічним завданням, що вирішується за допомогою спеціальних програмних і іноді апаратних засобів. Зокрема, виявлення може здійснюватися на основі аналізу мережевого трафіку і журналів (лог-файлів), у яких фіксуються різні дії. Виявлення може здійснюватися на основі сигнатур – формалізованих наборів ознак певних вірусів, типів атак тощо. Також, очевидно, джерелом інформації про порушення є повідомлення користувачів про відхилення в роботі інформаційних систем і поява явних негативних наслідків порушень.

Для забезпечення своєчасного виявлення порушень підприємство повинно організувати постійну (за необхідності – цілодобову) роботу фахівців, що відповідають за вирішення інцидентів. Для цього може бути вибраний один з можливих підходів:

– Організація власної чергової служби, що складається з компетентних фахівців, які несуть позмінне чергування і оснащені засобами мобільного зв'язку.

– Залучення сторонньої організації, що спеціалізується на наданні подібних послуг. Водночас співробітники підприємства повинні знати номери телефонів та інші способи зв'язку, за допомогою яких вони могли б оперативно повідомляти чергових фахівців про всі події.

Виявлення порушень може бути здійснено не тільки за явними ознаками, як-от повідомлення користувачів про припинення функціонування окремих елементів інформаційних систем, одночасне використання одного облікового запису на кількох робочих станціях або явне виявлення вірусів у даних, переданих локальною мережею, але й за деякими непрямими ознаками (аномальними явищами), які в окремих випадках можуть свідчити (а можуть і не свідчити) про порушення. Прикладами таких непрямих свідчень можуть бути:

– використання інформаційних систем і певних облікових записів у нехарактерний час (рано вранці, пізно ввечері тощо);

– різке нехарактерне підвищення навантаження на інформаційні системи або їх окремі елементи (сегменти мережі, сховища даних і т. ін.);

– зміна характеру поведінки користувачів (наприклад, послідовності певних дій під час використання інформаційної системи) та інші.

Для більш ефективного аналізу таких непрямих ознак та інтерпретації різних фактів фахівцям з реагування на інциденти може знадобитися аналіз функціональності інформаційних систем і взаємодія аналітиків департаменту інформаційної безпеки з користувачами (вивчення особливостей їх роботи). Також для автоматизації такого аналізу можуть бути використані спеціальні програмні засоби, які автоматично здійснюють статистичний аналіз мережевого трафіку і інших елементів інформаційної інфраструктури та сигналізують під час виявлення аномальної активності, щоб адміністратори могли провести подальший якісний аналіз виявлених відхилень і за необхідності зробити активні дії у відповідь. Загалом розробка та вдосконалення таких засобів аналізу в складі комплексних систем виявлення вторгнень є одним з перспективних напрямів розвитку засобів захисту інформації.

Отже, основним завданням на початковому етапі реагування є визначення характеру порушень і достовірне встановлення того, що виявлені аномальні події, дії і характеристики є дійсно порушеннями, а наприклад, не проявом особливостей роботи програмного забезпечення.

Одним з найважливіших організаційних аспектів реагування на інциденти (і зокрема, на окремі сигнали про деякі події) є та обставина, що може відбуватися більш-менш часте надходження помилкових сигналів (помилкових чи спеціально спровокованих) про деякі події, і реакція персоналу департаменту

інформаційної безпеки з часом може поступово слабшати (так само, як, наприклад, може притупитися увага під час частих помилкових спрацьовувань охоронної сигналізації). Зокрема, за оцінкою деяких фахівців, у середньому в 90 % випадків, коли користувачі повідомляють про те, що, на їхню думку, комп'ютер заражений вірусом, вони помиляються. Через це під час організації реагування на інциденти необхідно приділити особливу увагу психологічній підготовці персоналу, що відповідає за реагування, а також за можливості аналізувати причини появи таких хибних сигналів і запобігати їм надалі.

Також значимим питанням організації роботи з користувачами в ситуаціях реагування на інциденти є те, що взаємодія між користувачами і групами реагування, а також різних груп реагування між собою за можливості необхідно здійснювати спеціальними захищеними каналами зв'язку.

19.3. Локалізація та усунення наслідків

Локалізація та усунення наслідків є основним етапом, у межах якого, власне, здійснюється реагування на інцидент. На цьому етапі відбувається:

– визначення конкретних параметрів порушення (нападу), його характеру (конкретних сегментів мережі, серверів, груп робочих станцій, додатків, порушених нападом);

– попередній аналіз дій порушника і сценарію події (що відбувається) нападу, алгоритму роботи вірусу, що з'явився тощо;

– блокування дій порушника (якщо порушення триває);

– блокування (повне або часткове) роботи інформаційної системи (сервера, баз даних, сегмента мережі тощо) з метою недопущення подальших руйнівних дій, поширення шкідливих програм або витоку конфіденційної інформації.

Припинення нападу і відновлення нормальної роботи інформаційних систем може зажадати скоординованих дій не тільки самих співробітників департаменту інформаційної безпеки, але й:

– спеціалістів IT-підрозділів, відповідальних за інформаційні сервіси, що атакуються;

– користувачів атакованих інформаційних систем;

– підприємств-партнерів, які пов'язані з атакованими інформаційними ресурсами;

– розробників і постачальників атакованих інформаційних систем;

– постачальників телекомунікаційних послуг, через яких здійснюється атака;

– сторонніх консультантів, що спеціалізуються на відповідних проблемах інформаційної безпеки.

Одним з найбільш важливих обставин роботи на цьому етапі є те, якими повноваженнями володіє спеціаліст (черговий), відповідальний за реагування

на інциденти. Зокрема, необхідно заздалегідь передбачити можливість оперативного самостійного відключення тих чи інших інформаційних сервісів фахівцями з реагування на інциденти (самостійно або через відповідний ІТ-підрозділ). Особливо важливою є здатність відповідальних фахівців оперативно оцінити ситуацію, провести її аналіз (у більшості практичних ситуацій це необхідно буде робити за неповними даними про сторону, що нападає) і прийняти рішення про припинення роботи тих чи інших інформаційних сервісів, до виявлення і усунення загроз і/або введення в дію додаткових засобів протидії вторгненням. Під час прийняття такого рішення необхідно враховувати (зазвичай на основі експертних оцінок) як можливий збиток, який може бути викликаний виявленим порушенням, так і можливі збитки від зупинки інформаційних сервісів, яка може бути здійснена з метою запобігання збитку від дій сторони, що нападає. Характерним прикладом такої ситуації є напад на систему електронної торгівлі, коли сторона, що нападає, може завдати серйозної шкоди (викрасти конфіденційну інформацію учасників торговельних угод, самостійно вчинити незаконні угоди від імені учасників торгової системи тощо), а зупинка сервісу з метою запобігання такої шкоди може призвести до втрат, пов'язаних з упущеною вигодою від невиконаних угод і шкодою для ділової репутації. Іншим прикладом такої ситуації є реагування на розподілені атаки типу «відмова в обслуговуванні» (Distributed Deny of Service, DDoS), часто здійснювані на сервери в мережі Інтернет, коли може бути необхідно на деякий час повністю відключити сервер як на шкоду користувачам, так і в збиток власникам інформаційних ресурсів, розташованих на сервері.

Основою для прийняття рішень може бути заздалегідь сформований перелік (довідник) можливих основних інцидентів і ознак порушень (проникнень), у якому може бути наведена оцінка ризиків сумарних втрат і рекомендовані дії для кожного типу порушень (зокрема і перелік ситуацій, коли необхідно здійснити відключення сервісів, щоб уникнути витоку або порушення цілісності інформації, яка є найбільш критичною для всієї діяльності підприємства).

19.4. Ідентифікація нападника (або джерела розповсюдження шкідливих програм)

Ідентифікація нападника (або джерела розповсюдження шкідливих програм) є важливим кроком у процесі реагування, який здійснюють безпосередньо за локалізацією нападу. Якщо напад здійснювався з локальної мережі підприємства, за належного дотримання внутрішніх режимних правил це завдання може виявитися досить легким. Якщо напад було скоєно ззовні, завдання ідентифікації нападників принципово ускладнюється і в деяких ситуаціях проблема стає практично нерозв'язною. Зазвичай для виявлення джерела нападу необхідно:

– детально вивчити всі технічні аспекти нападу;

– провести якісний аналіз процесу нападу в контексті функціонування системи захисту інформації, що атакується;

– організувати взаємодію зі сторонніми організаціями, які можуть сприяти ідентифікації нападника.

Одним з найбільш важливих завдань аналізу процесу нападу є встановлення тієї інформації, яка була відома нападникам до початку нападу і якою вони скористалися для здійснення цього нападу. Зокрема, в процесі такого аналізу з певним ступенем впевненості можна встановити, що до початку нападу зловмисникам були відомі:

– інформація про структуру і склад інформаційної системи, що атакується, (використовувані програмні і апаратні засоби, їх архітектура і використовувані налаштування);

– відомості про режим роботи організації та функціонування окремих елементів інформаційної системи. Відомості про регламент деяких бізнес-процесів підприємства;

– конкретні ідентифікаційні дані (імена користувачів, паролі), необхідні для проникнення в інформаційну систему та/або правила (алгоритми) їх генерації.

Узагальнення всіх цих відомостей може допомогти встановити, які контакти були у нападників з атакованою компанією (а яких не було), і, зіставляючи факти, а також використовуючи метод виключення, постаратися обмежити коло осіб, які потенційно могли бути причетні до організації цього інциденту.

Зі свого боку, проведення такого аналізу буде можливим тільки в тому випадку, якщо всі інформаційні системи та системи захисту інформації налаштовані в належний спосіб (зокрема, в них ведуться всі необхідні системні журнали) і системні дані не були пошкоджені в процесі нападу.

Другим важливим напрямом організаційної та аналітичної роботи під час встановлення (ідентифікації) нападників, які вчинили напад ззовні, є взаємодія з адміністраторами систем (телекомунікаційних мереж, комп'ютерів, що використовувалися в якості проксі-серверів, тощо), з використанням яких було здійснено напад. Підходи до такої взаємодії в кожному конкретному випадку, імовірніше, будуть індивідуальними і можуть залежати від політики розкриття інформації адміністрації тієї мережі або вузла, через який здійснювалася атака. Також можуть бути зроблені дії для того, щоб у судовому порядку або із залученням правоохоронних органів зобов'язати адміністрації таких мереж і вузлів надати необхідну інформацію, пов'язану з подією нападу.

Процес ідентифікації повинен за можливості проводитися з урахуванням того, що згодом необхідно буде використовувати інформацію про нападників як доказ у кримінальному процесі. Зокрема, під час зняття (копіювання) необ-

хідних лог-файлів з атакованих комп'ютерів представниками правоохоронних органів, що проводять слідство у цій справі, мають бути дотримані всі процесуальні формальності, передбачені кримінально-процесуальним законодавством. Однією з особливостей процедури вилучення доказів у потерпілої сторони в цьому випадку є те, що поняті, присутні під час вилучення, повинні за можливості мати хоча б загальне уявлення про сенс проведеної процедури. Також на цьому етапі за необхідності може бути проведена техніко-криміналістична експертиза комп'ютерних систем.

19.5. Оцінка і подальший аналіз процесу нападу

Одним із заключних кроків процесу реагування на інцидент є **оцінка та аналіз процесу нападу і його обставин.** Цей аналіз необхідно проводити в контексті цілей і завдань функціонування всього підприємства, з урахуванням результатів роботи з ідентифікації осіб, які вчинили напад. Основні завдання аналітичної роботи на цьому етапі:

– аналіз цілей і мотивів нападників;

– аналіз фундаментальних (організаційних і технічних) причин, які зробили напад можливим і успішним (якщо він був успішним);

– аналіз наслідків (зокрема і довгострокових) нападу для всієї діяльності підприємства;

– аналіз і оцінка роботи персоналу та відношень з підприємствами-партнерами (зокрема і з постачальниками інформаційних систем та засобів захисту інформації).

Результатом аналізу повинні бути висновки, які можуть послугувати основою для організаційної роботи в різних напрямах:

– коригування та уточнення політики інформаційної безпеки підприємства;

– проведення додаткової роботи з персоналом підприємства (покарання, заохочення, додаткове навчання тощо);

– проведення додаткової роботи з персоналом департаменту інформаційної безпеки підприємства, а також персоналом IT-служб;

– перегляд відносин з контрагентами підприємства (покупцями, постачальниками тощо), що мають доступ до його інформації, що захищається, або до інформаційних систем;

– залучення сторонніх консультантів з інформаційної безпеки та фахівців із засобів захисту інформації;

– ініціювання технічного переоснащення окремих ділянок інформаційної інфраструктури підприємства.

Отже, аналіз і всебічна оцінка інцидентів є відправною точкою для реалізації комплексу заходів щодо вдосконалення системи забезпечення інформа-

ційної безпеки на підприємстві. Всі ці заходи повинні в майбутньому знизити ймовірність аналогічних інцидентів, а також зменшити ймовірність нанесення істотного збитку в разі їх повторення.

Важливим складником аналізу нападу також є *оцінка збитку від події порушення інформаційної безпеки.* Збиток може бути оцінений одночасно з декількох поглядів і залежить від характеру позаштатної ситуації, що виникла. Найбільш простим для кількісної економічної оцінки є прямий збиток: витрати на відновлення втраченої інформації (можуть бути розраховані на основі трудомісткості робіт з відновлення інформації та даних про середню вартість робочого часу відповідних фахівців), витрати на заміну скомпрометованих паролів, кодів і ключів, вартість пошкодженого обладнання, штрафні санкції за розголошення конфіденційної інформації (якщо такі санкції, наприклад, були передбачені договорами з підрядниками, постачальниками або замовниками) і под. Також оцінки потребує упущена вигода, яка може бути пов'язана як з безпосереднім припиненням (зупиненням, уповільненням) поточних операцій підприємства, так і з довгостроковим (перспективним) негативним впливом виниклої позаштатної ситуації – втратою довіри до підприємства, що призводить до відтоку замовників, формуванням негативного іміджу підприємства тощо. Окремо також може бути оцінене падіння ринкової вартості підприємства – його акцій (якщо йдеться про підприємство, акції якого котируються на біржовому ринку).

Найбільш складним для оцінки є моральний збиток і наслідки від розголошення інформації особистого характеру (наприклад, відомостей, що становлять лікарську таємницю). Конкретні суми моральної шкоди зазвичай можуть бути встановлені за результатами судових розглядів з окремими особами, яким такий збиток був нанесений, або процедур досудового врегулювання конфліктів (на основі вимог постраждалих осіб).

Заключним етапом процесу реагування також є усунення негативних наслідків нападу – локалізація шкоди, заподіяної подією порушенням. Ця робота може включати в себе:

– зміну скомпрометованих паролів окремих користувачів;

– перевстановлення пошкоджених операційних систем, а також пошкодженого програмного забезпечення;

– відновлення порушеної конфігурації (налаштувань) програмного забезпечення та операційних систем;

– відновлення пошкодженої інформації (баз даних, файлів) із раніше створених резервних копій та іншими способами.

У процесі відновлення працездатності інформаційних систем на деякий час можуть бути задіяні резервні (альтернативні) апаратні і програмні платформи.

До того ж необхідним завершальним кроком може бути додаткова інформаційна робота, яка може в себе включати:

– розсилку користувачам інформації про інциденти, що відбулися (у вигляді спеціальних листів і бюлетенів);

– передачу деяких відомостей про напад у засоби масової інформації;

– передачу відомостей про напад великим групам реагування на інциденти, пов'язаних з інформаційною безпекою, а також у науково-дослідні центри, що займаються проблемами захисту інформації;

– додаткову інформаційну роботу з постачальниками інформаційних систем та підрядниками, які здійснювали їх поставку, впровадження та налагодження.

Контрольні питання:

1. Що таке атака?
2. Назвіть основні кроки процесу реагування на інцидент.
3. Виявлення атак і розпізнавання вторгнень.
4. Як відбувається ідентифікація нападника?

ТЕМА 20
АУДИТ СТАНУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ

Аудит стану інформаційної безпеки на підприємстві являє собою експертне обстеження основних аспектів інформаційної безпеки, їх перевірку на відповідність певним вимогам. У деяких випадках під аудитом інформаційної безпеки мається на увазі перевірка захищеності окремих елементів інформаційної інфраструктури підприємства і надійності засобів захисту інформації. Однак ми керуємося тим, що аудит інформаційної безпеки є комплексним дослідженням усіх аспектів інформаційної безпеки (як технічних, так і організаційних) у контексті всієї господарської діяльності підприємства з урахуванням діючої політики інформаційної безпеки, об'єктивних потреб підприємства і вимог, що пред'являються третіми особами (державою, контрагентами тощо). У темі описуються цілі аудитів інформаційної безпеки, їх класифікації за типами, передбачувані результати роботи, а також детально розкривається процес проведення аудиту всіх основних етапів.

Ключові слова: *аудит, оцінка безпеки, управління інформаційною безпекою, контроль, безпека, шкода, камера відеоспостереження, поточний контроль, інформація, фізична захищеність.*

План

20.1. Аудит, види аудиту.
20.2. Етапи проведення аудиту.

20.1. Аудит, види аудиту

Аудит стану інформаційної безпеки на підприємстві являє собою експертне обстеження основних аспектів інформаційної безпеки, їх перевірку на відповідність певним вимогам. *У деяких випадках під аудитом інформаційної безпеки мається на увазі перевірка захищеності окремих елементів інформаційної інфраструктури підприємства (сегментів його мережі, окремих серверів, баз даних, інтернет-сайтів тощо) і надійності засобів захисту інформації (міжмережевих екранів, систем виявлення вторгнень тощо).* Однак ми керуємося тим, що аудит інформаційної безпеки є комплексним (за можливості вичерпним) дослідженням усіх аспектів інформаційної безпеки (як технічних, так і організаційних) у контексті всієї господарської діяльності підприємства з урахуванням діючої політики інформаційної безпеки, об'єктивних потреб підприємства і вимог, що пред'являються третіми особами (державою, контрагентами тощо).

Розрізняють два основні види аудиту: внутрішній (проводиться виключно силами співробітників підприємства) і зовнішній (здійснюваний сторонніми організаціями). Цілями аудиту можуть бути:

– встановлення ступеня захищеності інформаційних ресурсів підприємства, виявлення недоліків і визначення напрямів подальшого розвитку системи захисту інформації;

– перевірка керівництвом підприємства та іншими зацікавленими особами досягнення поставлених цілей у сфері інформаційної безпеки, виконання вимог політики безпеки;

– контроль ефективності вкладень в придбання засобів захисту інформації та реалізацію заходів щодо забезпечення інформаційної безпеки;

– сертифікація на відповідність загальновизнаним нормам і вимогам у сфері інформаційної безпеки (зокрема, на відповідність національним і міжнародним стандартам).

Одним зі стратегічних завдань, що вирішуються під час проведення аудиту інформаційної безпеки та отримання відповідного сертифіката, є демонстрація надійності підприємства, його здатності виступати в якості стійкого партнера, здатного забезпечити комплексний захист інформаційних ресурсів, що може бути особливо важливо під час здійснення угод, що передбачають обмін конфіденційною інформацією, яка має велику вартість (фінансовими відомостями, конструкторсько-технологічною документацією, результатами НДДКР тощо).

Якщо аудит є внутрішнім, групу аудиторів необхідно сформувати з-поміж таких фахівців, які самі не є розробниками і адміністраторами використовуваних інформаційних систем і засобів захисту інформації та не мали відношення до їх впровадження на цьому підприємстві.

Зазвичай підприємство може вдаватися до допомоги зовнішніх аудиторів з метою:

– підвищення об’єктивності, незалежності та професійного рівня перевірки;

– отримання висновків про стан інформаційної безпеки та відповідності міжнародним стандартам від незалежних аудиторів.

Компанії, що спеціалізуються на проведенні аудитів, можуть здійснювати перевірки стану інформаційної безпеки на відповідність таким загальновизнаним стандартам і вимогам:

– ISO 15408: Common Criteria for Information Technology Security Evaluation [Загальні критерії оцінки безпеки інформаційних технологій];

– BSI-IT: Baseline Protection Manual [Настанова базового рівня із захисту інформаційних технологій Агентства інформаційної безпеки Німеччини];

– COBIT: Control Objectives for Information and related Technology [Основні цілі для інформаційних і пов’язаних з ними технологій];

– інших документів (як-от SAC, COSO, SAS 55/78).

Водночас організація, що здійснює зовнішній аудит, повинна відповідати певним вимогам:

– мати право (ліцензію) на видачу висновків про відповідність певним вимогам (наприклад, акредитацію UKAS – United Kingdom Accreditation Service);

– співробітники повинні мати право доступу до інформації, що становить державну і військову таємницю (якщо така інформація є на підприємстві, що перевіряється);

– володіти необхідними програмними та апаратними засобами для вичерпної перевірки наявного у підприємства програмного і апаратного забезпечення.

20.2. Етапи проведення аудиту

Основними етапами проведення аудиту є:

– ініціювання проведення аудиту;

– безпосереднє здійснення збору інформації та проведення обстеження аудиторами;

– аналіз зібраних даних і вироблення рекомендацій;

– підготовка аудиторського звіту та атестаційного висновку.

Аудит повинен бути ініційований керівництвом підприємства з досить чітко сформульованою метою на певному етапі розвитку інформаційної системи або системи забезпечення інформаційної безпеки підприємства (наприклад, після завершення одного з етапів впровадження). Якщо аудит не є комплексним, на початковому етапі необхідно визначити його безпосередні межі:

– перелік обстежуваних інформаційних ресурсів та інформаційних систем (підсистем);

– перелік будівель, приміщень і територій, у межах яких проводитиметься аудит;

– елементи системи забезпечення інформаційної безпеки, які необхідно включити в процес перевірки (організаційне, правове, програмно-технічне, апаратне забезпечення).

Основна стадія – **проведення аудиторського обстеження та збір інформації** – зазвичай має включати в себе:

– аналіз наявної політики інформаційної безпеки та іншої документації організації;

– проведення нарад, опитувань, довірчих бесід та інтерв’ю зі співробітниками підприємства;

– перевірку стану фізичної безпеки інформаційної інфраструктури підприємства;

– технічне обстеження інформаційних систем – програмних і апаратних засобів (інструментальна перевірка захищеності).

Перш ніж приступити власне до аудиту інформаційної безпеки, аудиторам (зокрема якщо проводиться зовнішній аудит) необхідно ознайомитися зі струк-

турою підприємства, його функціями, завданнями та основними бізнес-процесами, а також із наявними інформаційними системами (їх складом, функціональністю, процедурами використання і роллю на підприємстві). На початковому етапі аудитори приймають рішення про те, наскільки глибоко і детально будуть досліджені окремі елементи інформаційної системи та системи захисту інформації. Також необхідно заздалегідь скоординувати з користувачами інформаційних систем процедури перевірки та тестування, що вимагають обмеження доступу користувачів (такі процедури за можливості повинні проводитися в неробочий час або в періоди найменшого завантаження інформаційної системи).

Якісний **аналіз діючої на підприємстві політики безпеки** є відправною точкою для проведення аудиту. Одне з перших завдань комплексного аудиту – встановлення того, якою мірою діюча політика відповідає об'єктивним потребам цього підприємства в безпеці, чи можуть дії в межах цієї політики забезпечити необхідний рівень захищеності інформації і засобів її обробки, зберігання та передачі. Це може вимагати проведення додаткової оцінки значимості основних інформаційних активів підприємства, їх вразливості, а також наявних ризиків і загроз. Аналіз політики також може включати оцінку таких її характеристик:

– повнота і глибина охоплення всіх питань, а також відповідність змісту політик нижнього рівня цілям і завданням, встановленим у політиках верхнього рівня;

– зрозумілість тексту політики для людей, які не є технічними фахівцями, а також чіткість формулювань і неможливість їх подвійного тлумачення;

– актуальність усіх положень і вимог політики, своєчасність обліку всіх змін, що відбуваються в інформаційних системах і бізнес-процесах.

Після перевірки основних положень політики безпеки в процесі аудиту можуть бути вивчені (перевірені) наявні класифікації інформаційних ресурсів за ступенем критичності і конфіденційності, а також інші документи щодо забезпечення інформаційної безпеки:

– організаційні документи підрозділів підприємства (положення про відділи, посадові інструкції);

– інструкції (положення, методики), що стосуються окремих бізнес-процесів підприємства;

– кадрова документація, зобов'язання про нерозголошення відомостей, дані співробітників, свідоцтва про проходження навчання, професійної сертифікації, атестації та ознайомлення з чинними правилами;

– технічна документація та користувацькі інструкції для різних використовуваних програмних і апаратних засобів (розроблених самим підприємством та придбаних у сторонніх постачальників): міжмережевих екранів, маршрутиза-

торів, операційних систем, антивірусних засобів, систем управління підприємством тощо.

Основна робота аудиторів у процесі збору інформації полягає у вивченні фактично застосованих заходів щодо забезпечення захисту інформаційних активів підприємства, як-от:

– організація процесу навчання користувачів прийомам і правилам безпечного використання інформаційних систем;

– організація роботи адміністраторів інформаційних і телекомунікаційних систем і систем захисту інформації (правильність використання програмних і апаратних засобів адміністрування, своєчасність створення і видалення облікових записів користувачів, а також налаштування їх прав в інформаційних системах, своєчасність заміни паролів і забезпечення їх відповідності вимогам безпеки, здійснення резервного копіювання даних, ведення протоколів усіх вироблених у процесі адміністрування операцій, вжиття заходів у разі виявлення несправностей тощо);

– організація процесів підвищення кваліфікації адміністраторів інформаційних систем і систем захисту інформації;

– забезпечення відповідності необхідних (відповідно з політикою безпеки та посадовими обов'язками) прав користувачів інформаційних систем і фактично наявних;

– організація призначення і використання спеціальних («суперкористувацьких») прав в інформаційних системах підприємства;

– організація робіт і координації дій у разі виявлення порушень інформаційної безпеки та відновлення роботи інформаційних систем після збоїв і нападів (практичне виконання «аварійного плану»);

– вжиття заходів антивірусного захисту (належне використання антивірусних програм, облік усіх випадків зараження, організація роботи з усунення наслідків заражень тощо);

– забезпечення безпеки придбаних програмних і апаратних засобів (наявність сертифікатів і гарантійних зобов'язань, підтримка з боку постачальника в усуненні виявлених недоліків тощо);

– забезпечення безпеки самостійно розроблюваного програмного забезпечення (наявність необхідних вимог у проєктній документації інформаційних систем, якість програмної реалізації механізмів захисту тощо);

– організація робіт зі встановлення та оновлення програмного забезпечення, а також контролю за цілісністю встановленого ПЗ;

– вживаються заходи щодо забезпечення обліку і збереження носіїв інформації (дисків, дискет, магнітних стрічок тощо), а також їх безпечного знищення після закінчення використання;

– ефективність організації взаємодії співробітників підприємства – користувачів інформаційних систем – зі службою інформаційної безпеки (зокрема з питань реагування на інциденти та усунення їх наслідків).

Одним з важливих напрямів аудиторської перевірки є контроль того, наскільки своєчасно і повно положення та вимоги політики безпеки й інших організаційних документів доводяться до персоналу підприємства. Зокрема, необхідно оцінити, наскільки систематично і цілеспрямовано здійснюється навчання персоналу (під час зайняття посад і в процесі роботи), і відповідно дати оцінку тому, якою мірою персонал розуміє всі пропоновані до нього вимоги, усвідомлює свої обов'язки, пов'язані із забезпеченням безпеки, а також можливу відповідальність, яка може настати у разі порушення встановлених вимог.

У процес проведення інтерв'ю, нарад і бесід із персоналом необхідно включити якомога більше співробітників підприємства, які мають хоча б якесь відношення до інформаційних систем і процедур обробки інформації: адміністраторів і розробників інформаційних систем, операторів та інших користувачів, допоміжний персонал тощо. Під час безпосередньої роботи з персоналом аудиторам необхідно з'ясувати особливості перебігу окремих бізнес-процесів, ролі окремих співробітників у цих процесах і їх потенційні можливості впливати на інформаційну безпеку. Також необхідно оцінити, якою мірою співробітники фактично виконують свої обов'язки щодо забезпечення інформаційної безпеки.

Одним із важливих завдань аудиту може бути встановлення того, наскільки підприємство здатне протидіяти внутрішнім загрозам в особі співробітників, які цілеспрямовано діють, щоб завдати збитку підприємству, і мають для цього різні можливості. Зокрема, для цього можуть бути досліджені:

– процедури відбору та прийняття нових співробітників на роботу, а також їх попередньої перевірки;

– процедури контролю за діяльністю співробітників (відстеження їх дій);

– процедури реєстрації користувачів і призначення їм прав в інформаційних системах;

– розподіл функцій між різними співробітниками і мінімізація їх привілеїв, а також можливої наявності надлишкових прав у деяких користувачів та адміністраторів.

Перевірка стану фізичної безпеки інформаційної інфраструктури зазвичай включає в себе:

– перевірку того, щоб найбільш важливі об'єкти інформаційної інфраструктури та системи захисту інформації розташовувалися в зонах (частинах будинків, приміщеннях), що мають пропускний режим, а також обладнаних камерами відеоспостереження та іншими засобами контролю (електронними замками, засобами біометричної ідентифікації тощо);

– перевірку наявності та працездатності технічних засобів, що забезпечують стійку роботу комп'ютерного та телекомунікаційного обладнання: джерел безперебійного енергопостачання, кондиціонерів (там, де це необхідно) тощо;

– перевірку наявності та працездатності засобів пожежної сигналізації та пожежогасіння;

– перевірку розподілу відповідальності за фізичний (технічний) стан об'єктів інформаційної інфраструктури підприємства.

Інструментальна перевірка захищеності є в основному технічним завданням і здійснюється з використанням спеціалізованого програмного забезпечення, яке підключається до інформаційної системи підприємства і автоматично проводить збір всіляких відомостей: версій встановлених операційних систем і програмного забезпечення, даних про мережеві протоколи, що використовуються, номерів відкритих портів, даних про версії встановлених оновлень тощо. До інших напрямів інструментального та технічного контролю також належать такі роботи:

– безпосереднє вивчення роботи окремих серверів, робочих станцій і мережевого устаткування відповідними технічними фахівцями, які можуть перевірити різні аспекти їх функціонування (процедури завантаження, виконувані процеси, вміст конфігураційних файлів тощо);

– збір і подальший аналіз даних про те, як виконуються процедури резервного копіювання, а також інші необхідні технічні процедури, передбачені регламентом;

– перевірка якості програмного забезпечення, самостійно розробленого підприємством (зокрема шляхом аналізу вихідних кодів і проєктної документації до нього), виявлення помилок, які можуть стати причиною збоїв, несанкціонованих проникнень, руйнування і витоку інформації та інших інцидентів;

– вивчення роботи мережі (мережевого трафіка, завантаження різних сегментів мережі тощо);

– проведення з метою тестування пробних, контрольованих «порушень» інформаційної безпеки (за можливості без нанесення реальної шкоди і у позаробочий час), як-от атаки типу «відмова в обслуговуванні» (DoS) або проникнення в певні бази даних і на певні сервери, а також використання різних відомих вразливостей з метою з'ясування конкретних параметрів безпеки, стабільності та надійності інформаційної системи, яка перевіряється.

Також у процесі аудиту може бути перевірено ведення журналів (лог-файлів) інформаційних систем і застосування інших інструментів збору та аналізу інформації, необхідних для забезпечення поточного контролю за дотриманням вимог інформаційної безпеки та своєчасного реагування на інциденти (засобів виявлення вторгнень, аналізаторів роботи локальних мереж тощо). Інформація,

накопичена в лог-файлах за час використання інформаційних систем, є одним із важливих об'єктів аналізу в процесі аудиту. На основі цих даних можуть бути зроблені оцінки та висновки щодо дотримання встановлених правил використання інформаційних систем, ефективності використовуваних засобів захисту інформації, поведінки користувачів, а також про потенційно можливі проблеми.

Аналіз усієї інформації, отриманої в процесі ознайомлення з документацією, контролю фактичного виконання всіх встановлених вимог, отримання відомостей від співробітників, вивчення роботи апаратних засобів і програмного забезпечення, перевірки фізичної захищеності та проведення інструментальних перевірок повинен бути проведений з урахуванням виявлених ризиків та потреб підприємства в інформаційній безпеці. Зокрема, такий аналіз передбачає виявлення конкретних особливостей програмних і апаратних засобів, бізнес-процедур, організаційних правил і розподілів функціональних обов'язків та повноважень, які можуть негативно вплинути на забезпечення інформаційної безпеки, а також опис причинно-наслідкових взаємозв'язків між виявленими особливостями функціонування підприємства і збільшенням ризиків порушення інформаційної безпеки. Всі досліджені обставини, виявлені недоліки та особливості повинні бути узагальнені, і має бути сформоване загальне уявлення про стан інформаційної безпеки на підприємстві, відображені основні переваги і недоліки діючої системи захисту інформаційних ресурсів, а також позначені основні пріоритети та напрями її подальшого розвитку та вдосконалення.

Результати аналізу можуть бути подані як у вигляді узагальнених коротких формулювань, що характеризують захищеність інформації підприємства (адресованих керівництву та власникам підприємства), так і у вигляді переліку конкретних зауважень і пропозицій, що належать до окремих ділянок роботи (адресованих керівнику департаменту інформаційної безпеки, керівнику служби безпеки, функціональним директорам та керівникам структурних підрозділів підприємства). Заключним результатом аналізу та узагальнення даних, отриманих у процесі аудиту, є звіт (висновок), який може включати в себе:

– оцінку стану (рівня) захищеності інформаційних ресурсів та інформаційних систем;

– висновки про практичне виконання вимог, передбачених політикою інформаційної безпеки підприємства та іншими вимогами та документами;

– висновки про ступінь відповідності фактичного рівня інформаційної безпеки вимогам певних стандартів і нормативних документів;

– пропозиції щодо удосконалення політики інформаційної безпеки та реалізації додаткових практичних заходів у цій сфері (як організаційних, так і технічних), а також про ті заходи, які необхідно реалізувати для проходження сертифікації на відповідність певному стандарту (якщо за результатами про-

веденого аудиту зроблено висновок про те, що поточний рівень захищеності інформаційних ресурсів підприємства не відповідає таким вимогам);

– висновок про ступінь відповідності політики безпеки підприємства та всього комплексу заходів щодо захисту інформації вимогам чинного законодавства та відомчих нормативних актів;

– оцінки економічної ефективності вкладень у ті чи інші засоби захисту інформації, а також організаційні заходи (віддачі від них);

– кількісна (грошова) оцінка можливих втрат від тих чи інших порушень, які можуть статися за наявного рівня забезпечення інформаційної безпеки, а також розрахунок необхідних вкладень, які необхідно здійснити для досягнення певного рівня захищеності.

Також за результатами аудиту можуть бути сформульовані додаткові рекомендації, що стосуються:

– перегляду окремих бізнес-процесів і процедур;

– вдосконалення роботи з персоналом підприємства;

– впровадження і використання сучасних технічних (програмних і апаратних) засобів обробки і захисту інформації;

– організації роботи із захисту інформації;

– вибору пріоритетів в процесі усунення наявних недоліків.

Контрольні питання:

1. Що таке аудит?

2. Назвіть основні етапи проведення аудиту.

3. Які основні роботи проводяться на етапі збору інформації та проведення обстеження аудиторами.

ТЕМА 21
НАДАННЯ ПОСЛУГ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У темі розглядаються організаційні питання надання різних послуг, пов'язаних із забезпеченням інформаційної безпеки: аудиторських, консультаційних, послуг зі впровадження технічних засобів захисту, а також послуг зі страхування інформаційних ризиків.

Ключові слова: *аутсорсинг, криптографічні засоби, загроза інформаційній безпеці, порушення інформаційної безпеки, Public Key Infrastructure, PKI, сервіс безпеки, діяльність, атака, збиток, аналіз, цифровий сертифікат, інформаційні технології, ділова репутація, електронний документообіг.*

План

21.1. Передумови розвитку ринку послуг із забезпечення інформаційної безпеки і його структура.

21.2. Особливості деяких видів послуг.

21.3. Інфраструктура публічних ключів.

21.1. Передумови розвитку ринку послуг із забезпечення інформаційної безпеки і його структура

Розвиток сучасних інформаційних технологій, зростання залежності діяльності багатьох підприємств і установ від функціонування інформаційних систем і постійне наростання обсягів і складності інформаційних потоків призвели до того, що завдання забезпечення інформаційної безпеки стали вимагати використання значних ресурсів. Зокрема, фінансові кошти, що виділяються на забезпечення інформаційної безпеки, займають усе більшу частку в бюджетах підприємств, а поточне і стратегічне управління захистом інформації вимагає більшої уваги не тільки з боку фахівців з інформаційних технологій, але і з боку керівників та власників підприємств. Найчастіше необхідні ресурси і зусилля керівників у цій сфері виявляються порівнянними з тими ресурсами, які витрачаються на здійснення основної діяльності підприємств. Отже, склалися передумови для формування ринку різних послуг із забезпечення інформаційної безпеки, які (послуги) допомогли б не тільки підвищити ефективність захисту інформаційних ресурсів, а й оптимізувати витрати підприємств і організацій. Основними факторами, які зумовили появу у підприємств потреб у послугах сторонніх фірм, які вирішують завдання забезпечення інформаційної безпеки, і виділення послуг із захисту інформаційних ресурсів у самостійну сферу бізнесу, стали:

– ускладнення і постійний розвиток сучасних систем обробки, зберігання та передачі інформації;

– ускладнення програмних і апаратних засобів, що використовуються для захисту інформації, необхідність розуміння складного комплексу теоретичних і методичних питань для їх ефективної експлуатації;

– зростання кількості інцидентів і різноманітності видів атак на інформаційні системи та їх інтенсивності;

– нестача кваліфікованих фахівців у сфері інформаційної безпеки і зростання витрат на їх утримання та професійну підготовку.

Причиною того, що підприємства виявляються зацікавленими у відмові від самостійного виконання певних функцій і залучення сторонніх спеціалізованих компаній для вирішення цих завдань (у сучасній практиці такий підхід прийнято називати «аутсорсингом» або «передачею на аутсорсинг»), є можливість підвищити ефективність процесів захисту інформації, певною мірою скоротити витрати на ці процеси, а також сконцентруватися на управлінні основною діяльністю підприємства і не відволікати ресурси та час керівників на вирішення завдань, що є за своєю суттю вторинними і допоміжними відносно основних цілей і завдань діяльності підприємства. Більш висока ефективність роботи спеціалізованих компаній – постачальників послуг у сфері інформаційної безпеки, порівняно з самостійним вирішенням цих завдань самими підприємствами, зазвичай пов’язана з тим, що високі витрати розподіляються між безліччю підприємств – клієнтів постачальника послуг. Характерними прикладами таких витрат, які, з одного боку, можуть бути неприпустимими для одного підприємства, але з іншого боку, можуть бути ефективно розподілені між кількома підприємствами, є:

– використання висококваліфікованих фахівців у відносно вузьких дисциплінах і галузях інформаційної безпеки (як-от використання криптографічних засобів, боротьба з вірусами, впровадження віртуальних приватних мереж і т. ін.);

– часте перенавчання та підвищення кваліфікації фахівців;

– постійне відстежування нових загроз і глибокий якісний аналіз поточного стану інформаційних технологій і тенденцій їх розвитку;

– придбання спеціалізованих програмних і апаратних засобів, необхідних для захисту інформації та аудиту інформаційних систем;

– забезпечення цілодобового чергування служб реагування на інциденти.

Незважаючи на всі переваги передачі окремих завдань забезпечення безпеки на аутсорсинг, цей підхід має і низку недоліків, які певною мірою можуть обмежувати його застосування:

– Підприємство, яке користується такими послугами, дещо обмежує себе в можливостях керувати своїми витратами і скорочувати витрати (накладні витрати), отже, потрапляє в певну залежність від цінової політики постачальників послуг, а також від кон’юнктури ринку.

– Співробітники компанії, що надає послуги, отримують доступ до найбільш важливої інформації підприємства-клієнта і його інформаційних систем, що потенційно може бути джерелом додаткових ризиків для інформаційної безпеки.

– Виникають додаткові загрози інформаційній безпеці під час взаємодії між компанією-постачальником і підприємством-клієнтом у процесі надання послуг (наприклад, може бути перехоплена інформація під час віддаленого адміністрування інформаційних систем підприємства-клієнта).

Основними послугами, які можуть бути передані на аутсорсинг (як окремо, так і в комплексі), є:

– послуги з проведення комплексних аудитів стану інформаційної безпеки на підприємстві;

– послуги з проведення аудитів (інструментальних перевірок) стійкості і надійності окремих інформаційних підсистем (мереж, програмних і апаратних платформ і т. ін.) і засобів захисту інформації, що використовуються підприємством;

– послуги з сертифікації інформаційних систем, вироблених програмних і апаратних засобів захисту інформації;

– консультаційні послуги, пов'язані з формуванням стратегії підприємства у сфері інформаційної безпеки і розробкою політики безпеки;

– послуги з проєктування системи захисту інформації;

– консультаційні послуги з вибору та адаптації окремих технологій захисту інформації (криптографії, біометричної ідентифікації і т. ін.) відповідно до певних умов ведення бізнесу;

– послуги зі впровадження системи захисту інформації, а також впровадження окремих технічних (програмних і апаратних) засобів та реалізації організаційних заходів;

– послуги з поточного адміністрування, підтримки та супроводу інформаційних систем і систем захисту інформації;

– послуги з реагування на інциденти, пов'язані з порушеннями інформаційної безпеки;

– послуги з навчання керівників підприємства, фахівців служби інформаційної безпеки та IT-служби, а також користувачів інформаційної системи підприємства.

Загалом на цей момент складно говорити про формування повноцінного ринку послуг у сфері інформаційної безпеки, оскільки у більшості менеджерів великих, а особливо середніх і малих підприємств, в основному не сформувалися уявлення про необхідні заходи в цій сфері, а фінансування робіт із забезпечення інформаційної безпеки часто здійснюється за залишковим принципом. Деякі великі розробники комплексних рішень у сфері інформаційної безпеки, хоча і функціонують досить активно, але фактично не є учасниками відкритого

ринку, оскільки їх продукція і послуги практично повністю орієнтовані на певних споживачів у державному секторі. Ще однією важливою особливістю ринку послуг у сфері інформаційної безпеки є те, що надання таких послуг іноді стає «побічним», додатковим видом (напрямом) діяльності для компаній, що займаються постачанням апаратних і програмних засобів захисту інформації, а також для компаній, що займаються розробкою комплексних рішень з автоматизації підприємств.

Можливим недоліком такого підходу потенційно може бути те, що консультанти й аналітики виявляються жорстко «прив'язані» до певних програмних і апаратних засобів (виробників, торгових марок) і не мають можливості гнучко підбирати окремі засоби захисту і формувати найбільш ефективні комплексні рішення відповідно до потреб кожного конкретного підприємства.

Але незважаючи на певні недоліки в розвитку ринку послуг із забезпечення інформаційної безпеки, незаперечним фактом є те, що багато таких послуг уже представлені на ринку, а основні ринкові і організаційні механізми починають відпрацьовуватися на практиці. Водночас однією з рекомендацій під час роботи з фірмами-постачальниками послуг у сфері інформаційної безпеки є правило – користуватися послугами кількох різних фірм і періодично міняти партнерів, які забезпечують вирішення тих чи інших проблем безпеки.

21.2. Особливості деяких видів послуг

Кожен вид послуг у цій сфері має свої специфічні характеристики як із погляду організації роботи компаній, що надають послуги, так і погляду структури ринку. Відповідно для ефективної роботи необхідний індивідуальний підхід до організації надання таких послуг, а також організації взаємодії між споживачами і постачальниками послуг.

Послуги з реагування на інциденти (порушення інформаційної безпеки) є одним із найбільш характерних прикладів обґрунтованості та доцільності передачі сервісів безпеки на аутсорсинг. Зокрема, доцільність відмови від самостійного виконання функцій реагування на інциденти та їх централізації в компанії, яка спеціалізується на таких завданнях, пов'язана з такими важливими особливостями, притаманними цьому процесу:

– вимагає постійного (цілодобового) чергування, що передбачає утримання в штаті як мінімум п'яти фахівців;

– передбачає наявність висококваліфікованих (а отже, високооплачуваних і затребуваних на ринку праці) фахівців, здатних швидко вжити ефективних заходів протидії загрозам (зокрема і вжити контрзаходів до нападників у процесі атаки, яка триває), а також самостійно прийняти необхідні рішення в процесі відображення атаки, яка триває;

– завантаження чергових фахівців, що відповідають за реагування на інциденти, може бути вкрай нерівномірним.

Отже, ефект від централізації функцій, пов'язаних з реагуванням на інциденти, складається з декількох елементів і дає можливості як для скорочення витрат і підвищення рівня захищеності підприємств-клієнтів, так і для отримання прибутку фірмами-постачальниками таких послуг. Водночас розмежування функцій між підприємством-клієнтом і компанією-постачальником послуг може залежати від таких факторів:

– рівень довіри підприємства-клієнта до фірми-постачальника послуг;

– усталена практика надання таких послуг і наявність у фірми-постачальника необхідних фахівців з певним рівнем кваліфікації;

– склад, характеристики та функціональність інформаційних систем підприємства-клієнта;

– рівень кваліфікації співробітників підприємства-клієнта (як користувачів інформаційних систем, так і співробітників департаменту інформаційної безпеки);

– оцінка наявних ризиків (ймовірності нанесення збитку);

– оцінка (зокрема і суб'єктивна) того, наскільки значимим є знання внутрішнього середовища підприємства співробітниками служби інформаційної безпеки та їх здатність «зсередини» координувати дії і вирішувати проблеми в разі будь-яких інцидентів.

До того ж у деяких випадках можуть існувати певні законодавчі обмеження на аутсорсинг процесів безпеки (зокрема, для державних підприємств).

Основні питання проведення аудитів інформаційної безпеки (зокрема зовнішніх аудитів)

Крім уже зазначених факторів, які зумовлюють необхідність проведення саме зовнішніх аудитів, а не внутрішніх (більш висока кваліфікація фахівців, право робити висновки про відповідність міжнародним стандартам і т. ін.), важливою є те, що зовнішні аудитори зазвичай не зацікавлені в поданні необ'єктивної інформації (на відміну від внутрішньої служби інформаційної безпеки). Якщо підприємство захоче створити власну незалежну службу для проведення аудитів інформаційної безпеки (окремо від департаменту інформаційної безпеки та інших підрозділів підприємства), результатом можуть виявитися дуже великі витрати, тим паче, що частота проведення таких аудитів зазвичай не дуже велика.

Необхідність вдаватися до послуг спеціалізованих фірм, пов'язаних із перевіркою захищеності і надійності окремих елементів інформаційної інфраструктури (серверів, мереж, міжмережевих екранів і т. ін.), обумовлена зазвичай наявністю у цих фірм спеціалізованих програмних і апаратних засобів, необ-

хідних для проведення таких перевірок (наприклад, спеціалізованих сканерів вразливостей), а також наявність спеціальних знань, навичок і різнобічного досвіду, накопиченого в процесі практичної роботи під час проведення подібних перевірок на різних підприємствах. Отримання подібного досвіду в межах одного підприємства, нехай навіть і дуже великого, практично неможливе. Одним з найбільш ефективних прийомів під час проведення таких перевірок є пробне (тестове) подолання захисту, коли перевіряючий імітує певний напад з метою здійснити порушення (зруйнувати базу даних, викрасти конфіденційну інформацію і т. ін.). Основними завданнями таких перевірок є:

– оцінка ефективності використовуваних технічних (програмних і апаратних) засобів захисту інформації;

– оцінка ефективності роботи фахівців, відповідальних за реагування на інциденти;

– контроль дотримання співробітниками підприємства вимог політики безпеки.

Для отримання найбільш достовірних результатів бажано, щоб на самому підприємстві про проведення такого тесту знали тільки кілька керівників, відповідальних за його організацію. Також важливою умовою проведення такої перевірки є чітка домовленість про те, наскільки далеко має зайти атака і який рівень проникнення і руйнівних дій є достатнім для того, щоб достовірно продемонструвати, що атакована (яка перевіряється) система є вразливою. У будь-якому випадку вся відповідальність за шкоду, завдану внаслідок здійснення такої перевірки, повністю лягає на підприємство, яке замовило таку послугу.

Консультаційні послуги, пов’язані з первинною постановкою системи управління інформаційною безпекою (первинним аналізом, формуванням та використанням політики безпеки), зазвичай бувають необхідні в ситуації, коли підприємство вперше ставить для себе завдання цілеспрямованого систематичного комплексного забезпечення інформаційної безпеки. У цих умовах залучення сторонніх консультантів є практично єдиним способом сформувати адекватну й ефективну політику безпеки в доволі стислі терміни, оскільки саме підприємство в такій ситуації зазвичай не має необхідних фахівців і керівників, які могли б вирішити весь комплекс завдань, пов’язаних з оцінкою ризиків, інвентаризацією інформаційних активів, виробленням стратегії, формуванням політики та організаційної структури департаменту інформаційної безпеки.

Залучена для вирішення всіх цих завдань консультаційна компанія повинна буде провести аналіз діяльності підприємства в декількох розрізах: з погляду основних бізнес-процесів, з погляду наявної інформаційно-технологічної та комунікаційної інфраструктури, а також з погляду використовуваних додатків (програмного забезпечення та баз даних). Отже, необхідна якість роботи щодо

забезпечення комплексної захищеності інформаційних ресурсів підприємства може бути досягнута тільки в тому випадку, якщо у консалтинговій компанії є необхідні фахівці, а також досвід роботи як на подібних підприємствах, так і з подібними програмними і апаратними платформами. Високі вимоги до кваліфікації фахівців, що працюють у консалтингових компаніях, пояснюються необхідністю не просто зрозуміти особливості функціонування тих чи інших бізнес-процесів та інформаційних систем, але і швидко оцінити їх слабкі місця, наявні ризики і найбільш ймовірні сценарії нанесення збитку інформаційним ресурсам.

Послуги з адміністрування інформаційних систем і засобів захисту інформації можуть надаватися як у комплексі з послугами з реагування на інциденти, так і незалежно від них. Фірми-постачальники послуг можуть здійснювати адміністрування таких систем:

– електронна пошта (захист від вірусів, спаму, порушення конфіденційності та інші порушення політики безпеки);

– мережеве обладнання (збір і аналіз інформації про функціонування маршрутизаторів, серверів та інших пристроїв);

– брандмауери (конфігурація та виконання установки до мережі, а також забезпечення своєчасного реагування на різні порушення);

– системи виявлення вторгнень (відстеження всіх «підозрілих» дій щодо мереж, серверів, додатків і баз даних).

Водночас підприємство-покупець може вдаватися до послуг інших фірм для контролю за тим, наскільки ефективно здійснюється адміністрування засобів захисту інформації, або самостійно здійснювати такий контроль за допомогою спеціальних сканерів.

У разі надання послуг з адміністрування фірма-постачальник зазвичай не може взяти на себе повну відповідальність за збереження інформації (так само, як і в разі надання послуг із реагування на інциденти), проте для встановлення формальних відносин підприємство-клієнт і фірма-постачальник можуть розробити Угоду про рівень обслуговування, яка повинна передбачати основні параметри функціонування інформаційних систем і їх захищеності (гарантований час надійної роботи систем, гарантовані строки відновлення працездатності в разі порушень і т. ін.).

21.3. Інфраструктура публічних ключів

Інфраструктура публічних ключів (Public Key Infrastructure, PKI) являє собою складну організаційно-технічну систему, засновану на сучасних технологіях і розвинених організаційних стандартах, яка дає змогу ефективно вирішувати деякі ключові проблеми інформаційної безпеки, і зокрема проблеми захисту

даних, що передаються по мережі (як локальній, так і глобальній), та ідентифікації сторін, що беруть участь в інформаційному обміні (користувачів, інформаційних систем, програмних процесів). Технологія PKI є основним інструментом, за допомогою якого на основі законодавчої бази може бути створений юридично значимий документообіг, який може стати основою для активного розвитку електронної торгівлі, надання фінансових, інформаційних та інших послуг, а також здійснення електронних платежів через інформаційні мережі загального користування. Можливість використання цієї технології для здійснення платежів і господарських операцій пов'язана з тим, що її найважливішим елементом є так званий цифровий сертифікат, що видається третьою стороною, яка фактично є гарантом того, що операції, що здійснюються з використанням певного цифрового сертифікату, відбуваються від імені певної особи. Отже, одним із ключових елементів інфраструктури публічних ключів є організаційні структури, які здійснюють ідентифікацію осіб (якщо йдеться про видачу сертифіката для однієї людини) і видачу електронного сертифіката встановленого зразка, що однозначно і достовірно представляє цю людину. Також ці центри вирішують безліч додаткових завдань, пов'язаних із забезпеченням ефективної роботи інфраструктури публічних ключів: ведуть списки анульованих сертифікатів, оновлюють минулі сертифікати і т. ін. Загалом уся сукупність використовуваних технічних і організаційних рішень, а також діюча юридична база дають можливість однозначно пов'язувати цифровий сертифікат (цифровий підпис) з певною фізичною особою і також гарантувати, що не відбувається порушення цілісності переданих повідомлень.

Сьогодні досить добре розроблені базові технічні стандарти та інформаційні технології (засоби криптографії, алгоритми, що реалізують хеш-функції і т. ін.), необхідні для побудови засобів захисту на основі PKI. Подальші перспективи розвитку в цій сфері пов'язані в основному зі вдосконаленням ринку послуг і організаційних механізмів.

Ідеологія роботи PKI передбачає створення мереж і взаємопов'язаних структур безлічі різних засвідчувальних центрів, що працюють у межах єдиної узгодженої політики і спираються на загальний «кореневий» засвідчувальний центр. На практиці ж найбільш поширене створення самостійних розрізнених засвідчуваних центрів, створюваних окремими підприємствами (наприклад, комерційними банками) на основі тиражованих програмних і апаратних рішень для забезпечення захищеності і надання юридичної значимості створюваних документів і транзакцій, що здійснюються в корпоративних інформаційних системах (наприклад, платіжні доручення) службовцями, клієнтами та бізнес-партнерами підприємства. Якщо підприємство самостійно розгортає PKI в межах власної інформаційної системи, всі відношення між адміністрацією і користувачами регулюються внутрішньою політикою.

Водночас одним із можливих підходів до впровадження технології PKI є передача функцій, пов'язаних із видачою і подальшим зверненням цифрових сертифікатів, на аутсорсинг. Передача функцій засвідчувального центру сторонній спеціалізованій компанії зазвичай вирішує для підприємства два важливі завдання:

– дає змогу уникнути значних витрат, пов'язаних із закупівлею та підтриманням програмних і апаратних засобів, а також найманням і навчанням персоналу;

– дає можливість застосовувати цифрові сертифікати за межами свого підприємства, а також використовувати на підприємстві сертифікати співробітників інших підприємств.

Компанія, що виконує функції засвідчувального центру, може передати частину робіт, які пов'язані з перевіркою документів осіб, які претендують на отримання сертифіката, і їх консультуванням, своїм партнерам – так званим «реєстраційним центрам». Їх основна функція полягає у спрощенні і прискоренні процедури перевірки документів та ідентифікації особистості під час видачі сертифіката для осіб, які не можуть особисто з'явитися в засвідчувальний центр.

Саме на основі мереж реєстраційних центрів, а також взаємодії різних засвідчувальних центрів (їх об'єднання в єдину мережу) має відбуватися побудова універсальної загальнодоступної інфраструктури публічних ключів. Передбачається, що основними користувачами – клієнтами засвідчувальних центрів, що бажають отримати цифрові сертифікати, – повинні бути особи, зацікавлені в доступі до різних спеціалізованих електронних сервісів, що полегшує взаємодію як з різними комерційними структурами (наприклад, банками), так і з державними органами.

Контрольні питання:

1. Що таке аутсорсинг?
2. Що таке інфраструктура публічних ключів?
3. Як розвивається ринок послуг із забезпечення інформаційної безпеки?

ТЕМА 22
НАДАННЯ ПОСЛУГ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ (СТРАХУВАННЯ)

Світова практика страхування інформаційних ризиків почала складатися в дев'яностих роках і отримала свій розвиток після 2000-го р., коли ризики інформаційної безпеки стали більш серйозними. У темі розглядаються організаційні питання надання різних послуг, пов'язаних із забезпеченням інформаційної безпеки: аудиторських, консультаційних, послуг з впровадження технічних засобів захисту, а також послуг зі страхування інформаційних ризиків.

Ключові слова: *аутсорсинг, криптографічні засоби, загроза інформаційній безпеці, порушення інформаційної безпеки, Public Key Infrastructure, PKI, сервіс безпеки, діяльність, атака, збиток, аналіз, досвід, цифровий сертифікат, технології, електронний документообіг.*

План

22.1. Страхування інформаційних ризиків. Основи методології страхування інформаційних ресурсів.

22.2. Ринок страхових послуг.

22.1. Страхування інформаційних ризиків. Основи методології страхування інформаційних ресурсів

Хоча страхування ризиків, пов'язаних з інформаційною безпекою, само по собі не є організаційним засобом захисту інформації (бо факт наявності або відсутності такої страховки не впливає на ймовірність нанесення шкоди інформаційних ресурсів), все ж воно є важливим і перспективним інструментом управління інформаційними ризиками на підприємстві.

З погляду ризик-менеджменту, страхування є головним інструментом так званої «передачі ризиків». Основним чинником, що обумовлює зацікавленість підприємств у страхуванні своїх інформаційних ресурсів, є те, що в разі будь-яких серйозних порушень у роботі інформаційних систем підприємство отримує можливість за рахунок страхових виплат відносно швидко відновити їх роботу, а також основні бізнес-процеси і компенсувати (хоча б частково) збиток від вимушеного простою і втрати інформаційних активів.

Згідно із законодавством об'єктом страхування можуть бути майнові інтереси, які не суперечать законодавству, пов'язані з володінням, користуванням, розпорядженням майном, а також пов'язані з відшкодуванням страхувальником заподіяної ним шкоди особі або майну фізичної особи, а також шкоди, заподіяної юридичній особі (страхування відповідальності). Отже, на практиці об'єктами страхування можуть бути:

– інформаційні ресурси (в будь-якому їх вигляді: бази даних, бібліотеки електронних документів тощо);

– програмне забезпечення (як уже використовувані програмні власні та покупні продукти, так і ті, що знаходяться в розробці);

– апаратне забезпечення інформаційних систем (мережеве обладнання, сервери, робочі станції, телекомунікаційне обладнання, периферія, джерела безперебійного живлення тощо);

– фінансові активи (грошові кошти, бездокументарні цінні папери) в електронній формі (зокрема кошти на рахунках, керованих за допомогою систем «клієнт-банк»).

Договір страхування (страховий поліс) може передбачати відшкодування прямих збитків у разі настання різних страхових випадків, як-от:

– вихід з ладу (збої в роботі) інформаційних систем, обумовлені недостатньою якістю використовуваних програмних і апаратних засобів, помилками під час їх проєктування, розробки, виробництва, установки, налаштування, обслуговування або експлуатації;

– навмисні протиправні дії співробітників підприємства, вчинені з метою завдати шкоди підприємству або отримати певну вигоду;

– напади (атаки) на інформаційні системи підприємства, які здійснені третіми особами з метою завдати шкоди інформаційним ресурсам підприємства і його інформаційним системам (пошкодити або знищити інформацію, що зберігається в електронному вигляді, отримати конфіденційні відомості, вивести з ладу програмні і апаратні засоби з метою припинити або призупинити функціонування певних сервісів і т. ін.);

– впливу шкідливих програм і макросів (вірусів, хробаків і т. ін.), що спричинили порушення роботи інформаційних систем, втрату інформації або розголошення конфіденційної інформації;

– розкрадання фінансових активів (грошових коштів, бездокументарних цінних паперів), вчинене шляхом здійснення різних неправомірних дій: крадіжки паролів і ключів, присвоєння особистості, внесення змін у програмне забезпечення і т. ін.

На додаток до основних ризиків, безпосередньо пов’язаних з інформаційними активами, також можуть бути застраховані:

– збитки від припинення основної господарської діяльності підприємства внаслідок порушення роботи інформаційних систем;

– додаткові витрати, пов’язані з підтриманням поточної господарської діяльності в період відновлення роботи пошкоджених інформаційних систем;

– додаткові витрати, пов’язані з терміновим відновленням роботи інформаційних систем, а також терміновим відновленням основної господарської діяльності підприємства;

– додаткові витрати на відновлення ділової репутації після того, як їй було завдано збитків внаслідок атаки на інформаційні ресурси та інформаційні системи.

Збитки від призупинення основної господарської діяльності підприємства можуть включати в себе упущену вигоду, зумовлену простоєм інформаційних систем (тобто той прибуток, який підприємство могло б отримати, але не отримало внаслідок виходу з ладу інформаційних систем), а також витрати на підтримку інфраструктури підприємства в період вимушеного простою (зазвичай це деякі постійні витрати, які не залежать від обсягу випуску продукції та інтенсивності господарської діяльності). Додаткові витрати, пов'язані з підтриманням поточної господарської діяльності в період відновлення роботи пошкоджених інформаційних систем, можуть виникати, якщо існують деякі альтернативні способи обробки і зберігання інформації та здійснення бізнес-процесів (наприклад, на базі програмних і апаратних засобів, а також телекомунікаційних каналів, тимчасово орендованих у спеціалізованих компаній), і підприємство визнає необхідним скористатися цими альтернативними способами. Водночас задіяння таких резервних ресурсів зазвичай має бути узгоджене зі страховою компанією, покриває ці витрати. Додаткові витрати, пов'язані з терміновим відновленням роботи інформаційних систем, можуть виникати, якщо, наприклад, у сторонніх постачальників існують деякі альтернативні (більш оперативні, порівняно зі звичайними) умови поставок обладнання та програмного забезпечення, а також надання послуг зі введення в дію інформаційних систем.

Усі ці видатки, очевидно, також можуть бути об'єктами страхування. Водночас у кожній ситуації страховику і страхувальнику необхідно детально проаналізувати різні альтернативи виходу з кризової ситуації і вибирати найбільш доцільні варіанти. Так, наприклад, страхова компанія може відмовитися компенсувати додаткові витрати, пов'язані з терміновим відновленням інформаційних систем, якщо більш вигідною є компенсація упущеної вигоди за період більш тривалого вимушеного простою.

Процедура страхування (життєвий цикл договору страхування) включає в себе кілька основних етапів (рис. 22.1).

1. Попереднє обстеження підприємства, аналіз наявних ризиків для інформаційної безпеки.

2. Формулювання рекомендацій щодо зменшення ризиків та реалізація підприємством відповідних заходів.

3. Узгодження умов страхування і укладення договору.

4. Аналіз збитку і його розрахунок у грошовому еквіваленті в разі реалізації застрахованих ризиків.

5. Узгодження і подальше здійснення страхових виплат, що покривають збитки.

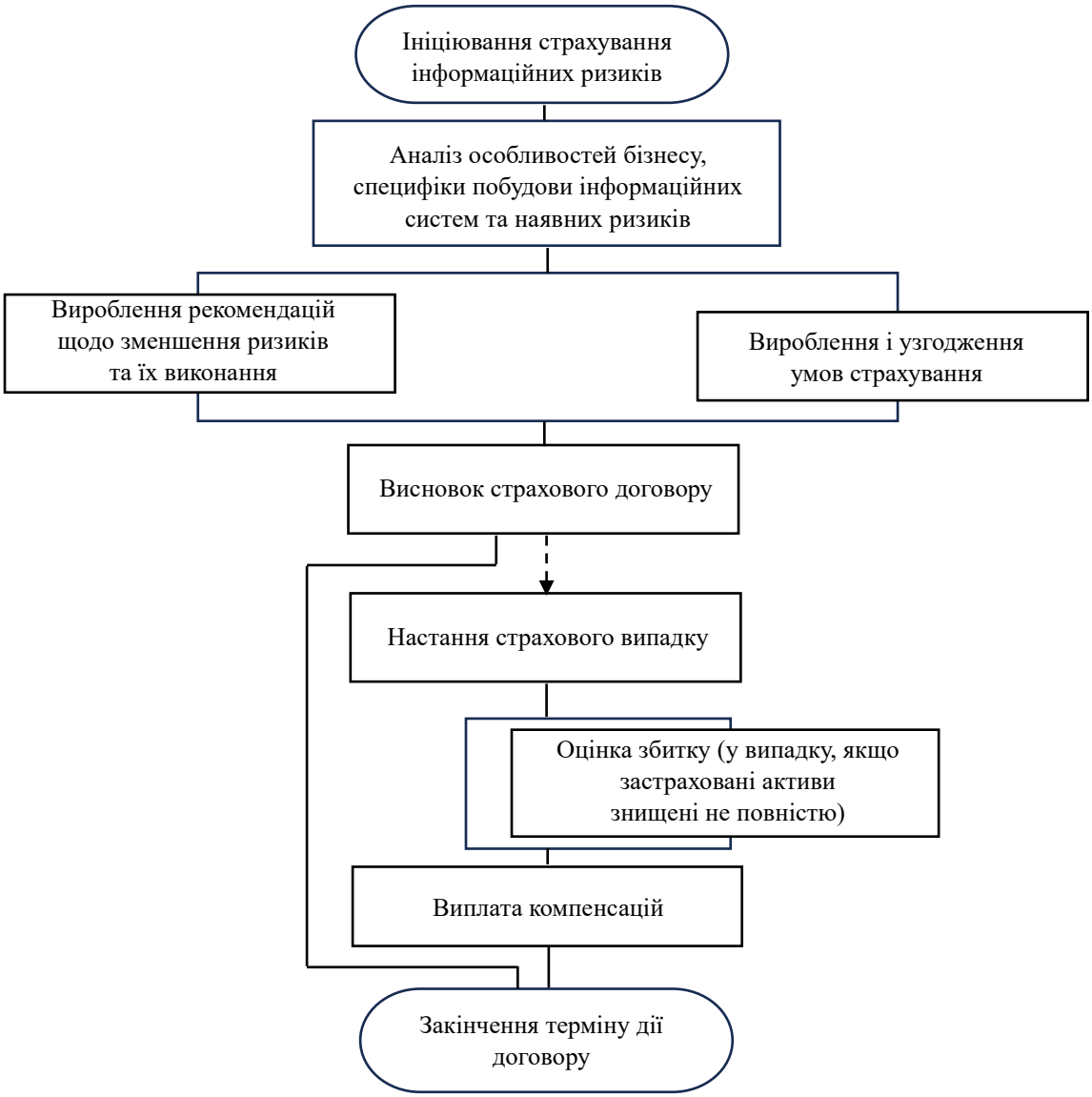

Рисунок 22.1. Основні стадії процесу страхування інформаційних ризиків перенабрати

Попереднє обстеження підприємства до укладення договору страхування в багато чому аналогічне проведенню зовнішнього аудиту і також може здійснюватися незалежною спеціалізованою компанією. Після закінчення такої перевірки можуть бути сформовані два основні документи:

– звіт (висновок) про стан інформаційної безпеки на підприємстві;

– рекомендації щодо підвищення рівня захищеності інформаційних ресурсів і зменшення ризиків.

Таке обстеження надалі створює передумови для прийняття рішення про можливість і доцільність страхування інформаційних ризиків цього підприємства, а також для обґрунтованого кількісного аналізу ризиків та визначення основних параметрів договору страхування.

На основі оцінок ризиків (з урахуванням реалізації рекомендованих заходів щодо їх зменшення) визначається одна з найбільш істотних умов договору

страхування – ставка страхування. Зазвичай її розмір не перевищує п'яти відсотків, однак на практиці він може варіюватися в діапазоні від декількох десятих часток відсотка до п'яти і більше відсотків. На розмір ставки у кожному конкретному випадку можуть вплинути декілька факторів:

– статистичні дані, що стосуються порушень інформаційної безпеки на аналогічних підприємствах;

– рівень захищеності інформаційних ресурсів цього підприємства (якість використовуваних технічних засобів, рівень організаційного забезпечення інформаційної безпеки на підприємстві і т. ін.);

– інтенсивність поточної господарської діяльності (виконання поточних бізнес-операцій);

– страхова сума – вартість інформаційних активів, що підлягають страхуванню (зазвичай чим більша вартість страхування ресурсів, тим нижча питома ставка страхування).

Крім ставки страхування, у процесі узгодження умов договору також визначається інший важливий параметр – ліміт відповідальності страхової компанії (максимальна величина коштів, які можуть бути виплачені страховиком страхувальнику протягом усього терміну дії договору страхування). Зазвичай страхова сума повинна бути достатньо великою, щоб у страхової компанії була можливість компенсувати накладні витрати (зокрема витрати на попереднє обстеження підприємства), пов'язані з укладанням договору страхування.

У разі реалізації ризику (виникнення страхового випадку) застраховані інформаційні ресурси можуть бути повністю втрачені. Водночас страхова компанія повинна буде зробити страхові виплати в повному обсязі (у межах встановленого ліміту відповідальності). У випадку, якщо пошкоджена тільки частина інформаційних ресурсів, для підприємства і страхової компанії починається складний процес визначення суми збитку, яка повинна бути компенсована. Така оцінка також може бути проведена незалежною третьою стороною. До того ж предметом аналізу в цій ситуації можуть бути всі обставини, пов'язані зі страховим випадком. Зокрема, договором страхування може бути передбачений обов'язок підприємства-клієнта вжити низку заходів у межах певного плану аварійних заходів з метою мінімізувати збиток. Отже, страхова компанія, перш ніж зробити виплати, повинна буде переконатися в тому, що підприємством-клієнтом були зроблені певні запобіжні заходи.

Та обставина, що взаємодія страховика і страхувальника під час визначення розміру страхових виплат є одним з найбільш проблемних питань, змушує передові компанії шукати нові форми організації процесу страхування. Так, наприклад, для вирішення проблем під час реалізації деяких страхових ризиків та зменшення збитків третьою стороною в договорі страхування може виступати компанія – постачальник інформаційних систем і комплексних рішень, яка у

разі настання страхового випадку може на деякий час (на період відновлювальних робіт) надати резервні програмні та апаратні засоби для забезпечення безперервності основної діяльності підприємства-страхувальника, а також організувати самі відновлювальні роботи. У цьому випадку страхова компанія може скоротити розмір страхових виплат на компенсацію упущеної вигоди підприємства-страхувальника і уникнути деяких зайвих виплат на відновлення втрачених інформаційних ресурсів.

Крім страхування власне інформаційних ризиків, також важливе значення має страхування цивільної відповідальності компаній, що надають інформаційні послуги та послуги із захисту інформації великій кількості користувачів:

– страхування цивільної відповідальності засвідчувальних центрів, що працюють в інфраструктурі публічних ключів;

– страхування відповідальності фондових бірж та інших електронних торговельних майданчиків із відшкодування майнової шкоди третім особам;

– страхування цивільної відповідальності розробників і постачальників засобів захисту інформації.

Необхідність страхування цивільної відповідальності компаній-постачальників продуктів і послуг перед споживачами в цьому випадку обумовлена тим, що їх послугами (продуктами) користується велика кількість клієнтів, кожен з яких з використанням цих продуктів і послуг управляє дорогими інформаційними активами (фінансовими засобами, конфіденційними відомостями, розголошення яких може призвести до величезних збитків, тощо). Отже, у компаній-постачальників таких продуктів і послуг виникають ризики того, що до них будуть пред'явлені позови про відшкодування збитку, понесеного клієнтами внаслідок того, що зловмисники скористалися вразливостями програмних продуктів, які були поставлені компаніями-розробниками. Очевидно, що власні активи і доступні засоби, наявні у компаній-постачальників, зазвичай набагато менші від потенційного збитку, який може виникнути у їхніх клієнтів. Внаслідок цього страхування виявляється єдиним засобом забезпечення відповідальності, а отже, побудови цивілізованих відношень на ринку засобів захисту інформації, а також послуг із захисту інформації.

22.2. Ринок страхових послуг

Світова практика страхування інформаційних ризиків почала складатися в дев'яностих роках і отримала свій розвиток після 2000-го р., коли, з одного боку, ризики інформаційної безпеки стали більш серйозними, ніж будь-коли, а з іншого – в західних країнах остаточно склалася практика не включати інформаційні ризики в універсальні страхові поліси, якими зазвичай покривалися основні бізнес-ризики. Отже, до теперішнього часу найбільшими світовими компаніями, що надають послуги зі страхування інформаційних ризиків, є:

– Британська страхова компанія «Lloyds of London»;
– американська компанія «AIG»;
– Zurich North America («The E-Risk Edge solution»);
– страхова група «Chubb»;
– страхова компанія «Marsh».

Страхування інформаційних ризиків компанією Lloyds of London здійснюється спільно з відомою компанією Counterpane, що надає послуги з оцінки стану захищеності інформаційних ресурсів і за поточної підтримки інформаційної безпеки. Також у цій роботі беруть участь компанії Frank Crystal & Co. і SafeOnline Ltd. Ці фірми пропонують два основні спільні страхові продукти:

– Internet Asset and Income Protection Coverage [Покриття ризиків, пов'язаних з інформаційними активами і інформаційною діяльністю] – програма страхування інформаційних ресурсів окремих компаній;

– Internet Asset and Income Protection Warranty Plan [План гарантування інформаційних активів та інформаційної діяльності»] – заснований на страхуванні план гарантування надійності роботи постачальників послуг інтернету.

Американська страхова компанія American International Group, Inc. (AIG), що діє в 130 країнах світу, в особі свого підрозділу AIG eBusiness Risk Solutions (AIG eBRS) пропонує програму страхування інформаційних ризиків netAdvantage (AIG netAdvantage Suite). У рамках своєї комплексної програми страхування ця компанія пропонує знижки клієнтам, які користуються певними засобами захисту інформації. Для забезпечення ефективності та комплексності послуг зі страхування AIG eBRS організовує технологічні альянси з компаніями, які постачають засоби захисту інформації, а також провідними аудитами безпеки.

У межах програми netAdvantage пропонується кілька варіантів страхового захисту:

– захист від збитків у разі неправомірного розголошення приватних даних;
– захист від знищення (втрати) даних або програмного забезпечення;
– захист від збитків у разі порушення операційної діяльності (упущена вигода і додаткові витрати) у разі порушень інформаційної безпеки;
– страхова компенсація витрат на нейтралізацію вразливостей;
– страхова компенсація витрат на відновлення ділової репутації (PR) у разі реалізації ризиків.

Контрольні питання:

1. Що є об'єктами страхування інформаційних ризиків?
2. Назвіть основні стадії процесу страхування інформаційних ризиків.
3. Назвіть найбільші світові компанії, що надають послуги зі страхування інформаційних ризиків.

ТЕМА 23
МІЖНАРОДНИЙ СТАНДАРТ ISO/IEC 27001

У темі розглядаються основні аспекти та положення, а саме інформаційні технології, методи забезпечення безпеки, системи менеджменту інформаційної безпеки, міжнародного стандарту ISO/IEC 27001.

ISO/IEC 27001 встановлює вимоги до створення, впровадження, підтримки та постійного поліпшення системи менеджменту інформаційної безпеки в контексті організації. Він також включає в себе вимоги до оцінки і обробки ризиків інформаційної безпеки з урахуванням потреб організації. Вимоги, викладені в ISO/IEC 27001, є загальними і призначені для застосування всіма організаціями, незалежно від їх типу, розміру і характеру. Входить в групу стандартів ISO 27000 – СУІБ та тісно пов'язаний зі стандартом ISO/IEC 27002.

***Ключові слова**: інформаційна безпека, менеджмент, міжнародний стандарт, політика інформаційної безпеки, ризики, компетентність, моніторинг, аудит.*

План

23.1. Розгляд міжнародного стандарту ISO/IEC 27001.

23.1. Розгляд міжнародного стандарту ISO/IEC 27001

1. СФЕРА ЗАСТОСУВАННЯ

Цей стандарт визначає вимоги до проектування, впровадження, підтримки та постійного вдосконалення системи управління інформаційною безпекою з урахуванням обставин організації. Цей стандарт також містить вимоги для оцінювання та оброблення ризиків інформаційної безпеки, пов'язаних з потребами організації. Вимоги, наведені в цьому стандарті, є загальними та можуть бути запроваджені для всіх організацій незалежно від типу, розміру та природи. Вилучення будь-якої з вимог, наведених у розділах 4–10, неприпустимо в разі, якщо організація прагне відповідати цьому стандарту.

2. НОРМАТИВНІ ПОСИЛАННЯ

Наведені нижче нормативні документи в цілому або в частині необхідні для застосування цього стандарту. У разі датованих посилань застосовують лише наведені видання. У разі недатованих посилань потрібно користуватись останнім виданням нормативних документів (разом зі змінами).

ISO/IEC 27000 Information technology – Security techniques – Information security management systems – Overview and vocabulary.

3. ТЕРМІНИ ТА ВИЗНАЧЕННЯ ПОНЯТЬ

У цьому стандарті використовують терміни та визначення, які надано в ISO/IEC 27000.

4. ОБСТАВИНИ ОРГАНІЗАЦІЇ

4.1. Розуміння організації та її обставин

Організація повинна визначити внутрішні та зовнішні обставини, які важливі для її цілей та впливають на можливість досягнення наперед запланованого результату(-ів) її системи управління інформаційною безпекою.

Примітка. Визначення цих обставин стосується визначення внутрішнього та зовнішнього середовища організації, розглянутого в розділі 5.3 ISO 31000: 2009.

4.2. Розуміння потреб та очікувань зацікавлених сторін

Організація повинна визначити:

a) зацікавлені сторони, які важливі для системи управління інформаційною безпекою;

b) вимоги цих зацікавлених сторін, важливих для інформаційної безпеки.

Примітка. Вимоги зацікавлених сторін можуть охоплювати законодавчі та регуляторні вимоги, а також контрактні зобов'язання.

4.3. Визначення сфери застосування системи управління інформаційною безпекою

Організація повинна визначити межі та можливість застосування системи управління інформаційною безпекою для встановлення її сфери застосування. Для визначення сфери застосування організація повинна розглянути:

a) зовнішні та внутрішні обставини, зазначені в 4.1;

b) вимоги, зазначені в 4.2;

c) інтерфейси та залежності між діями, які виконує організація, і тими, що виконують інші організації.

Сфера застосування має бути доступною як документована інформація.

4.4. Система управління інформаційною безпекою

Організація повинна розробити, впровадити, підтримувати та постійно вдосконалювати систему інформаційної безпеки відповідно до вимог цього стандарту.

5. КЕРІВНИЦТВО

5.1. Керівництво та зобов'язання

Вище керівництво повинно продемонструвати дії з управління та зобов'язання по відношенню до систем управління інформаційною безпекою:

a) гарантуванням, що політика інформаційної безпеки та цілі інформаційної безпеки розроблені та сумісні зі стратегічними планами організації;

b) гарантуванням інтеграції вимог системи інформаційної безпеки в процеси організації;

c) гарантуванням, що ресурси, потрібні для системи управління інформаційною безпекою, доступні;

d) доведенням до відома організації важливості ефективного управління інформаційною безпекою та відповідності вимогам системи управління інформаційною безпекою;

e) гарантуванням, що система управління інформаційною безпекою досягне своїх запланованих результатів;

f) призначенням та підтримкою осіб для досягнення ефективності системи управління інформаційною безпекою;

g) сприянням постійному вдосконаленню;

h) підтримкою інших пов'язаних ролей вищого керівництва, щоб продемонструвати їх керівну роль, яку вони застосовують у сферах їх відповідальності.

5.2. Політика

Вище керівництво повинно запровадити політику інформаційної безпеки, яка:

a) відповідає цілям організації;

b) містить цілі інформаційної безпеки (див. 6.2) або зазначає основні положення для визначення цілей інформаційної безпеки;

c) містить зобов'язання відповідати застосованим вимогам, пов'язаним з інформаційною безпекою;

d) містить зобов'язання щодо постійного вдосконалення системи управління інформаційною безпекою.

Політика інформаційної безпеки має:

e) бути доступною як документована інформація;

f) бути розповсюдженою в середині організації;

g) бути доступною зацікавленим сторонам, за потреби.

5.3. Організаційні ролі, відповідальності та повноваження

Вище керівництво повинно гарантувати, що відповідальності та повноваження для ролей, пов'язаних з інформаційною безпекою, призначені й доведені.

Вище керівництво повинно призначити відповідальності та повноваження для:

a) гарантування, що система управління інформаційною безпекою відповідає вимогам цього стандарту; і

b) звітування вищому керівництву щодо результативності системи управління інформаційною безпекою.

Примітка. Вище керівництво може також призначити відповідальності та повноваження для звітування щодо результативності системи управління інформаційною безпекою в межах організації.

6. ПЛАНУВАННЯ

6.1. Дії щодо ризиків та можливостей

6.1.1. Загальні положення

Під час планування системи управління інформаційною безпекою організація повинна розглянути питання, описані в 4.1, і вимоги, описані в 4.2, а також визначити ризики та можливості, які потрібно мати на увазі, щоб:

a) гарантувати, що система управління інформаційною безпекою може досягти запланованого результату(-ів);

b) запобігти або зменшити небажані ефекти; і

c) досягти постійного вдосконалення.

Організація повинна планувати:

d) дії, які стосуються цих ризиків та можливостей,

e) як саме

1) інтегрувати й упровадити ці дії до процесів її системи управління інформаційною безпекою;

2) оцінювати ефективність цих дій.

6.1.2. Оцінка ризиків інформаційної безпеки

Організація повинна визначити та застосовувати процес оцінювання ризиків інформаційної безпеки, який:

a) встановлює та підтримує критерії ризиків інформаційної безпеки, які містять:

1) критерії прийняття ризиків;

2) критерії для виконання оцінки ризиків інформаційної безпеки;

b) гарантує, що повторні оцінки ризиків інформаційної безпеки призводять до послідовних, дійових та порівняльних результатів;

c) ідентифікує ризики інформаційної безпеки:

1) застосовує процес оцінювання ризиків інформаційної безпеки для ідентифікації ризиків, пов’язаних із втратою конфіденційності, цілісності й доступності в межах сфери застосування системи управління інформаційною безпекою;

2) ідентифікує власників ризиків;

d) виконує аналіз ризиків інформаційної безпеки:

1) оцінює потенційні наслідки, які будуть результатом реалізації ризиків, ідентифікованих в 6.1.2 c) 1);

2) оцінює практичну імовірність появи ризиків, ідентифікованих у 6.1.2 c) 1);

3) визначає рівні ризиків;

e) оцінює ризики інформаційної безпеки:

1) порівнює результати аналізу ризиків з критеріями ризиків, визначеними в 6.1.2 a);

2) визначає пріоритети проаналізованих ризиків для оброблення ризиків.

Організація повинна зберігати документовану інформацію стосовно процесу оцінювання ризиків інформаційної безпеки.

6.1.3. Оброблення ризиків інформаційної безпеки

Організація повинна визначити та застосовувати процес оброблення ризиків інформаційної безпеки для:

a) вибору доречних опцій оброблення ризиків інформаційної безпеки з урахуванням результатів оцінки ризиків;

b) визначити всі заходи безпеки, які необхідно впровадити для вибраної (-их) опції(-ій) оброблення ризиків;

Примітка. Організація може розробити необхідні заходи безпеки або ідентифікувати їх з будь-якого джерела.

c) порівняти заходи безпеки, визначені в 6.1.3 b) вище, з наведеними в додатку A, і підтвердити, що не було опущено потрібних заходів безпеки;

Примітка 1. Додаток А містить всебічний перелік цілей заходів безпеки та заходів безпеки. Користувачів цього стандарту відсилаємо до додатка А для впевненості, що необхідні заходи безпеки не було пропущено.

Примітка 2. Цілі заходів безпеки повністю долучено до вибраних заходів безпеки Перелік цілей заходів безпеки та заходи безпеки, надані в додатку А, не є вичерпними і можуть бути потрібні додаткові цілі заходів безпеки та заходи безпеки.

d) підготувати Положення щодо застосовності, яке містить:

– необхідні заходи безпеки (див. 6.1.3 b) та c));

– обґрунтування для їх застосування;

– впроваджені необхідні заходи безпеки чи ні;

– обґрунтування для виключень заходів безпеки, наданих у додатку А;

e) розробити план оброблення ризиків інформаційної безпеки; та

f) отримати від власників ризиків підтвердження плану оброблення ризиків інформаційної безпеки та згоду на залишкові ризики інформаційної безпеки. Організація повинна зберігати задокументовану інформацію щодо процесу оброблення ризиків інформаційної безпеки.

Примітка. Процес оцінювання та оброблення ризиків інформаційної безпеки в цьому стандарті відповідає принципам та загальним настановам, зазначеним в ISO 31000.

6.2. Цілі інформаційної безпеки та планування їх досягнення

Організація повинна встановити цілі інформаційної безпеки для відповідних функцій та рівнів. Цілі інформаційної безпеки мають:

a) відповідати політиці інформаційної безпеки;

b) бути вимірюваними (якщо доцільно);

c) враховувати вимоги до інформаційної безпеки, які застосовують, а також результати оцінювання ризиків та оброблення ризиків;

d) бути розповсюдженими; та

e) оновлюватися, за потреби.

Організація повинна зберігати документовану інформацію щодо цілей інформаційної безпеки. Під час планування дій для досягнення цілей інформаційної безпеки організація повинна визначити:

f) що треба зробити;

g) які ресурси будуть потрібні;

h) хто буде відповідальним;

i) коли процес буде завершено; та

j) як результати будуть оцінювати.

7. ПІДТРИМКА

7.1. Ресурси

Організація повинна визначити й забезпечувати наявність ресурсів, потрібних для розроблення, впровадження, підтримання й постійного вдосконалення системи управління інформаційною безпекою.

7.2. Компетенція

Організація повинна:

a) визначити рівень необхідної компетентності персоналу, який виконує роботи, що впливають на результативність інформаційної безпеки;

b) гарантувати, що цей персонал має компетенцію на основі відповідного навчання, тренінгів або досвіду;

c) за можливості, забезпечувати виконання певних дій для досягнення необхідної компетенції та оцінювати ефективність таких дій;

d) зберігати відповідну документовану інформацію як доказ компетентності.

Примітка. Можливі дії можуть охоплювати, наприклад: проведення тренінгів, наставництво або перепризначення наявних працівників, або наймання на роботу чи за контрактом компетентних осіб.

7.3. Обізнаність

Персонал, який виконує функції під наглядом організації, повинен бути обізнаним в:

a) політиці інформаційної безпеки;

b) його вкладі в ефективність системи управління інформаційною безпекою, враховуючи переваги від вдосконалення результативності інформаційної безпеки; та

c) розумінні невідповідності вимогам системи управління інформаційною безпекою.

7.4. Комунікація

Організація повинна визначити потребу у внутрішніх та зовнішніх комунікаціях з питань системи управління інформаційною безпекою, включаючи:

a) з яких питань спілкуватися;

b) коли спілкуватися;

c) з ким спілкуватися;

d) хто повинен спілкуватися; та

e) процеси, за допомогою яких комунікація повинна відбуватися.

7.5. Документована інформація

7.5.1. Загальні положення

Система управління інформаційною безпекою організації повинна включати:

a) документовану інформацію, визначену цим стандартом;

b) документовану інформацію, визначену організацією як необхідну для ефективності системи управління інформаційною безпекою.

Примітка. Обсяги документованої інформації для системи управління інформаційною безпекою можуть бути різними для різних організацій залежно від:

1) розміру організації й типу її діяльності, процесів, продуктів і послуг;

2) складності процесів та їх взаємодії; і

3) компетенції персоналу.

7.5.2. Створення та оновлення

У разі створення й оновлення документованої інформації організація повинна гарантувати відповідну:

a) ідентифікацію та опис (наприклад, назву, дату, автора чи посилальний номер);

b) формат (наприклад, мову, версію програмного забезпечення, графіки) та носії (наприклад, папір, електронні); та

c) перегляд і затвердження для відповідності й адекватності.

7.5.3. Контроль документованої інформації

Задокументована інформація, визначена системою управління інформаційною безпекою та цим стандартом має контролювати для гарантії того, що:

a) вона доступна й придатна для використання, де і коли вона потрібна; і

b) її належним чином захищено (наприклад, від втрати конфіденційності, помилкового використання або втрати цілісності). Для контролю документованої інформації організація повинна виконувати такі дії відповідним чином:

c) розподіл, доступ, повернення та використання;

d) збереження та консервування, зокрема й консервування чіткості / розбірливості;

e) контроль змін (наприклад, контроль версій);

f) утримування й розташування.

Документована інформація від зовнішнього джерела, визначена організацією як необхідна для планування та функціонування системи управління інформаційною безпекою, має бути ідентифікована відповідних чином і контрольована.

Примітка. Доступ означає рішення стосовно дозволу лише на перегляд документованої інформації чи дозволу та повноважень на перегляд і зміну документованої інформації тощо.

8. ФУНКЦІОНУВАННЯ

8.1. Робоче планування й контроль

Організація повинна планувати, впроваджувати й контролювати процеси, необхідні для виконання вимог інформаційної безпеки, а також впроваджувати дії, визначені в 6.1. Організація також повинна впроваджувати плани для досягнення цілей інформаційної безпеки, визначених в 6.2.

Організація повинна зберігати документовану інформацію в обсязі, необхідному для впевненості, що процес виконується як було заплановано.

Організація повинна контролювати заплановані зміни та переглядати наслідки непередбачених змін, застосовуючи дії для усунення будь-яких шкідливих дій, за потреби.

Організація повинна гарантувати, що процеси, віддані на аутсорсинг, визначені й контрольовані.

8.2. Оцінювання ризиків інформаційної безпеки

Організація повинна виконувати оцінювання ризиків через заплановані інтервали або коли запропоновані чи відбуваються суттєві зміни з урахуванням критеріїв, визначених в 6.1.2 a).

Організація повинна зберігати задокументовану інформацію стосовно результатів оцінювання ризиків інформаційної безпеки.

8.3. Оброблення ризиків інформаційної безпеки

Організація повинна впровадити план оброблення ризиків інформаційної безпеки.

Організація повинна зберігати задокументовану інформацію стосовно результатів оброблення ризиків інформаційної безпеки.

9. ОЦІНЮВАННЯ РЕЗУЛЬТАТИВНОСТІ

9.1. Моніторинг, вимірювання, аналіз та оцінювання

Організація повинна оцінювати результативність інформаційної безпеки та ефективність системи управління інформаційною безпекою. Організація повинна визначити:

a) що саме потрібно моніторити й вимірювати, включаючи процеси інформаційної безпеки та заходи безпеки;

b) методи моніторингу, вимірювань, аналізу та оцінювання, які може бути застосовано для гарантії обґрунтованих результатів;

Примітка. Обрані методи, які надають порівняні та відтворювані результати, можна розглядати як обґрунтовані.

c) коли моніторинг та вимірювання потрібно виконувати;

d) хто повинен виконувати моніторинг та вимірювання;

e) коли результати моніторингу та вимірювань потрібно аналізувати й оцінювати;

f) хто повинен аналізувати й оцінювати ці результати. Організація повинна зберігати відповідну задокументовану інформацію як доказ результатів моніторингу та вимірювань.

9.2. Внутрішній аудит

Організація повинна проводити внутрішні аудити через заплановані інтервали часу для забезпечення того, що інформація чи система управління інформаційною безпекою:

a) відповідають

1) власним вимогам організації для її системи управління інформаційною безпекою;

2) вимогам цього стандарту;

b) ефективно впроваджена та підтримується.

Організація повинна:

c) планувати, розробляти, впроваджувати та підтримувати програму(-и) аудиту, зокрема й частоту, методи, відповідальності, заплановані вимоги та звітність. Програма(-и) аудиту повинна(-і) враховувати аналіз важливості процесів, що їх розглядають, і результати попередніх аудитів;

d) визначити критерії аудиту та сферу застосування для кожного аудиту;

e) призначити аудиторів і виконати аудити, які гарантують об’єктивність і неупередженість процесу аудиту;

f) гарантувати, що результати аудиту буде доведено до відповідного керівництва;

g) зберігати документовану інформацію як доказ програми аудиту та результатів аудиту.

9.3. Перегляд з боку керівництва

Вище керівництво повинно переглядати систему управління інформаційною безпекою організації через заплановані проміжки часу для гарантування її постійної придатності, адекватності й ефективності. Перегляд з боку керівництва повинен стосуватися розгляду:

a) статусу дії, що є наслідком попереднього перегляду керівництва;

b) зміни в зовнішніх та внутрішніх обставинах, які мають відношення до системи управління інформаційною безпекою;

c) зворотного впливу на результативність інформаційної безпеки, охоплюючи тенденції в:

1) невідповідностях та коригувальних діях;

2) результатах моніторингу та вимірювань;

3) результатах аудиту;

4) досягненнях цілей інформаційної безпеки;

d) зворотного зв’язку від зацікавлених сторін;

e) результатів оцінювання ризиків і статусу плану оброблення ризиків;

f) можливостей для постійного вдосконалення.

Вихідні дані перегляду з боку керівництва повинні включати рішення стосовно можливостей постійного вдосконалення та будь-яких потреб внесення змін до системи управління інформаційною безпекою.

Організація повинна зберігати документовану інформацію як доказ результатів переглядів з боку керівництва.

10. ВДОСКОНАЛЕННЯ

10.1. Невідповідності й корегувальні дії

У разі виявлення невідповідностей організація повинна:

a) реагувати на невідповідності і за можливості:

1) виконувати дії для контролю та їх корекції;

2) вживати заходів щодо наслідків;

b) оцінювати потреби в діях для усунення причин невідповідностей для запобігання їх повторення чи виникнення будь-де за допомогою:

1) перегляду невідповідностей;

2) визначення причин невідповідностей;

3) визначення, чи існують подібні невідповідності або потенційно можуть з'являтися;

c) впровадити певні дії, за потреби;

d) переглянути ефективність виконаних коригувальних дій;

e) внести зміни до системи управління інформаційною безпекою, за потреби.

Коригувальні дії мають бути адекватними до наслідків виявлених невідповідностей. Організація повинна зберігати документовану інформацію як доказ:

f) сутності невідповідностей та будь-яких послідовних дій, що були виконані;

g) результати будь-яких коригувальних дій.

10.2. Постійне вдосконалення

Організація повинна постійно вдосконалювати придатність, адекватність та ефективність системи управління інформаційною безпекою, гарантування її постійної придатності, адекватності та ефективності.

Контрольні питання

1. Що таке інформаційна безпека?
2. Що таке менеджмент інформаційної безпеки?
3. Що таке політика інформаційної безпеки?
4. Дайте визначення поняття компетентність.
5. Що таке аудит?

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна література

1. Управління інформаційною безпекою: навч.-метод. посіб. / А. І. Поворознюк, О. А. Поворознюк. Харків: НТУ «ХПІ», 2021. 135 с.

2. Поворознюк А. І., Поворознюк О. А., Філатова Г. Є. Багатокритеріальна оцінка альтернатив при проєктуванні двохфакторної автентифікації суб'єктів-користувачів в системах захисту інформації. *Системи управління, навігації та зв'язку.* 2021. Вип. 2(64). С. 92–95.

3. Замула О. А., Горбенко Ю. І., Шумов А. І. Нормативно-правове забезпечення інформаційної безпеки. Комплексні системи захисту інформації: навч. посіб. Харків: ХНУРЕ, 2010. 78 с.

4. Замула О. А. Захист держаних секретів: навч. посіб. ХНУРЕ. 2004. 206 с.

5. ANSI/X3/SPARC Study Group on Database Management Systems: Interim report, 1975. P. 92–141.

6. CSC-STD-003-85, Computer Security Requirements Guidance for Applying the Department of Defense System Evaluation Criteria in Specific Environments. *Federation of American Scientist.* URL: www.fas.org/irp/nsa/rainbow/std003.htm

7. Datapro Reports on Information Security. Vol. 1–3, 1990–1993. *SCM.Portal.* URL: portal.acm.org/citation.cfm?id=17735

8. DoD 5200.28-STD. Department of Defence Trusted Computer System Evaluation Criteria (TCSEC) 1985. URL: ftp.fas.org/irp/nsa/rainbow /std001.htm

9. Evaluation Levels Manual, Department of Trade and Industry, Computer Security Branch, Kingsgate House. Vol. 22. P. 66–74.

10. ISO/DIS 2382/8. Data processing. *Vocabulary. Part 8: Control, integrity and security. ISO.* 1985. 35 p.

11. National Bureau of Standards, «Data Encryption Standard», January 1977, NIST NBS-FIPS PUB 46. Безопасность информационных технологий. URL: http://www.security.ukrnet.net/modules/sections/index.php?ar-id=181&op= viewarticle

12. NCSC-TG-001. A Guide to Understanding Audit in Trusted Systems. *Federation of American Scientist.* URL: fas.org/irp/nsa/rainbow /tg001.htm

13. NCSC-TG-003. A Guide to Understanding Discretionary Access Control in Trusted Systems. Federation of American Scientist. URL: ftp.fas.org/irp/nsa/rainbow/ tg003.htm

14. NCSC-TG-005. Version-1. Trusted Network Interpretation of the trusted Computer System Evaluation Criteria. *National Technical Information Service.* URL: http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html& identifier= ADA255422

15. NCSC-TG-006. A Guide to Understanding Configuration Management in Trusted Systems. Federation of American Scientist. URL: www.fas.org-/irp/nsa/rainbow/tg006.htm

16. NCSC-TG-009. Version-1. Computer Security Subsystem Interpretation of the Trusted Computer System Evaluation Criteria. *Federation of American Scientist.* URL: ftp.fas.org/irp/nsa/rainbow/tg009.htm

17. NCSC-TG-021. Version-1. Draft Trusted Database Management System Interpretation of the Trusted Computer System Evaluation Criteria. *Безопасность информационных технологий.* URL: http://www.security.ukrnet.net/modules/sections/index.php?artid=181&op=viewarticle

18. Gladny H. M. Performance of Computer Installation, Berke. 1978, Proceedings. P. 151–200.

19. HighLand H. J. Novell network virus alert., C&S. 1990. Vol. 9. № 7. P. 570.

20. Linde Richard R. Operating System Penetration, Proceedings. 1975 NCC. P. 361–368.

21. Linden T. A. (editor) Security Analysis and Enhancements of Computer Operating Systems, Institute for Computer Sciences and Technology of National Bureau of Standarts, Washington, D.C.20234, Report NBSIR 76-1041, April 1976.

22. Olson I. M., Abrams M. D., Computer Acces Policy Choices. *Computer & Security.* 1990. Vol. 9, № 8. P. 699–714.

23. Security & Protection. 1978. Vol. 10, № 2. P. 23–40.

24. Smith G. S. New Age Technology Threats and Vulnerabilities. *Journal of Forensic Accounting.* 2001. P. 125–130.

25. Straub D. W., Widom C. S. Deviancy by bit and bytes: computer abusers and control measures. *Computer security: A Global Challenge.* Netherlands, 1984. P. 431–441.

26. Parker T. A. Application Access Control Standarts for Distributed Systems. *Computer & Security.* Vol. 9, № 6. P. 319–330.

27. Parker T. A., Security in Open Systems – A Report on the Standart work of ECMA's TC32/TG9, P. 38–50 in Proc. 10th Natl. Computer Security Conf., IEEE, Baltimore, September, 1987.

28. Yves le Roux. Technical Criteria for Security Evaluation of Information Technology Products: Information Security Guide, 1990–1991. P. 59–62.

29. Zabihollah Rezaee. Financial Statement Fraud: Prevention and Detection, 2002. P. 276–279.

Допоміжна література

1. Закон України «Про інформацію» від 02.10.1992 р.

2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 31.05.2005 р., № 2594-IV, Київ, 2005.

3. Про заходи щодо захисту інформаційних ресурсів держави. Затверджено Указом Президента України № 582 від 10.04 2000 р.

4. Петренко С. А., Петренко А. А. Аудит безопасности. Internet. Москва: ДМК Пресс, 2002. 416 с.

4. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Постанова КМУ від 29.03.2006 р. № 373. Київ, 2006.

5. Порядок проведення робіт із створення комплексних систем захисту інформації в інформаційно-телекомунікаційних системах. НД ТЗІ 3.1-003-2005.

6. Закон України «Про державну таємницю» від 21.01.1994 р. *Закони України.* Київ, 1997. Т. 7.

7. Закон України «Про захист інформації в автоматизованих системах» від 05.07.1994 р. *Закони України.* Київ, 1997. Т. 7.

8. Закон України «Про рекламу». *Відомості Верховної Ради (ВВР).* 1996. № 39. С. 181.

9. Закон України «Про авторське право і суміжні права» від 23.12.1993 р. Закони України. Київ, 1996. Т. 6.

10. Закон України «Про банки та банківську діяльність» від 20.03.1991 р. *Закони України.* Київ, 1996. Т. 1.

11. Закон України «Про інформацію» від 02.10.1992 р. *Закони України.* Київ, 1996. Т. 4.

12. Закон України «Про науково-технічну інформацію» від 25.06.1993 р. *Закони України.* Київ, 1996. Т. 5.

13. Закон України «Про охорону прав на винаходи та корисні моделі» від 15.12.1993 р. *Закони України.* Київ, 1996. Т. 6.

14. Закон України «Про охорону прав на знаки для товарів та послуг» від 15.12.1993 р. *Закони України.* Київ, 1996. Т. 6.

15. Закон України «Про охорону прав на промислові зразки» від 15.12.1993 р. *Закони України.* Київ, 1996. Т. 6.

16. Постанова Кабінету Міністрів України «Про перелік відомостей, що не становлять комерційної таємниці» від 9 серпня 1993 р. № 611. *Збірник постанов Уряду України.* 1993. № 12.

17. Постанова Верховної Ради України «Про Концепцію (основи державної політики) національної безпеки України» від 18 липня 1995 р. № 532-95-п. *Відомості Верховної Ради (ВВР).* 1997. № 10. С. 85.

18. Постанова Верховної Ради України «Про Концепцію (основи державної політики) національної безпеки України» від 16 січня 1997 р. № 3/97-ВР. *Право України.* 1997. № 3. С. 84–89.

19. Кодекс про адміністративні правопорушення. *Відомості Верховної Ради Української РСР (ВВР).* 1984. Додаток до № 51. Ст. 1122.

20. Кримінальний кодекс України. *Відомості Верховної Ради (ВВР).* 2001. № 25–26. Ст. 131.

21. Стенг Д., Муи С. Секреты безопасности сетей. Киев: Диалектика, Информейшн Компьютер Энтерпрайз, 1996. 544 с.

22. Дюбуа Д., Прад А. Теория возможностей. Приложения к представлению знаний в информатике. Киев: Радио и связь, 2020. 288 с.

23. Antonucci D. The Cyber Risk Handbook. New Jersey: John Wiley & Sons, 2017. 433 с.

24. Kohnke A., Sigler K., Shoemaker D. Implementing Cybersecurity A Guide to the National Institute of Standards and Technology Risk Management Framework. Boca Raton: CRC Press, 2017. 338 с.

25. Kuypers M., Maillart T., Elisabeth P. An Empirical Analysis of Cyber Security Incidents at a Large Organization. FSI. 2015. URL: https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/kuypersweis_v7.pdf

26. Talabis M., Martin J. Information Security Risk Assessment Toolkit. Practical Assessments through Data Collection and Data Analysis. Waltham: Elsevier, 2013. 281 с.

27. Білоконь Д. С., Федулова І. В. Процес управління ризиками інформаційної безпеки. *Наукові праці НУХТ.* 2016. № 6. С. 84–91.

28. Бучик С. С., Шалаєв В. О. Аналіз інструментальних методів визначення ризиків інформаційної безпеки інформаційно-телекомунікаційних систем. *Наукоємні технології.* 2017. № 3. С. 215–225.

29. Замула А. А., Северинов А. В., Корниенко М. А. Анализ моделей оценки рисков информационной безопасности для построения системы защиты информации. *Наука і техніка Повітряних Сил Збройних Сил України.* 2014. № 2. С. 133–138.

30. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги: (ISO/IEC 27001:2013, IDT) ДСТУ ISO/IEC 27001: 2015. Київ: ДП «УкрНДНЦ», 2016. 89 с. (Національні стандарти України).

31. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Звід практик щодо заходів інформаційної безпеки: (ISO/IEC 27002:2013, IDT) ДСТУ ISO/IEC 27002:2015. Київ: ДП «УкрНДНЦ», 2016. 110 с. (Національні стандарти України).

32. Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки: (ISO/IEC 27002:2011, IDT) ДСТУ ISO/IEC 27005:2015. Київ: ДП «УкрНДНЦ», 2016. 91 с. (Національні стандарти України).

33. Керування ризиком. Словник термінів: (ISO Guide 73:2009, IDT) ДСТУ ISO Guide 73:2013. Київ: Мінекономрозвитку, 2014. 17 с. (Національні стандарти України).

34. Керування ризиком. Методи загального оцінювання ризику: (ISO/ IEC 31010:2009, IDT) ДСТУ ISO/IEC 31010:2013. Київ: Мінекономрозвитку, 2015. 80 с. (Національні стандарти України).

35. Пузиренко О. Г., Івко С. О., Лаврут О. О. Аналіз процесу управління ризиками інформаційної безпеки в забезпеченні живучості інформаційно-телекомунікаційних систем. *Системи обробки інформації.* 2014. № 8. С. 128–134.

36. Спроба локалізації ISO Guide 73:2009 «Risk management – vocabulary» / В. В. Мохор, О. М. Богданов, О. М. Крук, В. В. Цуркан. *Ukrainian Scientific Journal of Information Security.* 2012. № 2. С. 12–22.

37. ISO/IEC 27001, ISO Guide 73:2002, ISO/IECTR 18044:2018. Менеджмент информационной безопасности. URL: http://iso27.com/ (дата звернення: 15.12.2020).

38. SAE J1739:2000 Potential Failure Mode and Effects Analysis in Design (Design FMEA) and Potential Failure Mode and Effects Analysis in Manufacturing and Assembly Processes (Process FMEA), and Potential Failure Mode and Effects Analysis for Machinery.

39. Bashir M., Christin N. Three case studies in quantitative information risk analysis. Proceedings of the CERT/SEI *«Making the Business Case for Software Assurance Workshop».* Pittsburgh, PA, September 2008. P. 77–86.

40. Burtescu E. Decision Assistance in Risk Assessment Monte Carlo Simulations. Informatica Economica. 2012. Vol. 16. № 4.

41. Isabel L. Nunes and Mário Simões-Marques. Applications of Fuzzy Logic in Risk Assessment – The RA_X Case. *Centre of Technologies & Systems and Faculdade de Ciências e Tecnologia, Universidade Nova de Lisboa, Portuguese Navy.* Portugal, 2012.

42. Захист інформації в автоматизованих системах управління: навч. посіб. / укл. І. А. Пількевич, Н. М. Лобанчикова, К. В. Молодецька. Житомир: Вид-во ЖДУ ім. І. Франка, 2015. 226 с.

43. Логінова Н. І., Дробожур Р. Р. Правовий захист інформації: навч. посіб. Одеса: Фенікс, 2015. 264 с., іл.

44. Остапов С. Е. Євсеєв С. П., Король О. Г. Технологія захисту інформації: навч. посіб. Харків: Вид. ХНЕУ, 2013. 476 с.

45. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби: посібник / В. Л. Бурячок, С. В. Толюпа, В. В. Семко та ін. Київ: ДУТ-КНУ, 2016. 178 с.

46. Shang K., Hossen Z. Applying Fuzzy Logic to Risk Assessment and Decision Making. *Casualty Actuarial Society, Canadian Institute of Actuaries.* Society of Actuaries. November 2013.

47. Boc K., Vaculik J., Vidrikova D. Fuzzy approach to risk analysis and its advantages against the qualitative approach. *Proceedings of the 12th International Conference «Reliability and Statistics in Transportation and Communication»*. Transport and Telecommunication Institute, LV-1019, Riga, Latvia.

48. Pokoradi L. Fuzzy logic-based risk assessment. URL: http://www.zmka.hu/docs/Volume1/Issue1/pdf/04poko.pdf (дата звернення: 25.12.2013).

49. The Security Risk Management Guide. Microsoft Corporation, 2006. URL: http://www.microsoft.com/technet/security/topics/policiesandprocedures/secrisk/default (дата звернення: 09.01.2020).

50. Державний стандарт України Захист інформації. Технічний захист інформації. Основні положення. ДСТУ 3396.0-96. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=38883&cat_id=38836

51. Перелік засобів технічного захисту інформації, дозволених для забезпечення технічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом. URL: https://data.gov.ua/dataset/eab73672-181f-4b20-8819-56d47723ff11

52. Закон України Про криптографічний та технічний захист інформації URL: https://ips.ligazakon.net/document/NT1819

53. Курс лекцій з навчальної дисципліни «Кібербезпека банківських та комерційних структур». URL: http://www.dut.edu.ua/uploads/l_1718_48052949.pdf

54. Актуальні проблеми управління інформаційною безпекою держави X Всеукраїнська науково-практична конференція. URL: http://academy.ssu.gov.ua/upload/file/konf_04_04_2019.pdf

55. Правові засади інформаційної безпеки України: монографія / П. Д. Біленчук, Л. В. Борисова, І. М. Неклонський, В. О. Собина; за ред. П. Д. Біленчука. Харків: 2018. 289 с. URL: https://cutt.ly/5ugjj6s

56. Інформаційна безпека України. Наукові доповіді та тези учасників науково-технічної конференції 12–13 березня 2015 р. URL: https://cutt.ly/IugjQBZ

57. Лабораторний практикум з навчальної дисципліни «Інформаційна безпека»: навч.-практ. посіб. / С. В. Кавун, В. В. Носов, В. В. Огурцов, О. В. Манжай. Харків: Вид. ХНЕУ, 2008. 256 с.

58. Europol. Internet Organised Crime Threat Assessment 2018. URL: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018

59. Europol. Public Awareness and Prevention Guides. 2018. URL: https://www.europol.europa.eu/activities-services/public-awareness-and-preventionguides

60. Fisher T. Free and Public DNS Servers. *Lifewire.* 2018. URL: https://www.lifewire.com/free-and-public-dns-servers-2626062

61. Захист конфіденційну інформацію – персональних даних. URL: https://cutt.ly/iuggGRH

62. Закон України «Про інформацію». URL: https://zakon.rada.gov.ua/laws/show/2657-12

63. Закон України Про захист інформації в інформаційно-телекомуніка-ційних системах № 80/94-ВР від 05.07.1994 р. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80

64. Global Cybersecurity Index (GCI) 2018. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

65. Рибальченко Л. В., Косиченко О. О. Проблеми безпеки персональних даних в Україні. *Регіональна економіка.* Запоріжжя. 2019. С. 57–62.

66. Доктрина інформаційної безпеки України. URL: http://www.zakon3.rada.gov.ua/laws/show/514/2009

67. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи. URL: http://www.justinian.com.ua/article.php?id=3222

68. «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України». Рішення Ради національної безпеки і оборони України від 28 квітня 2014 р. URL: https://zakon.rada.gov.ua/laws/show/n0004525-14#Text

69. Про основи національної безпеки України: Закон України. Відомості Верховної Ради України. 2003. № 39. Ст. 351. Із змінами, внесеними згідно із Законом № 3200-IV (3200-15) від 15.12.2005. ВВР. 2006. № 14. Ст. 116.

70. Доктрини «Інформаційної безпеки України» від 25 лютого 2017 р. № 47/2017. URL: https://zakon3.rada.gov.ua/laws/show/47/2017?lang

Навчальне видання

Загоруйко *Любов Василівна*
Дудатьєв *Андрій Веніамінович*

КОНСПЕКТ ЛЕКЦІЙ
з дисципліни
«УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ»

Редактор О. А. Солдатова
Технічний редактор Т. О. Важеніна-Гопрак

Підписано до друку 19.12.2023.
Формат 60×84/16. Папір офсетний.
Друк – цифровий. Умовн. друк. арк. 16,27.
Тираж 30. Зам. 90.

Донецький національний університет імені Василя Стуса
21021, м. Вінниця, 600-річчя, 21
Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру
серія ДК № 5945 від 15.01.2018