МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТУСА

В. Г. Крижановський, Д. В. Чернов

СИСТЕМИ УПРАВЛІННЯ ДОСТУПОМ

Методичні вказівки до самостійної роботи
з дисципліни для здобувачів освіти ОС «Бакалавр»
спеціальності 125 Кібербезпека та захист інформації
Частина 1

Вінниця
2024

УДК 004.056.52:681.5(075.4)
С 409

Рекомендовано до друку вченою радою
факультету інформаційних і прикладних технологій
Донецького національного університету імені Василя Стуса
(протокол № 8 від 20 березня 2024 р.)

Укладачі:
Крижановський В. Г., професор кафедри прикладної математики та кібербезпеки Донецького національного університету імені Василя Стуса;
Чернов Д. В., доцент, старший викладач кафедри прикладної математики та кібербезпеки Донецького національного університету імені Василя Стуса.

Рецензент:
Штовба С. Д., д-р техн. наук, професор, професор кафедри інформаційних технологій Донецького національного університету імені Василя Стуса.

С 409 Системи управління доступом: методичні вказівки до самостійної роботи з дисципліни для здобувачів освіти ОС «Бакалавр» спеціальності 125 Кібербезпека та захист інформації. Частина 1 / уклад. В. Г. Крижановський, Д. В. Чернов. Вінниця: ДонНУ імені Василя Стуса, 2024. 16 с.

У методичних вказівках надано додаткові відомості для вивчення теми «Системи контролю й управління доступом» курсу «Системи управління доступом», які належать до питань фізичного доступу осіб до приміщень та деяких ресурсів. Вказівки рекомендовані для студентів закладів вищої освіти спеціальності 125 Кібербезпека та захист інформації і можуть бути корисними студентам споріднених спеціальностей.

УДК 004.056.52:681.5(075.4)

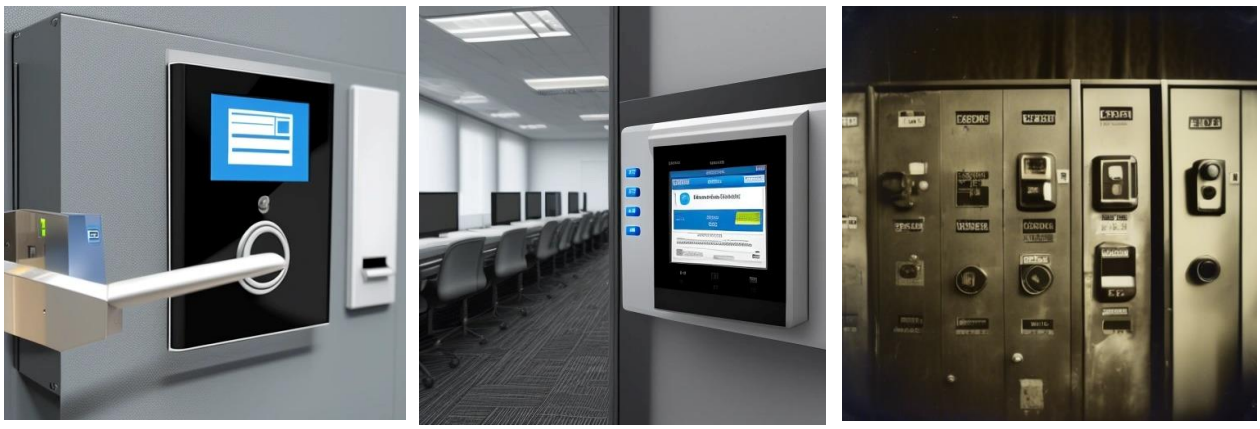
ЗМІСТ

ВСТУП

У сучасному світі вислів «Системи управління доступом» можна трактувати доволі широко:

- у сенсі «Системи контролю й керування доступом» (скорочено СКУД) – комплекс апаратних і програмних засобів для управління доступом, реєстрацію входів та виходів суб'єктів, обмеження входу / виходу (рис. 1);
- у сенсі контрольованого доступу до активів – процес автентифікації, авторизації та обліку, англійською AAA – Authentication, Authorization, Accounting;
- загальний випадок – це отримання доступу як людиною, так і машиною до ресурсів інформаційної системи, куди входить всесвітня павутина та інтернет речей.

У цих методичних вказівках розглянемо перше визначення, а саме СКУД.



https://aigallery.app/

https://earnwithhasan.com/tools/ai-image-generator/

Рисунок 1. Узагальнені графічні представлення про СКУД. Зображення згенеровано за допомогою ШІ. Наведено для загальних відомостей

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ СИСТЕМ КОНТРОЛЮ Й УПРАВЛІННЯ ДОСТУПОМ

Систему контролю й управління доступом використовує служба охорони підприємства чи організації для посилення охорони об'єкта й контролю допуску співробітників до службових та технічних приміщень об'єкта, а також управління евакуаційними дверима в разі аварійних ситуацій [1].

Вхід і вихід співробітників у дозволені зони доступності здійснюють за персоніфікованими електронними картками-перепустками в автоматичному режимі у дозволений час. Постійні (особисті) картки-перепустки виготовляють для співробітників і видають їм для особистого користування. Код, записаний на картку-перепустку, є незмінним особистим кодом співробітника, з використанням якого він має можливість проходити в дозволені зони доступу й виділені приміщення, і на підставі якого автоматично реєструють присутність.

Через втрату картки-перепустки системі забороняють її використання, і у разі спроби скористатися втраченою карткою повинен бути згенерований сигнал тривоги.

Усі приміщення, залежно від призначення й характеру здійснюваних у них операцій, поділяють на зони за доступністю.

Система контролю доступу об'єкта повинна забезпечувати:

– доступ у приміщення за електронною карткою-перепусткою;

– доступ у приміщення за електронною карткою-перепусткою й кодом, що набирають на клавіатурі зчитувача;

– вихід із приміщення з використанням картки-перепустки або кнопки виходу;

– звук сигналу тривоги у приміщенні охорони у випадку несанкціонованого проникнення в зони доступу (зламування, незакриття дверей, спроба підбирання коду);

– примусове розблокування (з обов'язковим розбиванням захисного скла або автоматичне з пульта оператора) у випадку пожежі або іншої екстреної ситуації дверей евакуаційних виходів, якщо їх оснащено засобами контролю доступу з реєстрацією цих фактів на сервері системи контролю й управління доступом;

– облік, реєстрування й документування фактів проходження співробітників у місцях установлення пристроїв системи контролю й управління доступом із зазначенням дати й часу проходження;

– створення й ведення бази даних на всіх співробітників зі введенням у неї паспортних та інших даних, кольорових фотографій, а також її оперативне коригування;

– доступ до бази даних та журналу подій, а також видавання довідок із них із виведенням на принтер і екран монітора оператора системи на вимогу користувача залежно від рівня доступу;

– замовник визначає рівні доступу до бази даних і журналу подій системи, а також може змінювати їх у процесі експлуатації системи;

– облік, реєстрування й документування дій оператора;

– резервування журналу подій і бази даних співробітників.

До складу системи контролю й управління доступом входить таке обладнання:

– робоче місце оператора системи контролю й управління доступом, обладнане комп'ютером із монітором і принтером;

– локальні контролери управління й збирання інформації;
– дистанційні або інші зчитувачі;
– кнопки ручного розблокування дверей під час виходу із приміщень;
– електромагнітні, електромеханічні замки;
– блоки живлення контролерів і замків;
– обладнання й програмне забезпечення для виготовлення карток-перепусток і ведення інформаційної бази даних;
– електронні ключі (картки).

За допомогою системи контролю доступу також досягаються:
– ідентифікація осіб, що мають право доступу;
– розмежування доступу до різних приміщень;
– керування автоматичними режимами;
– реєстрація часу перебування особи на об'єкті;
– обробка інформації та ведення статистики.

Впровадження СКУД дає змогу організувати безпеку та контроль об'єктів без залучення великої кількості працівників охорони та стабільну роботу автоматизованих систем у режимі 24/7 (наприклад, банкоматів, які встановлено в окремих приміщеннях відділень).

2. ОБЛАДНАННЯ ТА ПРИНЦИП РОБОТИ

Ключовий елемент, що встановлює право доступу особи на контрольну територію, – це **ідентифікатор** [2]. Цю функцію можуть виконувати:
– картка з магнітною смужкою;
– безконтактна картка;
– спеціальний брелок;
– цифровий код, що безпосередньо вводиться на клавіатурі;
– унікальні особисті ознаки людини: відбитки пальця / долоні, малюнок сітківки ока тощо.

Ідентифікатор є джерелом інформації, яка може бути в різній формі, і вона зчитується різними методами (контактний або безконтактний рідер, оптичне введення, біометрична інформація) і передається на контролер для подальшої обробки. До зчитувачів інформації зазвичай ставлять вимоги підвищеної стійкості до механічних та кліматичних впливів.

На основі отриманих даних саме контролер приймає рішення щодо надання чи заборони доступу. Залежно від типу системи, контролер може працювати автономно чи в поєднанні з іншими, під керуванням головного комп'ютера. Для гарантованої безперервної роботи контролер забезпечено блоком резервного живлення або власним акумулятором.

Отримана інформація зберігається в пам'яті системи для подальшого використання: складання звітів, статистики, обліку робочого часу.

Додаткове обладнання: конвертори, датчики, кнопки виходу, турнікети, електронні замки, механізми доведення дверей, геркони, сигнали тривоги тощо.

За потреби до системи контролю і управління доступом може бути встановлене спеціалізоване програмне забезпечення.

3. СФЕРА ВИКОРИСТАННЯ

Залежно від застосування розрізняють централізовані та автономні СКУД.

Централізовані системи, в яких контролери об'єднані в єдину мережу та підключені до комп'ютера, що здійснює загальне керування, входять до складу вже наявних систем: відеоспостереження, пожежної та охоронної сигналізації.

Їх встановлюють на великих офісних та промислових об'єктах з великою кількістю співробітників та відвідувачів. Система дає змогу одночасно керувати значною кількістю пунктів пропуску, оперативно вводити зміни до програми та додавати нові функції.

Автономні системи самостійно керують роботою периферійних елементів та контролюють точки доступу. Використовуються в адміністративних, суспільних та освітніх закладах, приватних будівлях тощо.

Автономні СКУД широко застосовують у банківській сфері для обмеження доступу до банкоматів, унеможливлюючи встановлення на них скімерів (спеціальних пристроїв для зчитування реквізитів із банківської картки клієнта). Також до СКУД інтегрують електронні системи антискімінгу, що дає змогу вчасно виявити несанкціоновані дії з банкоматом та запобігти намірам зловмисників, заблокувавши банкомат.

Безпосередньою перевагою автономних систем є помірна вартість та простота встановлення, легке керування і надійність в експлуатації.

Програмне забезпечення з мережевими функціями має більше значення для централізованих систем, оскільки автономні системи фактично побудовані на базі мікроконтролерів з відповідними спеціалізованими програмами.

Використання СКУД допомагає [3]:

– закрити несанкціонований доступ на територію, в будівлю, окремі поверхи і приміщення;

– відслідковувати часове переміщення співробітників і відвідувачів по об'єкту;

– вести табельний облік робочого часу кожного співробітника;

– здійснювати часовий і персональний контроль відкриття внутрішніх приміщень.

Зазвичай СКУД використовуються як один зі складників інтегрованої системи безпеки. Найбільш поширена інтеграція – з системою відеоспостереження і системою охоронної сигналізації.

Принцип дії СКУД простий: кожен співробітник отримує пластикову картку або інший пропуск, що містить індивідуальний код. Біля входу на підприємство або в інше приміщення, що підлягає контролю, встановлюються зчитувачі – спеціальні пристрої, що зчитують з пропусків код і передають його в систему. Кожен код містить відповідну інформацію про права власника пропуску. На основі зіставлення цієї інформації та ситуації, за якої був пред'явлений пропуск, система приймає одне з таких рішень: відкриває прохід, переводить приміщення в режим охорони або вмикає сигнал тривоги. СКУД запам'ятовує всі факти пред'явлення пропусків і пов'язані з ними дії. Ця інформація надалі використовується системою для складання різноманітних звітів.

Залежно від застосовуваної СКУД на об’єкті, окремі її пристрої можуть бути об’єднані в єдиний блок (контролер зі зчитувачем) або взагалі бути відсутніми (персональний комп’ютер).

Зчитувачі СКУД є програмно-апаратними засобами системи та призначені для зчитування коду з брелків, міток, магнітних і безконтактних карт.

Приклад системи СКУД представлено на рис. 2.

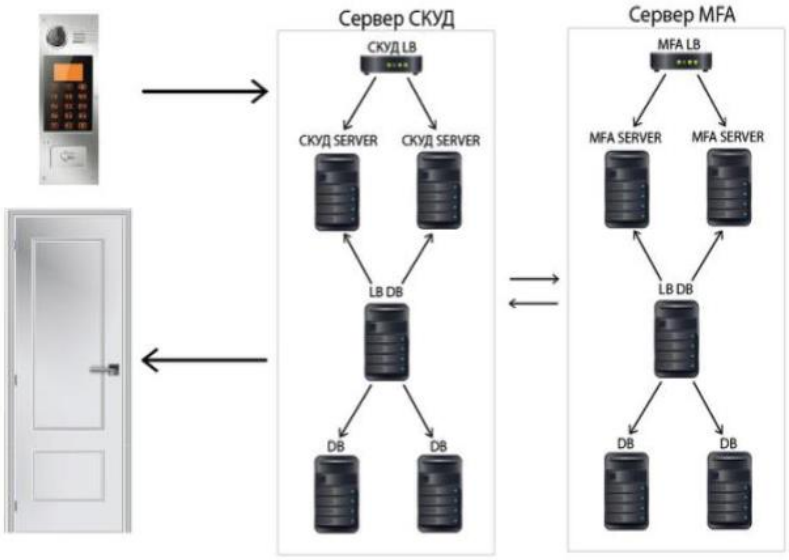


Рисунок 2. Схема побудови СКУД

У процесі автентифікації можуть брати участь три фактори:

– щось, що ми знаємо – пароль;
– щось, що ми маємо – пристрій автентифікації;
– щось, що є частиною нас – біометрика.

Пароль – це секретна інформація, якою повинен володіти тільки авторизований суб’єкт. Паролем може бути мовне слово, текстове слово, комбінація для замка або персональний ідентифікаційний номер (PIN). Сьогодні розроблено кілька методів реалізації систем автентифікації із застосуванням одноразових паролів.

1. Метод «запит / відповідь». На початку процедури автентифікації користувач відправляє на сервер свій логін. У відповідь на це останній генерує випадкову послідовність символів і відправляє її назад. Користувач за допомогою свого ключа зашифровує ці дані і відправляє їх серверу. Сервер у цей час за допомогою секретного ключа, що належить користувачу, кодує вихідну послідовність. Далі проводиться порівняння обох результатів шифрування. Уразі їх повного збігу вважається, що автентифікація пройшла успішно.

2. Метод «тільки відповідь». Програмне або апаратне забезпечення користувача самостійно генерує вихідні дані, які будуть зашифровані та відправлені на сервер для порівняння. Водночас у процесі створення даних використовується значення попереднього запиту. Сервер теж володіє такими даними. Тобто він, використовуючи ім’я користувача, знаходить значення його попереднього запиту та генерує встановленим алгоритмом ідентичний рядок.

3. Метод «синхронізація за часом». У ньому в якості початкових даних виступають поточні показники годинника спеціального пристрою або комп'ютера, на якому працює людина. Ці дані зашифровуються за допомогою таємного ключа, що у відкритому вигляді відправляються на сервер разом з ім'ям користувача. Під час отримання запиту сервер фіксує поточний час від свого таймера, зашифровує його та порівнює два значення.

4. Метод «синхронізація за подією». Цей метод майже ідентичний попередній технології. Тільки в якості ключа в ньому використовується не час, а кількість успішних процедур автентифікації, проведених до цієї процедури. Це значення підраховується двома сторонами окремо одна від одної.

У деяких системах реалізуються змішані методи, де в якості початкового значення використовується два або навіть більше типів інформації.

Технологія одноразових паролів вважається досить надійною. Але вони також мають недоліки, що діляться на дві групи. До першої належать потенційно небезпечні вузькі місця, притаманні всім методам реалізації. Найбільш серйозною з них є можливість підміни сервера автентифікації. Під час цього користувач буде відправляти свої дані прямо зловмиснику. Інша вразливість властива тільки синхронним методам реалізації одноразових паролів, оскільки існує ризик розсинхронізації інформації на сервері і в програмному або апаратному забезпеченні користувача. Усе це робить парольний механізм слабо захищеним.

Пристрій автентифікації. Тут важливий факт володіння суб'єктом – унікальним предметом. Це може бути особиста печатка, ключ від замка; для комп'ютера це файл даних, що містять характеристику.

Автентифікаційні пристрої поділяють на дві категорії: пасивні та активні. В обох випадках пристрої несуть у собі базовий секрет, і для того, щоб виготовити копію пристрою, необхідно мати копію базового секрету. Пасивні автентифікаційні пристрої зберігають базовий секрет, наприклад, ключі від механічних замків, карточки банкомата, більшість типів електронних перепусток тощо. Проблемою таких пристроїв є те, що дані, які в них записані, можуть бути легко відтворені за допомогою копії. Активні автентифікаційні пристрої можуть у різних обставинах генерувати різні вихідні дані. Наприклад, пристрій може бути задіяний у протоколі автентифікації за методом запитання / відповідь або забезпечувати іншу функцію шифрування, в якій використовується базовий секрет цього пристрою. Значною перевагою активних пристроїв є те, що вони не передають свого базового секрету, а використовують його. Дізнатись секрет у такому випадку теоретично можливо, але практично досить малоймовірно.

Автентифікація із застосуванням активних автентифікаційних пристроїв передбачає генерацію різних типів повідомлень під час кожної спроби власника автентифікувати себе, це значить, що для зловмисника немає сенсу перехоплювати згенеровану послідовність і відтворювати попередній набір повідомлень.

Біометрика. Характеристикою є фізична особливість суб'єкта. До групи фізіологічних показників належать такі джерела біометричних даних:

1) відбитки пальців – технологія перейнята від систем, які використовувалися правоохоронними органами для зіставлення відбитків;

2) геометрія руки – зчитувальні пристрої сприймають розмір пальців користувача, товщину та геометрію руки;

3) характеристики ока: сітківка – в таких системах використовується ретинальна камера, розміщена позаду спеціального окуляра; користувач розміщує око напроти окуляра і камера записує картину кровоносних судин сітківки ока людини; райдужна оболонка – в цих системах використовується спеціальна камера, яка досліджує райдужну оболонку ока і фіксує її характерний образ;

4) обличчя – камера сканує обличчя і порівнює зображення із зображенням, що зберігається в записі користувача.

На відміну від фізіологічних показників, поведінкові не завжди мають вимірювати одне і те ж саме: людині може бути запропоновано сказати, написати чи пройтись у певний спосіб, аби зменшити ризик відтворення. До поведінкових показників належать такі:

1) голос – система просить користувача сказати кілька слів, на їх основі будується кілька голосових шаблонів. Такий підхід має низку недоліків: велика ймовірність помилок у шумному середовищі, легко обманути записом голосу користувача;

2) підпис – система порівнює представлений підпис з оригіналом. Для зниження ризику підробки надійні системи також вимірюють динаміку руху руки, силу натиску, нахил пера;

3) динаміка роботи на клавіатурі – системи відстежують поведінку користувача під час роботи на клавіатурі, а потім використовують унікальні особливості цієї поведінки для автентифікації.

Основною проблемою підходів у біометричній автентифікації є зіставлення біометричних показників. Якщо біометричні показники змінились чи були пошкоджені, представлені незвичним способом, то зіставлення може бути невдалим, що веде до відмови автентифікації законному користувачу. З'являється ризик помилкового прийняття однієї людини за іншу. Іншою проблемою є загроза атак відтворення. Атакуючий може отримати біометричні показники жертви або за допомогою зовнішнього записуючого пристрою, або шляхом копіювання показників у двійковому коді. Опис схеми взаємодії користувача та СКУД зчитувача з позитивним результатом представлено на рис. 3.

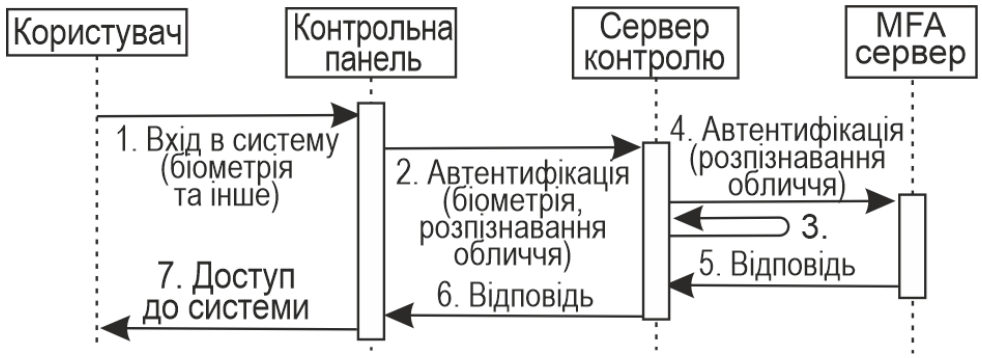


Рисунок 3. Принцип взаємодії користувача та СКУД зчитувача: З – біометрія (не використана або невдала спроба)

На рис. 3 користувач входить у систему, використовуючи біометрію і токен. Access Control-панель відправляє дані біометрії і токена на Access Control-сервер. Виконується автентифікація біометрії на Access Control-сервері. Access Control-сервер автентифікує токен на MFA-сервері (MFA – Мультифакторна ідентифікація Azure). MFA-сервер відправляє відповідь Access Control-серверу. Access Control-сервер відправляє відповідь Access Control-панелі. Access Control-панель дає доступ до системи.

4. ДВОФАКТОРНА АВТЕНТИФІКАЦІЯ В СИСТЕМАХ КОНТРОЛЮ І УПРАВЛІННЯ ДОСТУПОМ

Одним із найважливіших завдань інформаційної безпеки для будь-якої організації є управління та керування доступом до інформаційних систем і ресурсів. Адже правильно побудована та впроваджена система керування й управління доступом (СКУД) може значно знизити ризики несанкціонованих дій, можливості витоку інформації, ризики отримання користувачами неправомірного доступу та прав до інформаційних ресурсів тощо [5].

Отже, основним завданням систем управління доступом до інформаційних ресурсів є запобігання несанкціонованому доступу до конфіденційної інформації або дії з інформацією, що порушують встановлені правила доступу до інформаційних систем.

Установка системи контролю та управління доступом є однією з найбільш важливих і необхідних систем у структурі будь-якого підприємства. Система контролю і управління доступом до інформаційних систем та ресурсів повинна надавати користувачам лише необхідний доступ, а процес управління доступом повинен бути керованим та контрольованим. Сучасні технічні засоби СКУД дають змогу вирішувати низку важливих проблем, як-от:

– протидія промисловому шпигунству;
– протидія крадіжкам;
– захист конфіденційної інформації;
– моніторинг дій користувачів та співробітників організації;
– керування та розмежування доступом.

Додаткові завдання СКУД – це ідентифікація осіб. Система контролю і управління доступом складається з цілої низки компонентів, починаючи з тих, які ідентифікують співробітника, і закінчуючи тими, що приймають рішення про надання доступу.

У більшості випадків для забезпечення безпечного доступу одного фактора автентифікації недостатньо. Відомо, що будь-які способи ідентифікації та автентифікації мають свої недоліки. Тому побудувати захищену на 100 % систему неможливо. Однак, використовуючи переваги факторів автентифікації в комплексі, можна звести ризики до мінімуму.

Наприклад, розпізнавання обличчя у СКУД має один істотний недолік – можливість підміни зловмисником зображення реальної людини його портретом, тобто

спроба видати портрет за реальну людину, що призведе до проникнення зловмисника на об'єкт інформаційної діяльності. Підвищити ефективність СКУД у цьому випадку можна за допомогою багатофакторної ідентифікації. Наприклад, двофакторна ідентифікація припускає використання кодової клавіатури і Prox-карти. Принципово завдання захисту від несанкціонованого доступу така ідентифікація не вирішує, проте ускладнює роботу порушників, адже їм у цьому випадку необхідно вкрасти або зімітувати карту і дізнатися код (пароль) доступу.

Для підвищення надійності та точності роботи системи ідентифікації та автентифікації користувачів пропонується об'єднувати біометричні характеристики із класичним способом автентифікації, а саме графічним паролем. Використання графічних паролів є більш зручними та більш практичними для користувачів, за допомогою цього підвищується рівень безпеки та доступу до інформаційних систем [6].

5. ЧОТИРИ ТРЕНДИ КОНТРОЛЮ ДОСТУПУ З 2023 РОКУ

Перехід на мобільні пристрої. Пандемія змінила сприйняття та практику контролю доступу. Ще до появи коронавірусу за даними опитування, проведеного компанією HID у 2019 р., 54 % підприємств оновили або планували перехід на систему управління мобільним доступом у найближчі три роки. Є підстави вважати, що це число буде рости у зв'язку з проблемами зі здоров'ям, безпекою та санітарією, які висунув на перший план коронавірус [7].

За даними Security Journal Americas (стаття від 17.01.2024), очікується, що до 2028 р. ринок облікових даних для контролю мобільного доступу сягне понад 750 млн доларів США, порівняно з доходом у 2022 р., який становив лише 295 млн доларів США – сукупний річний темп зростання (CAGR) становить приблизно 17 %.

Зростання кількості мобільних облікових даних не дивне. Майже половина населення світу володіє смартфонами, їх число вагомо збільшується у промислово розвинених країнах. Приблизно 84 % дорослих у Великій Британії володіють смартфонами та носять їх із собою всюди. Інакші справи з картками доступу та іншими стандартними елементами, які мають одноразове застосування та часто забуваються або губляться, що є вагомою витратою для роботодавця.

Багатофакторна та мультимодальна автентифікація. Мобільні облікові дані дають змогу використовувати як мультимодальну, так і багатофакторну аутентифікацію. Мультимодальний означає підтвердження особи або отримання доступу з використанням як мінімум двох окремих біометричних даних, або ж дозвіл доступу за допомогою будь-якого з різних облікових даних, як-от ключі доступу або PIN-код. Багатофакторна автентифікація включає в себе підтвердження особи або отримання доступу як мінімум за допомогою двох методів або облікових даних.

Багатофакторна автентифікація широко використовується в цифровому доступі. Наприклад, коли співробітник входить у систему безпеки компанії, він повинен використовувати додатковий метод для перевірки особистості за допомогою одноразового токена через SMS або іншу програму.

Хоча двофакторна автентифікація обов'язкова в регульованих галузях, вона також з'являється в нерегульованих вертикалях. Розвиток мультимодальних зчитувачів буде і далі підживлювати цю тенденцію.

Біометрія. Протягом десятиліть прихильники біометрії передбачали, що ми стоїмо на порозі біометричної революції. Це, як і раніше, не так, але стартапів предостатньо, технології все ширше впроваджуються, ціни знижуються, а опір біометрії послабшав. За прогнозами Future Market Insights, «безконтактні біометричні технології будуть ловити хвилю, створену пандемією COVID-19, до річного темпу зростання в 17,4 % з 2020 до 2030 р.». Згідно з цим аналізом, технологія розпізнавання обличчя захопить вагому частину ринку біометрії, оскільки організації застосовують її для перевірки особистості та контролю доступу. Але інші технології також принесуть користь, зокрема безконтактні біометричні зчитувачі для ідентифікації за відбитками пальців, райдужною оболонкою, долоні та голосу.

Хоча інша аналітична компанія – ABI Systems – передбачає, що ринок біометрії загалом буде менш стійким, експерти все ж прогнозують вагоме зростання двох технологій: розпізнавання облич та зіставлення райдужної оболонки ока.

Модель на основі хмари / підписки. Раніше організації були пов'язані обмеженнями пропрієтарних систем безпеки на базі приміщення. Управління, інтеграція, оновлення програмного забезпечення та обслуговування виснажили цінні ресурси.

Світ хмарних обчислень, SaaS (контроль доступу як послуга) та модель на основі передплати перевернули старі способи стандартних систем. Традиційно організації купували обладнання, як-от зчитувачі, контролери, картки доступу та радіобрелки, а потім підключали СКУД до локального сервера. Встановлення, тестування та обслуговування проводилися вручну. У системах на основі передплати обладнання – зчитувачі та панелі – залишається на місці, а сервери, програмне забезпечення та дані розташовані в центрі обробки даних постачальника. Це централізований спосіб управління СКУД, цілодобова підтримка та переваги великого постачальника рішень, що містять:

– мінімальні витрати на запуск;
– масштабованість;
– миттєві оновлення;
– мінімальний час простою;
– підвищену безпеку;
– інтегроване управління декількома об'єктами;
– негайне додавання, видалення або зміну прав доступу;
– часте резервне копіювання даних;
– постійне поліпшення та розвиток продукту.

Університети та інші заклади вищої освіти були в авангарді запровадження облікових даних для мобільних пристроїв, реагуючи на вимоги молодих користувачів, які ставили на перше місце мобільні пристрої і безліч переваг, які вони пропонують. Це не тільки підвищує безпеку, але й оптимізує роботу.

Студенти цінують зручність використання своїх смартфонів для доступу, що знижує ризик і вартість їх втрати або втрати карток фізичного доступу, а адміністратори економлять час і гроші на видачі та управлінні обліковими даними.

Той факт, що багато студентів готові обміняти певний рівень конфіденційності на більшу зручність, також сприяв прийняттю цих облікових даних.

У міру того, як ці облікові дані використовуються все більше, наприклад, для оплати їжі через програму чи гаманець, які надають доступ, установи збирають все більше персональних даних.

Ця велика кількість інформації з різних джерел дає змогу більше персоналізувати досвід студентів, задовольняючи унікальні потреби та графіки.

Це може бути так само просто, як відкритий доступ до будівлі вдень, але обмежений доступ для певних користувачів у неробочий час або навіть використання інструменту підрахунку зайнятої площі, щоб охорона могла приймати зважені рішення щодо місця патрулювання, якщо студенти навчаються пізно вночі.

Збільшення обсягу даних також несе велику відповідальність, тому вкрай важливо, щоб університети вживали належних заходів кібербезпеки для захисту від потенційних ризиків для даних.

Однак це також спрощує інтеграцію мобільних облікових даних у наявні системи, щоб забезпечити безперебійний контроль доступу.

ВИСНОВКИ

Системи контролю й управління доступом (СКУД) визнані одним з обов'язкових компонентів комплексної безпеки для об'єктів та інформаційно-комунікаційних систем. І незважаючи на сторіччя їх розвитку, у сучасних реаліях продовжується їх розвиток на основі нових технологій. Фахівцям з кібербезпеки та захисту інформації потрібно мати повні знання про ці системи та їх зв'язок з іншими напрямами діяльності у галузі кібербезпеки.

СПИСОК КОНТРОЛЬНИХ ЗАПИТАНЬ

1. Охарактеризуйте завдання фізичного захисту на підприємстві.
2. Архітектура і технології сучасних систем контролю доступу.
3. Захист на основі одноразових паролів.
4. Система контролю доступу на основі аналізу біометрії обличчя.
5. Апаратні та програмні засоби біометрії.
6. Якими основними властивостями повинна володіти система контролю та управління доступу?
7. Чим відрізняються автономні та централізовані СКУД?
8. Що таке пристрої автентифікації?
9. Що таке контроль доступу як сервіс?
10. Що таке двофакторна автентифікація?

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Інформаційна безпека: навч. посіб. / за заг. ред. Ю. Я. Бобала, І. В. Горбатого; Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв, та ін. Львів: Видавництво Львівської політехніки, 2019. 580 с.

2. Сайт компанії ZKTeco. Biometric & Computer Vision. URL: www.zkteco.com

3. Резанов Б. М., Бульба С. С., Шокотько Д. В. Фактори автентифікації системи контролю та управління доступом. *Системи управління, навігації та зв'язку*. 2017. Вип. 3(43). С. 63–65.

4. Методичні вказівки до виконання лабораторних та самостійних робіт з дисципліни «Комплексні системи контролю та управління доступом» для здобувачів вищої освіти галузі знань 12 «Інформаційні технології» / уклад. С. В. Кухаренко. Одеса: НУ «ОЮА», 2020. 32 с.

5. Бондаренко О. В., Карпінець В. В. Двофакторна автентифікація в системах контролю і управління доступом. Тези доповідей Всеукраїнської науково-практичної Інтернет-конференції студентів, аспірантів та молодих науковців *Молодь в науці: дослідження, проблеми, перспективи* (МН-2020) (м. Вінниця, 18–29 травня 2020 р.). 2020. URL: https://conferences.vntu.edu.ua/index.php/mn/mn2020/paper/view/10276

6. Authentication using graphical passwords: Basic results / S. Wiedenbeck, J. Waters, J. C. Birgit, A. Brodsky. 2016. URL: http://www.jimwaters.info/pubs/Graphical-Password-Basic-Results-2005.pdf

7. Чотири тренди контролю доступу на 2021 р. URL: https://worldvision.com.ua/chetyre-trenda-kontrolya-dostupa-na-2021-god/

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

Навчальне видання

Крижановський Володимир Григорович
Чернов Дмитро Вікторович

СИСТЕМИ УПРАВЛІННЯ ДОСТУПОМ

Методичні вказівки до самостійної роботи
з дисципліни для здобувачів освіти ОС «Бакалавр»
спеціальності 125 Кібербезпека та захист інформації
Частина 1

Редактор О. А. Солдатова
Технічний редактор Т. О. Важеніна-Гопрак

Підписано до друку 21.11.2024
Формат 60×84/16. Папір офсетний.
Друк – цифровий. Умовн. друк. арк. 0,93.
Тираж 30. Зам. 29.

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