– №127. – С. 33–37. . – Режим доступу до ресурсу: https://eprints.kname.edu.ua/43274/1/4756-9455-1-SM.pdf

3. Передерій Т. Система FRAUD-моніторингу в запобіганні та виявленні шахрайств з платіжними картками / Т. Передерій, О. Маковоз // Актуальні питання протидії кіберзлочинності та торгівлі людьми / Т. ПЕРЕДЕРІЙ, О. МАКОВОЗ. – Харків, 2018. – С. 310–314. . – Режим доступу до ресурсу: https://univd.edu.ua/general/publishing/konf/23_11_2018/pdf/92.pdf

Устенко С.В.
д.е.н., професор
Солодкий А.В.
магістр
Київський національний економічний університет імені Вадима Гетьмана,
stasustenko@ukr.ne, andsol92@gmail.com

СИСТЕМА КОНТРОЛЮ ТА УПРАВЛІННЯ БЕЗПЕКОЮ ОФІСУ

Сучасний офіс являє собою приміщення, яке призначене для роботи певної кількості людей з урахуванням складного технологічного середовища. Ніхто в офісі не застрахований від випадків займання, проникнення сторонніх осіб тощо. Відбувається багато процесів, які можуть залишитися непоміченими й завдати великої шкоди. Все це вимагає застосування ефективних та інноваційних підходів для забезпечення та контролю безпеки як офісного персоналу, так і офісу загалом, для чого і призначені системи контролю та управління безпекою офісу.

Система контролю та управління безпекою офісу (СКУБО) є програмно-апаратним комплексом, в якому об'єднуються різні види систем, технології, заходи для забезпечення безпеки персоналу, обладнання та інформації в офісному приміщенні. Модульна структура систем такого типу дає змогу інтегрувати її в офіси різних розмірів, використовуючи різні підсистеми, що визначають ключові аспекти безпеки офісу. Серед них є основні:

- система контролю і управління доступом (СКУД);
- системи охоронної сигналізації;
- система відеоспостереження;
- системи протипожежного захисту.

СКУД є однією з основних складових СКУБО. Вона забезпечує безпеку території чи об’єкта, обмежуючи доступ до різних зон або до всього об'єкта у цілому. Основне завдання СКУД – контролювати доступ до певних приміщень. Основними пристроями слугують ідентифікатори, зчитувачі, контролери, турнікети, електромеханічні, електромагнітні замки, засувки, шлагбауми.

За архітектурою, СКУД поділяється на автономну й мережеву. Автономний тип архітектури характеризується використанням одного або декількох незалежних контролерів. Обмін даними між компонентами відбувається через інтерфейси RS-485 та RS-232. При цьому налаштування кожного контролера здійснюється окремо.

Мережева архітектура характеризується використанням центрального контролера – сервер управління з програмним забезпеченням, з яким з’єднані всі локальні контролери та з якими відбувається обмін інформацією. Для забезпечення інформаційного зв'язку контролерів використовуються інтерфейси RS-485, RS-232 та Ethernet.

Охоронна сигналізація – це сукупність спільно діючих технічних засобів для виявлення проникнення та подібних протиправних дій на об'єкті, що охороняється. Вона забезпечує збір, обробку, передачу та подання, у заданому вигляді, службової інформації.

Головне завдання такого обладнання – швидке оповіщення про виникнення надзвичайної події, використовуючи інтерфейси Ethernet, GSM, 2G, 3G, 4G, LTE.

Сама система складається з охоронної централі, охоронних датчиків сигналізації, сирени, радіобрелків або клавіатури сигналізації, інших приладів.

В залежності від типу підключення, система буває бездротовою та дротовою. В дротових охоронних системах використовуються інтерфейси RS-485/-232. Такі системи вважаються більш надійним й мають набагато менше помилкових спрацьовувань, які можуть бути пов'язані з розрядкою батарейки в датчику. В бездротових системах всі компоненти з'єднуються по спеціальному радіоканалу. В якості живлення датчиків використовуються батарейки та акумулятори, які, через деякий час, потребують заміни.

За принципом роботи охоронної сигналізації та формування тривожного повідомлення можна виділити наступні її види: автономну, GSM та пультову.

Автономний комплекс реагує на виникнення позаштатної події спрацьовуванням сирени і включенням світлового сигналу. Більше тривожні повідомлення нікуди не йдуть.

GSM-сигналізація включає стандартний автономний комплект приладів, але ще доповнюється опцією автодозвону або надсилає СМС-повідомлення по мобільній мережі на вказані номери. Пультовий комплекс інформує оператора охоронного персоналу про виникнення позаштатної ситуації. Характеризується високою надійністю та ефективністю за рахунок використання різних каналів зв'язку (радіо, GSM, телефонних ліній, Ethernet).

Система відеоспостереження – це програмно-апаратний комплекс, призначений для організації відеоконтролю як на локальних, так і на територіально-розподілених об'єктах.

Її основне призначення - це візуальне спостереження, запис (відеореєстрація) подій на ділянках, об'єктах. Система відеоспостереження дозволяє здійснювати безперервний контроль, фіксувати обстановку у зоні спостереження й переглядати записи відеокамер.

Система відеоспостереження складається з відеокамери, відеореєстратора, монітора, накопичувача, додаткових засобів, засобів монтування та з'єднаня компонентів системи.

Залежно від принципу передачі відеосигналу, система відеоспостереження поділяється на аналогове та мережеве відеоспостереження.

Камери аналогового відеоспостереження підключаються до відеореєстратора за допомогою коаксіального кабелю. Такі відеокамери мають високоякісні цифрові матриці, а отримане зображення перетворюється аналого-цифровим перетворювачем для передачі сигналу по аналогових лініях.

Мережеве відеоспостереження складається з IP-камер, які самостійно можуть підключатися до глобальної або локальної мережі. Відеосигнал передається цифровими пакетами за допомогою інтернет протоколів на сервери. IP-обладнання оснащується різними смарт-функціями.

Системи протипожежного захисту – це комплекс технічних засобів, встановлений на об'єкті, який призначений для виявлення, локалізації та ліквідації пожежі, захисту людей, матеріальних цінностей від впливу небезпечних факторів пожежі. До його складу відноситься засоби пожежної сигналізація та пожежогасіння.

Залежно від методу визначення місця займання, система поділяється на аналогову, адресну та змішаного типу. Аналогові ідентифікують місце пожежі за номером пожежного шлейфу.

Адресна сигналізація конкретно визначає та вказує місце виникнення пожежі.

Змішаний тип адресно-аналогової пожежної сигналізації застосовується для модернізації вже існуючої системи.

Всі ці підсистеми об'єднуються в одну за допомогою багатьох компонентів, таких як сервер, програмне забезпечення, центри керування підсистемами. Програмне забезпечення

даної системи дає змогу зручно відстежувати та керувати безпекою офісу. Подібні системи широко використовуються в офісних, промислових приміщеннях.

Список використаних джерел

1. Litvinchuk I. Спосіб оцінювання інтегрованих систем безпеки на об'єкті інформаційної діяльності [Електронний ресурс] / I. Litvinchuk, N. Korshun, M. Vorokhob // Електронне наукове видання «Кібербезпека: освіта, наука, техніка», 2(10), 135–143. – 2020. – Режим доступу до ресурсу: https://doi.org/10.28925/2663-4023.2020.10.135143.
2. Роговий М. І. Дослідження особливостей використання охоронних СКУД [Електронний ресурс] / Роговий М. І. – 2019. – Режим доступу до ресурсу: http://openarchive.nure.ua/handle/document/10963.

Науковий керівник: Устенко С.В., д.е.н., професор.

Фетісов О. О.
аспірант
Приватний вищий навчальний заклад
«Європейський університет»
ofetisov@e-u.edu.ua

ПРАКТИЧНЕ ЗАСТОСУВАННЯ БЛОКЧЕЙН-ТЕХНОЛОГІЙ В УПРАВЛІННІ БЕЗПЕКОЮ ПІДПРИЄМСТВА

Блокчейн - це надзвичайно інноваційна концепція, що створює фундаментальні зміни у світі технологій та фінансів. Він уособлює собою зростаючий список записів, відомих як блоки, які взаємодіють між собою з використанням криптографічних методів. Кожен блок утримує в собі не лише дані про проведені транзакції та час їх виконання, а й зв'язок з попереднім блоком у послідовності, завдяки надійному криптографічному хешу.

Описаний як "цифрова розподілена книга для транзакцій", блокчейн відзначається своєю бездоганною властивістю незмінності даних. Інформація, що занесена в цей механізм, недоступна для будь-яких модифікацій, забезпечуючи надійну і безпекову збереженість даних. Зберігаючи відкритий та розподілений характер, блокчейн дозволяє ефективно реєструвати операції між різними сторонами у надійний, довірчий та стійкий спосіб. [1, с. 12]

Згідно [2] виділимо ключові галузі застосування блокчейн-технологій для управління безпекою підприємства.

Payments. Платежі, здійснені через блокчейн, легко перевірити, оскільки в системі в будь-який момент є запис необхідної інформації. Блокчейн-транзакції також ефективні проти хакерів або будь-яких спроб фальсифікувати певний запис, оскільки зміни видно по всій мережі. Якщо дані в одному блоці будуть підроблені, це буде легко виявлено в усіх блоках. Перехресна перевірка інформації також сприятиме швидкому виявленню зловживань.. Блокчейн забезпечує відстеження всіх транзакцій і відстеження активів.

Smart contracts. Смарт-контракти також працюють так само, як і платежі та перекази, оскільки вони усувають потребу в веденні документації вручну. Розробка цифрових процесів для скорочення ручної передачі та зберігання документів підвищує безпеку та захищає, а також економить час і кошти, необхідні для створення ручних контрактів.