3. Барало О.В., Самойленко П.Г., Гранат С.Є., Ковальов В.О. Автоматизація технологічних процесів і системи автоматичного керування: Навч. посібник. Київ: Аграрна освіта, 2010. 557 с.

4. Невлюдов І.Ш., Новоселов С.П., Сичова О.В. Технологія програмування промислових контролерів в інтегрованому середовищі CODESYS: Навч. посібник. Харків: ХНУРЕ, 2019 . 264 с.

5. ОВЕН. Обладнання для автоматизації [Електронний ресурс]. URL: https://owen.ua/

ОСНОВНІ МЕТОДИ КІБЕРБЕЗПЕКИ У ЦИФРОВУ ЕПОХУ: СУЧАСНІ СТРАТЕГІЇ ЗАХИСТУ

Жорняк А.С., здоб. ВО
Науковий керівник – **Петрова Р.В.,** канд. техн. наук, доц.
Харківський національний університет радіоелектроніки

Цифрова епоха докорінно змінює сучасний світ, розширюючи можливості для обміну інформацією та взаємодії. Проте з розвитком технологій зростають і ризики кібератак, які ставлять під загрозу конфіденційність, цілісність і доступність даних. Забезпечення кібербезпеки вимагає комплексного підходу, що включає технічні, адміністративні та організаційні заходи захисту інформації.

Аутентифікація користувачів та управління доступом - ключові елементи будь-якої стратегії кібербезпеки. Одним із найбільш надійних методів аутентифікації є багатофакторна аутентифікація (MFA), яка вимагає підтвердження особистості користувача за допомогою кількох різних факторів, таких як пароль, одноразовий код, біометричні дані або токен. Також популярність здобувають системи управління доступом, що обмежують права користувачів, запобігаючи доступу до ресурсів без відповідного рівня повноважень.

Шифрування є основним методом захисту конфіденційності даних як при їхньому зберіганні, так і під час передачі. Існують різні види шифрування: симетричне, що використовує один ключ для шифрування і дешифрування, та асиметричне, де для кожної операції використовуються окремі ключі. Це дозволяє забезпечити захист інформації від несанкціонованого доступу навіть у разі перехоплення даних під час їхньої передачі в мережі.

Сучасні системи кібербезпеки повинні бути здатні виявляти загрози в режимі реального часу. Системи виявлення вторгнень (IDS) та аналітики безпеки (SIEM) автоматично обробляють великий обсяг інформації та сигналізують про підозрілі дії, що допомагає швидко реагувати на загрози та зменшувати можливу шкоду. Це значно скорочує час виявлення та реагування на інциденти, що є критично важливим для забезпечення безпеки великих інформаційних систем.

Серед поширених кіберзагроз особливо виділяються віруси, трояни, шкідливі додатки та програми-вимагачі. Антивірусне програмне забезпечення та інші рішення для боротьби з шкідливим ПЗ допомагають у ранньому виявленні та видаленні зловмисних компонентів. Згідно з дослідженням, оновлене програмне забезпечення та регулярні сканування знижують ризик зараження системи та крадіжки даних на 60%.

Безпека інформації залежить не лише від технологій, а й від людського фактора. Навчання користувачів, їхнє ознайомлення з основами кібербезпеки, такими як розпізнавання фішингових повідомлень та уникнення небезпечних сайтів, допомагає значно знизити ризики. Дослідження показують, що понад 70% інцидентів кібербезпеки пов’язані з людськими помилками, що підкреслює важливість підвищення рівня обізнаності серед користувачів.

Сегментація мережі – це розподіл мережевих ресурсів на окремі сегменти для обмеження поширення загроз у разі злому однієї з частин мережі. Брандмауери контролюють потік даних та блокують несанкціоновані з'єднання, зменшуючи ймовірність зовнішніх атак. Такий підхід значно підвищує рівень безпеки, оскільки дозволяє обмежити зону ураження навіть у разі успішної атаки.

З огляду на те, що все більше компаній використовують хмарні сервіси, особливо актуальним стає захист хмарних інфраструктур. Включення шифрування даних, обмеження доступу до хмарного середовища, контроль на рівні віртуальних серверів та регулярний аудит безпеки є основними складовими захисту інформації в хмарних сервісах. Компанії також активно використовують стратегії «Zero Trust» для підвищення захищеності своїх хмарних середовищ.

Комплексний підхід до кібербезпеки вимагає інтеграції різних методів захисту для запобігання можливим загрозам. Забезпечення безпеки даних у цифрову епоху є ключовим завданням, що вимагає як сучасних технологій, так і високого рівня обізнаності користувачів. Стратегія кібербезпеки повинна постійно адаптуватися до нових викликів та загроз, що виникають у швидкозмінному цифровому середовищі.

Крім цього, важливо також впроваджувати регулярні аудити безпеки, які дозволяють виявити уразливі місця в системі та вжити необхідних заходів для їх усунення. Використання сучасних технологій, таких як штучний інтелект та машинне навчання, може суттєво підвищити ефективність виявлення і реагування на загрози, надаючи можливість прогнозувати потенційні атаки на основі аналізу даних.

У підсумку, ефективна кібербезпека в умовах цифрової епохи вимагає всебічного і системного підходу. Інтеграція технологій, таких як багатофакторна аутентифікація, шифрування, системи виявлення вторгнень та аналітики безпеки, разом із стратегічним управлінням доступом і сегментацією мережі дозволяє значно знизити ризики, пов’язані з кібератаками. Однак технології самі по собі не є панацеєю; людський фактор відіграє критичну роль у забезпеченні безпеки. Навчання користувачів основам кібербезпеки, підвищення їх обізнаності про загрози та розробка корпоративних політик, що регулюють поведінку в мережі, є невід'ємною частиною загальної стратегії.

З огляду на стрімкий розвиток технологій та зміну ландшафту загроз, компанії повинні залишатися гнучкими і готовими адаптувати свої стратегії кібербезпеки до нових викликів. Регулярні аудити, оцінки ризиків та впровадження нових рішень, зокрема в області штучного інтелекту, дозволять забезпечити проактивний підхід до захисту даних.

Отже, з огляду на зростаючу залежність суспільства від цифрових технологій, важливо, щоб держави, підприємства та користувачі об'єднали зусилля для створення безпечного цифрового середовища. Лише спільними зусиллями можна забезпечити надійний захист інформації, що є основою для розвитку сучасних економік і суспільств у цілому. В умовах швидко змінюваного цифрового світу забезпечення кібербезпеки має стати пріоритетом для всіх.

Інформаційні джерела:

1. Легомінова С., Гайдур Г. Аналіз сучасних загроз інформаційній безпеці організацій та формування інформаційної платформи протидії їм. *Кібербезпека: освіта, наука, техніка*. 2023. № 2(22), С. 54-67. URL://doi.org/10.28925/2663-4023.2023.22.5467.

2. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. Київ: ДУТ, 2015. 288 с.

КІБЕРБЕЗПЕКА ІНФОРМАЦІЙНО-АНАЛІТИЧНИХ СЕРВІСІВ УПРАВЛІННЯ ПІДПРИЄМСТВОМ

Кащена Н.Б., д-р екон. наук, проф.
Бакаляр Д.Г., PhD
Державний біотехнологічний університет

Інформаційно-аналітичні сервіси управління підприємством формують інформаційній простір прийняття бізнес-рішень. За умов високої невизначеності та конкуренції вони є драйверами сучасного менеджменту та розвитку бізнесу, що дозволяють оптимізувати інфокомунікаційні канали взаємодії суб’єктів економічних відносин і генерують релевантні масиви обліково-аналітичних даних для оцінки, контролю та оптимізації бізнес-процесів, підтримки інновацій та адаптації до цифрових змін, оперативного управління, стратегічного планування та прогнозування фінансово-економічних показників й ринкових трендів [1].

Інформація у сучасному світі є одним з найцінніших активів [2], а можливість оперативно її обробляти та аналізувати [3; 4] формує конкурентні переваги підприємства. Тому необхідно дбати про надійний захист обліково-аналітичних даних інформаційних сервісів. Бо їх уразливість ставить під загрозу не тільки бізнес-процеси, але й стратегічні цілі розвитку бізнесу. Так, можливі кіберзагрози (рис. 1) та компрометація даних можуть призвести до втрати конкурентних переваг, фінансових збитків і репутаційних ризиків.