УДК 621.313

Д.Р. Ільчук
С. С. Штефанеса

Аналіз сучасного стану технологій захисту інформації в комп'ютеризованих інформаційно-вимірювальних системах

Вінницький національний технічний університет

Анотація *У даній роботі розглянуто та досліджено технології захисту інформації, поняття інформаційної безпеки, конфеденційності даних. Визначено мету та цілі захисту інформації. Проаналізовано принципи, вимоги, види, заходи, технології та практики захисту інформації.*

Ключові слова: інформаційна безпека, конфіденційність, доступність, безпека, шифрування, тестування, відмовостійкість та відмова, реагування та інциденти, управління вразливістю, криптографія, хмарна безпека, безпека кінцевої точки.

Abstract *Information protection technologies, concepts of information security, data confidentiality are considered and researched in this work. The purpose and goals of information protection are defined. The principles, requirements, measures, technologies and practices of information protection are analyzed.*

Keywords: information security, confidentiality, availability, security, encryption, testing, failover and failback, incident response, vulnerability management, cryptography, cloud security, endpoint security.

Вступ

Сьогодні інформація стала найціннішим ресурсом в нашому світі, і її безпека стає ключовим питанням для індивідів, компаній та установ будь-якого рівня та сфери діяльності. Статистика показує, що середня вартість одного витоку інформації у світі становить близько 5,3 мільйона доларів, що є прикладом того, наскільки дорогоцінною може бути недбалість у питаннях інформаційної безпеки. Це число є лише вершинкою айсберга, оскільки наслідки витоку інформації можуть бути набагато серйознішими, ніж лише фінансові втрати. Вони можуть включати в себе ризики для репутації, порушення конфіденційності особистих даних, а також загрози для національної безпеки. Тому питання інформаційної безпеки стає не тільки економічним, але й соціокультурним і політичним викликом.

Враховуючи важливість захисту інформації в сучасному світі, проведемо аналіз технологій захисту інформації з метою знайти ефективні рішення, які забезпечать конфіденційність, цілісність та доступність цінних даних в цифровому світі.

Результати дослідження

Втрата даних і пошкодження щорічно коштують організаціям мільярди. Одна подія з кібербезпеки коштує близько 100 000 доларів США за інцидент, і витрати продовжують зростати. Організація, яка стала жертвою витоку даних, повинна витрачати гроші на покриття судових витрат, штрафів за недотримання вимог і нових інструментів кібербезпеки. Таким чином, запровадження належного контролю для захисту інформації є загальним рентабельним.

Мета захисту даних — зупинити крадіжку даних до того, як організація постраждає від дорогих наслідків успішного зламу. Це також захищає клієнтів від втрати їхніх даних через зловмисників і, можливо, від крадіжки особистих даних і шахрайства. Уникнення компромісу також не є єдиною перевагою. Захист даних допомагає корпораціям знайти цінність своїх даних, каталогізуючи їх для використання в майбутньому.

Безперервність роботи залежить від захисту інформації. Щоб підтримувати безперервність, підприємствам потрібні способи відновлення після події кібербезпеки. Наприклад, неправильна конфігурація або неочікуваний збій системи може призвести до пошкодження даних. Після цих подій запрацюють плани захисту даних. Час, необхідний для відновлення бізнесу після простою, впливає на дохід. Чим довше система страждає від простою, тим довше бізнес не може підтримувати продуктивність. Без продуктивності бізнес не може підтримувати дохід. Крім того, простої можуть вплинути на зростання майбутнього доходу та завдати шкоди бренду[1,7].

Інформаційна безпека – це набір методів та заходів, призначених для захисту даних від несанкціонованого доступу або змін. Ось широкий огляд політики, принципів і людей, які використовуються для захисту даних[3].

Інформаційна безпека захищає конфіденційну інформацію від несанкціонованих дій, включаючи перевірку, модифікацію, записування та будь-яке порушення чи знищення. Мета полягає в тому,

щоб забезпечити безпеку та конфіденційність важливих даних, таких як деталі облікових записів клієнтів, фінансові дані чи інтелектуальна власність.

Основними принципами інформаційної безпеки є конфіденційність, цілісність і доступність. Кожен елемент програми інформаційної безпеки повинен бути розроблений для реалізації одного або кількох із цих принципів. Разом вони називаються тріадою ЦРУ.

1. Конфіденційність: Заходи конфіденційності призначені для запобігання несанкціонованому розголошенню інформації. Метою принципу конфіденційності є збереження особистої інформації та забезпечення її видимості та доступу лише для тих осіб, які нею володіють або потребують її для виконання своїх організаційних функцій.

2. Цілісність: Узгодженість включає захист від несанкціонованих змін (додавання, видалення, зміни тощо) даних. Принцип цілісності гарантує, що дані є точними та надійними та не змінюються неправильно, випадково чи зловмисно.

3. Доступність: Доступність — це захист здатності системи робити програмні системи та дані повністю доступними, коли це потрібно користувачеві (або у визначений час). Мета доступності — зробити технологічну інфраструктуру , програми та дані доступними, коли вони потрібні для організаційного процесу або для клієнтів організації[2].

В ідеальному світі дані завжди повинні бути конфіденційними, у правильному стані та доступними; на практиці, звісно, часто доводиться вибирати, на яких принципах інформаційної безпеки акцентувати увагу, і це вимагає оцінки ваших даних. Наприклад, якщо зберігаємо конфіденційну медичну інформацію, зосереджуємося на конфіденційності, тоді як фінансова установа може наголошувати на цілісності даних, щоб гарантувати, що чийсь банківський рахунок не буде зараховано чи дебетовано неправильно.

Відмінності між захистом інформації, безпекою та конфіденційністю

Захист інформації, безпека та конфіденційність – пов’язані терміни, які часто використовуються як синоніми, але кожен з них має різні значення та наміри:

Захист інформації: заходи захисту, які запобігають несанкціонованому доступу, використанню, розголошенню, зміні або знищенню інформації. Захист даних охоплює всі фізичні, технічні, адміністративні та юридичні ініціативи для захисту даних.

Безпека: протоколи для захисту комп’ютерних систем, програмного забезпечення та мереж від злому доступу, використання, зміни чи знищення. Безпека охоплює фізичні, технічні й адміністративні системи для захисту комп’ютерів і мережевої інфраструктури.

Конфіденційність: у контексті захисту інформації конфіденційність охоплює всі заходи, вжиті для захисту особистої та конфіденційної інформації, наприклад обмеження доступу до даних; отримання згоди на її збір, оприлюднення та використання; а також забезпечення точності та актуальності даних[1].

Види інформаційної безпеки

Розглядаючи інформаційну безпеку, ми повинні знати багато підтипів. Ці підтипи охоплюють конкретні типи інформації, інструменти, що використовуються для захисту інформації, і області, де інформація потребує захисту.

Безпека програми: Стратегії безпеки додатків захищають додатки та інтерфейси прикладного програмування (API). Ви можете використовувати ці стратегії для запобігання, виявлення та виправлення помилок або інших вразливостей у своїх програмах. Якщо не захистити, уразливості додатків і API можуть стати шлюзом до ваших ширших систем, піддаючи вашій інформації ризик.

Безпека інфраструктури: Стратегії безпеки інфраструктури захищають компоненти інфраструктури, включаючи мережі, сервери, клієнтські пристрої, мобільні пристрої та центри обробки даних. Важливою метою безпеки інфраструктури є мінімізація залежностей та ізоляція компонентів, дозволяючи при цьому взаємозв’язок.

Хмарна безпека забезпечує захист, подібний до безпеки додатків та інфраструктури, але зосереджена на хмарних або підключених до хмарних компонентах і інформації. Хмарна безпека додає додаткові засоби захисту та інструменти, щоб зосередитися на вразливостях, які виникають через інтернет-сервіси та спільні середовища, такі як загальнодоступні хмари.

Безпека кінцевих точок допомагає захистити кінцеві точки кінцевих користувачів, такі як ноутбуки, настільні ПК, смартфони та планшети, від кібератак. Організації впроваджують безпеку кінцевих точок для захисту пристроїв, які використовуються для роботи, включно з підключеними до локальної мережі та з використанням хмарних ресурсів.

Криптографія використовує практику, яка називається шифруванням, щоб захистити інформацію шляхом приховування вмісту. Коли інформація зашифрована, вона доступна лише

користувачам, які мають правильний ключ шифрування. Якщо у користувачів немає цього ключа, інформація буде незрозумілою.

Реагування на інциденти – це набір процедур та інструментів, які можна використовувати для виявлення, розслідування та реагування на загрози чи шкідливі події. Він усуває або зменшує шкоду, заподіяну системам через атаки, стихійні лиха, системні збої або людські помилки.

Управління вразливістю — це практика, призначена для зменшення невід'ємних ризиків у програмі чи системі. Ідея цієї практики полягає у виявленні та виправленні вразливостей до того, як проблеми будуть виявлені або використані. Чим менше вразливостей має компонент або система, тим безпечнішими є ваша інформація та ресурси.

Управління даними про здоров'я: Управління медичними даними (HDM) полегшує систематичну організацію медичних даних у цифровій формі. Мета полягає в тому, щоб зробити лікування пацієнтів ефективним і допомогти отримати інформацію для покращення медичних результатів, одночасно захищаючи безпеку та конфіденційність медичних даних.

Цифрова криміналістика – це ідентифікація, збір і аналіз електронних доказів. Майже кожен злочин сьогодні має компонент цифрової криміналістики, а експерти з цифрової криміналістики надають важливу допомогу в поліцейських розслідуваннях[6].

Вимоги до захисту інформації

Щоб реалізувати представлені вище принципи, система повинна відповідати ряду вимог:

1. Централізованість. Процес управління завжди є централізованим, а система, використовувана для його реалізації, повинна підходити під структуру об'єкту, який треба оберігати.

2. Плановість. Система захисту інформації повинна базуватися на взаємодії усіх підрозділів, спрямованих на реалізацію прийнятої політики безпеки.

3. Конкретика і цілеспрямованість. Захищатися повинні конкретні інформаційні ресурси, які можуть бути цікаві для конкурентів.

4. Активність. Захист інформації повинен організовуватися з наполегливістю, тому важливі засоби прогнозування, експертних системи і інших інструментів, спрямованих на реалізацію принципу "виявити і усунути".

5. Надійність і універсальність. Система повинна застосовувати різні методи і засоби для запобігання витоку.

6. Відкритість. У будь-який час має бути можливість змінити або доповнити заходи забезпечення безпеки.

7. Економічний ефект. Важливо, щоб витрати на захист не були більше розміру можливого збитку.

Заходи захисту інформації

Як уже має бути зрозуміло, майже всі технічні заходи, пов'язані з кібербезпекою, певною мірою стосуються інформаційної безпеки, але тут варто подумати про заходи інформаційної безпеки в широкому плані:

1. Технічні заходи включають апаратне та програмне забезпечення, яке захищає дані — від шифрування до брандмауерів

2. Організаційні заходи включають створення внутрішнього підрозділу, присвяченого інформаційній безпеці, а також включення до обов'язків деяких співробітників кожного відділу.

3. Людські заходи включають проведення тренінгів для користувачів щодо належних практик інформаційної безпеки

4. Фізичні заходи включають контроль доступу до офісів і, особливо, центрів обробки даних

5. Сучасні технологі захисту інформації[3,4]

Технології та практики захисту інформації

Створення ефективної стратегії інформаційної безпеки вимагає застосування різноманітних інструментів і технологій. Більшість стратегій використовують певну комбінацію наступних технологій.

Брандмауери: Брандмауери — це рівень захисту, який можна застосувати до мереж або програм. Ці інструменти дозволяють фільтрувати трафік і повідомляти дані про трафік системам моніторингу та виявлення. Брандмауери часто використовують встановлені списки схваленого чи несхваленого трафіку та політики, що визначають швидкість або обсяг дозволеного трафіку[5].

Управління інцидентами безпеки та подіями (SIEM): Рішення SIEM дозволяють отримувати та співвідносити інформацію з усіх ваших систем. Таке об'єднання даних дозволяє командам ефективніше виявляти загрози, ефективніше керувати попередженнями та створювати кращий контекст для розслідувань. Рішення SIEM також корисні для реєстрації подій, які відбуваються в

системі, або звітування про події та продуктивність. Потім ви можете використовувати цю інформацію, щоб підтвердити відповідність або оптимізувати конфігурації.

Запобігання втраті даних (DLP): Стратегії DLP включають інструменти та практики, які захищають дані від втрати або модифікації. Це включає класифікацію даних, резервне копіювання даних і моніторинг того, як дані передаються між організацією та за її межами. Наприклад, ви можете використовувати рішення DLP для сканування вихідних електронних листів, щоб визначити, чи конфіденційна інформація неналежним чином передається.

Система виявлення вторгнень (IDS): Рішення IDS — це інструменти для моніторингу вхідного трафіку та виявлення загроз. Ці інструменти оцінюють трафік і попереджають про будь-які випадки, які здаються підозрілими або шкідливими.

Система запобігання вторгненням (IPS): Рішення безпеки IPS схожі на рішення IDS, і вони часто використовуються разом. Ці рішення реагують на трафік, визначений як підозрілий або зловмисний, блокуючи запити або завершуючи сеанси користувачів. Ви можете використовувати рішення IPS для керування мережевим трафіком відповідно до визначених політик безпеки.

Аналітика поведінки користувачів (UBA): Рішення UBA збирають інформацію про дії користувачів і співвідносять цю поведінку з базовою лінією. Рішення потім використовують цю базову лінію як порівняння з новою поведінкою для виявлення невідповідностей. Потім рішення позначає ці невідповідності як потенційні загрози. Наприклад, ви можете використовувати рішення UBA для моніторингу дій користувачів і визначення, якщо користувач починає експортувати великі обсяги даних, що вказує на внутрішню загрозу.

Кібербезпека блокчейну: Кібербезпека блокчейну — це технологія, яка базується на незмінних транзакційних подіях. У технологіях блокчейн розподілені мережі користувачів перевіряють автентичність транзакцій і забезпечують підтримку цілісності. Хоча ці технології ще не використовуються широко, деякі компанії починають включати блокчейн у нові рішення.

Виявлення кінцевої точки та відповідь (EDR): Рішення з кібербезпеки EDR дозволяють відстежувати діяльність кінцевих точок, виявляти підозрілу активність і автоматично реагувати на загрози. Ці рішення призначені для покращення видимості кінцевих пристроїв і можуть використовуватися для запобігання проникненню загроз у ваші мережі або виходу інформації. Рішення EDR покладаються на постійний збір даних кінцевої точки, механізми виявлення та реєстрацію подій[5,6] .

Розширене виявлення та реагування (XDR): XDR — це набір технологій, які допомагають службам безпеки підвищити ефективність виявлення загроз, а також швидкість їх розслідування та реагування. XDR об’єднує дані з усіх рівнів IT-середовища, включно з мережами, електронною поштою, кінцевими точками, пристроями Інтернету речей, хмарними робочими навантаженнями, системами ідентифікації та серверами, і збагачує джерела аналізом загроз для виявлення обхідних, складних загроз. XDR забезпечує автоматизоване, готове виявлення загроз, дослідження та реагування (TDIR) на різні загрози. Оскільки рішення XDR є хмарними, організації можуть застосовувати їх для гетерогенних розподілених IT-середовищ. Ці готові рішення негайно забезпечують цінність і допомагають підвищити продуктивність команд безпеки.

Хмарне керування безпекою (CSPM): CSPM — це набір практик і технологій, які можна використовувати для оцінки безпеки ваших хмарних ресурсів. Ці технології дають змогу сканувати конфігурації, порівнювати засоби захисту з контрольними тестами та гарантувати однакове застосування політик безпеки. Часто рішення CSPM надають рекомендації чи вказівки щодо виправлення, які можна використовувати для покращення рівня безпеки.

Віддалений доступ VPN і SASE: Віртуальна приватна мережа віддаленого доступу (VPN) дозволяє організаціям надавати безпечний віддалений доступ до даних і програм, які знаходяться в корпоративній мережі. VPN створює тунель між мережею та віддаленим користувачем. Він захищає трафік, що проходить через тунель, шифруючи його. Віддалений доступ VPN підключає одного користувача до локальних ресурсів, але не забезпечує видимість хмарних ресурсів. Secure Access Service Edge (SASE) забезпечує безпеку в гібридному середовищі, забезпечуючи видимість усіх ресурсів. SASE – це хмарна служба, яка не покладається на VPN або автономні проксі-сервери. Натомість він надає різні інструменти безпеки мережі як хмарний сервіс.

BYOD: Принесіть свій власний пристрій (BYOD) — це підхід, який дозволяє співробітникам використовувати свої особисті пристрої, такі як ноутбуки, планшети, смартфони, USB-накопичувачі та ПК, для робочих цілей. Це означає, що співробітники можуть використовувати свої пристрої для підключення до корпоративної мережі та доступу до конфіденційних систем і конфіденційних даних. BYOD може покращити взаємодію з користувачем, дозволяючи співробітникам працювати

на знайомих пристроях з будь-якого місця. Це дозволяє співробітникам використовувати свої пристрої для віддаленої роботи з дому або під час подорожі. Однак BYOD часто призводить до тіньових IT-спеціалістів, оскільки IT-персонал погано бачить (якщо взагалі) ці кінцеві точки та не може належним чином запровадити та підтримувати заходи безпеки. Організації можуть захистити себе від загроз BYOD, використовуючи віртуалізацію додатків і рішення безпеки кінцевих точок, щоб розширити видимість і отримати комплексні засоби безпеки та керування.

Розвідка загроз: Розвідка про загрози – це інформація, зібрана з ряду джерел про поточні або потенційні атаки на організацію. Інформація аналізується, уточнюється та систематизується, а потім використовується для запобігання та зменшення ризиків кібербезпеки. Основна мета аналізу загроз — показати організаціям ризики, з якими вони стикаються через зовнішні загрози, такі як загрози нульового дня та вдосконалені постійні загрози (APT). Розвідка про загрози включає поглиблену інформацію та контекст про конкретні загрози, наприклад, хто є суб'єктами загрози, їхні можливості та мотивація, а також показники компрометації (IoC). Маючи цю інформацію, організації можуть приймати зважені рішення про те, як захиститися від найшкідливіших атак.

Мікросегментація — це техніка безпеки, яка розділяє мережу на окремі зони та використовує політики, щоб диктувати, як доступ до даних і додатків у цих зонах можна контролювати. Це дає змогу командам із безпеки визначати, як додатки чи робочі навантаження можуть обмінюватися даними в системі, у якому напрямку дані можуть надаватися, і чи потрібні заходи безпеки чи інші заходи автентифікації. На відміну від сегментації мережі, для якої зазвичай потрібне апаратне забезпечення та орієнтована на трафік Північ-Південь (потоки даних клієнт-сервер між центрами обробки даних), мікросегментація покладається на програмне забезпечення та адаптована до трафіку Схід-Захід або потоків даних між серверами програми. Мікросегментація обмежує тип трафіку, який може латерально проходити через мережу, що може запобігти поширеним методам атаки, таким як латеральний рух. Його можна застосовувати в усій мережі, як у внутрішньому центрі обробки даних, так і в хмарних середовищах[5,6].

Висновки

Отже, в даній роботі було проаналізовано сучасний стан технологій захисту інформацій в комп'ютеризованих інформаційно-вимірювальних системах. Розглянуто принципи, вимоги та види захисту інформації. Проаналізовано сучасні технології та практики захисту інформації.

В результаті чого можна зробити висновок що технології захисту інформації в сучасному світі значно прогресують і кожна із технологій має своє призначення і обов'язково використовується провідними компаніями світу. Основна мета захисту інформації полягає в забезпеченні конфіденційності, цілісності та доступності цінних даних та ресурсів, забезпечуючи відстоювання від потенційних загроз, які можуть виникнути в результаті кібератак, недбалості або наміреної деструкції. Це важлива мета, оскільки вона гарантує, що інформація залишається захищеною від несанкціонованого доступу, змін та втрати, що може мати серйозні наслідки для індивідів, компаній та суспільства в цілому. Кожна з наведених технологій і практик грає важливу роль у сфері інформаційної безпеки, і їх вибір залежить від конкретних потреб та контексту організації. Брандмауери: Контролюють мережевий трафік. SIEM: Аналізують та виявляють загрози з різних джерел. DLP: Захищають конфіденційні дані від витоку. IDS та IPS: Виявляють та реагують на потенційні загрози. UBA: Виявляють невідповідності в поведінці користувачів. Кібербезпека блокчейну: Забезпечують цілісність та автентичність транзакцій у розподіленій мережі. EDR: Відстежують та реагують на загрози на кінцевих пристроях. XDR: Покращують виявлення та реагування на загрози. CSPM: Оцінюють та забезпечують безпеку хмарних ресурсів. VPN і BYOD: Забезпечують безпечний віддалений доступ та поліпшують продуктивність. Розвідка загроз: Допомагає розуміти потенційні загрози. Мікросегментація: Забезпечує контроль доступу в мережі шляхом розділення на зони.

Важливо пам'ятати, що вибір технологій повинен враховувати конкретні потреби та ризики організації. Часто комбінування декількох технологій допомагає досягнути більш високого рівня захисту інформації. Також важливо постійно оновлювати та адаптувати свою стратегію інформаційної безпеки відповідно до змін загроз і технологій.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Data-protection [Електронний ресурс] – Режим доступу до ресурсу: https://www.proofpoint.com/us/threat-reference/data-protection.
2. Data-security, information-security [Електронний ресурс] – Режим доступу до ресурсу: https://www.imperva.com/learn/data-security/information-security-infosec/.
3. What is information security? [Електронний ресурс] – Режим доступу до ресурсу: https://www.csoonline.com/article/568841/what-is-information-security-definition-principles-and-jobs.html.
4. Захист інформації [Електронний ресурс] – Режим доступу до ресурсу: https://publish.com.ua/biznes/zakhist-informatsiji-aktualnist-i-metodi.html.
5. What is the protection of data and confidentiality? [Електронний ресурс] – Режим доступу до ресурсу: https://cloudian.com/guides/data-protection/data-protection-and-privacy-7-ways-to-protect-user-data/#protection-technologies.
6. What Is Information Security? Goals, Types and Applications [Електронний ресурс] – Режим доступу до ресурсу: https://www.exabeam.com/explainers/information-security/information-security-goals-types-and-applications/.
7. Information security protection goals and their significance [Електронний ресурс] – Режим доступу до ресурсу: https://www.dqsglobal.com/intl/learn/blog/information-security-protection-goals-and-their-significance.

Штефанеса Сергій Сергійович — *студент групи КІВТ – 23м, факультет інформаційних електронних систем, Вінницький національний технічний університет, м. Вінниця, e-mail: serhiishtefanesa@gmai.com*

Науковий керівник: *Ільчук Дмитро Русланович – асистент кафедри інформаційних радіоелектронних технологій і систем, Вінницький національний технічний університет, м. Вінниця, e-mail: demabels@gmail.com*

Shtefanesa Serhii Serhiyovich — *student of KIVT group - 23m, Faculty of Information Electronic Systems, Vinnytsia National Technical University, Vinnytsia, e-mail: serhiishtefanesa@gmail.com.*

Academic supervisor: *Ilchuk Dmytro Ruslanovych - assistant of the Department of Information Radio Electronics of technologies and systems, Vinnytsia National Technical University, Vinnytsia, e-mail: demabel@vntu.edu.ua*