DOI: 10.59647/978-617-520-936-3/1

Захист інформаційних систем підприємств

Іван Божок, студент [1 i] (ORCID: 0009-0007-7744-7678)

[1] *Київський національний університет будівництва і архітектури, 03037, м. Київ, проспект Повітряних Сил, 31, Україна*

АНОТАЦІЯ

Безліч компаній як мінімум один раз за рік зазнавали зовнішньої атаки або зіштовхувалися з внутрішніми інцидентами інформаційної безпеки. Уявіть собі, кожну секунду у світі створюються сотні одиниць нового шкідливого програмного забезпечення. Несанкціонований доступ до особистої інформації, фінансових рахунків або комерційної таємниці може заподіяти багато шкоди. Це може призвести до великих збитків через втрату репутації та фінансових активів, порушення приватності користувачів тощо. Тож кожна особа, організація, підприємство чи фінансова установа має дбати про захист даних.

Ключові слова: інформаційна безпека, захист даних, кіберзагрози, шкідливе програмне забезпечення, корпоративні дані, контролю доступу, захист інформаційних систем, конфіденційність, комплексний захист.

1. ВСТУП

Прогресивний сучасний бізнес прагне максимальної автоматизації та активного розвитку власного інформаційного середовища. Якісне здійснення цього неможливе без реалізації комплексної системи захисту інформації на підприємстві. Особливо, якщо компанія бере на себе відповідальність за особисті відомості, що надаються клієнтами. Таким чином, можна зробити логічний висновок – захист корпоративних даних є обов'язковим і має бути здійснений якісно.

2. МЕТА

Основна мета компанії полягає у забезпеченні безпеки наступних аспектів:

- всіх наявних баз даних, які містять цінні відомості;
- документообігу компанії, що здійснюється в електронному форматі;
- різних технічних аспектів, пов'язаних із інформаційною інфраструктурою підприємства;
- комерційних питань, включаючи конфіденційні дані про бізнес-процеси.

Отримання зазначених відомостей сторонньою організацією може призвести до серйозних наслідків, аж до руйнування конкурентної позиції. Тому важливо мати висококваліфікованих спеціалістів, відповідальних за комплексний захист інформації на підприємстві та її належний контроль.

3. СПОСОБИ НЕЗАКОННОГО ОТРИМАННЯ ІНФОРМАЦІЇ СТОРОННІМИ ОСОБАМИ

Сторонні особи можуть використовувати різні способи отримання інформації. Розглянемо деякі з них:

- Розсилання шкідливих посилань. Зловмисники можуть надсилати електронні повідомлення, що містять шкідливі посилання, щоб отримати доступ до конфіденційної інформації.
- Використання вірусів. Шкідливе програмне забезпечення може бути використане для проникнення в систему та крадіжки даних.
- Встановлення шпигунських плагінів. За допомогою спеціальних програмних розширень зловмисники можуть отримувати доступ до матеріалів, що надсилаються через браузер.
- Використання хибного програмного забезпечення. Шахраї можуть використовувати програми, які автоматично змінюють функції, щоб отримати доступ до конфіденційних даних.

Таким чином, для забезпечення повної конфіденційності даних на підприємстві необхідна розробка та реалізація комплексної системи захисту інформації на підприємстві, що включають як апаратну, так і програмну складові.

4. ВИДИ ЗАХИСТУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ

Система захисту складається з багатьох взаємопов'язаних частин: організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем.

- **Фізичний захист:** включає заходи для забезпечення безпеки фізичного середовища, такі як контроль доступу до приміщень, використання камер спостереження, замки і система сигналізації. Також до нього можна віднести безпеку фізичних носіїв інформації: паперові документи, флеш-накопичувачі, жорсткі диски тощо. Він передбачає захист від втрати, пошкодження або незаконного використання.
- **Організаційний захист**: охоплює політики, процедури і практики, розроблені для забезпечення безпеки інформації в організації. Це включає політику навчання персоналу щодо безпеки, розподіл обов'язків і контроль доступу.
- **Фінансовий захист:** стосується захисту фінансових транзакцій і даних. Включає заходи для запобігання шахрайству, крадіжкам і фінансовим злочинам, такі як мережеві системи перевірки платежів і моніторинг фінансових операцій.
- **Технічний захист інформації**: охоплює апаратні методи захисту, які включають фізичні бар'єри для

обмеження доступу до системи, програмні методи або поєднання технічних та програмних засобів. Технічний захист також передбачає резервне копіювання і відновлення даних, і може охоплювати інші заходи, що стосуються безпеки комп'ютерних систем і мереж.

5. ЗАХОДИ ТА МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ

Створюючи системи захисту на підприємстві, необхідно враховувати, що, по-перше, для ефективного захисту інформаційних ресурсів потрібна реалізація цілої низки різноманітних заходів, які можна розподілити на три групи: юридичні, організаційно-економічні й технологічні. По-друге, хоча розробкою заходів у кожній із трьох груп повинні займатися фахівці відповідних галузей знань, які застосовують свої способи і методи для досягнення заданих цілей, успіх значною мірою буде залежати від того, наскільки в рамках системного підходу вдасться визначити і реалізувати взаємні зв'язки між відповідними визначеннями, принципами, способами і механізмами захисту.

Аналіз поглядів і концептуальних підходів до формування сучасних ефективних систем інформаційної безпеки підприємства дозволив сформулювати основні функції та завдання і намітити організаційні основи функціонування відповідних підрозділів інформаційної безпеки. У сучасному поданні рольових функцій служби інформаційної безпеки можна виділити чотири напрями:

1) розробка методології та методик аналізу загроз, оцінки рівня інформаційної безпеки підприємства і системи її забезпечення;

2) організація і здійснення конкретних видів діяльності із захисту інформації;

3) експлуатація технічних засобів захисту інформації;

4) аудит і контроль функціонування системи інформаційної безпеки підприємства.

Завдання забезпечення інформаційної безпеки необхідно вирішувати системно. Це означає, що засоби захисту інформації повинні застосовуватися одночасно і під централізованим управлінням

6. АВТОМАТИЗАЦІЯ КІБЕРЗАХИСТУ ТА ШТУЧНИЙ ІНТЕЛЕКТ (AI)

Кібербезпека і штучний інтелект (ШІ) стають все більш взаємопов'язаними, причому ШІ відіграє значну роль у посиленні заходів з кібербезпеки. Штучний інтелект — це широкий термін, що описує процес імітації людського інтелекту в машинах, щоб вони могли міркувати і використовувати логіку для вирішення проблем. ШІ у кібербезпеці базується на тому ж принципі: використання швидкості та обчислювальної потужності ШІ для створення протоколів кібербезпеки, які передбачають, ідентифікують та зменшують загрози.

Сучасні тенденції передбачають використання штучного інтелекту для автоматизації операцій з кібербезпеки та протидії загрозам "нульового дня", коли зловмисники використовують вразливості, невідомі виробникам програмного забезпечення.

Однією з можливостей для команд кібербезпеки є розробка нових та інноваційних способів виявлення та реагування на загрози. Вони можуть використовувати штучний інтелект для автоматизації завдань безпеки та створення більш адаптивних рішень для бізнесу та галузей.

Штучний інтелект навчається на власному досвіді. Генеративний ШІ перетинається з кібербезпекою, аналізуючи і навчаючись на величезних обсягах даних, щоб виявляти закономірності і приймати обґрунтовані рішення щодо реагування на потенційні загрози. Хоча він може вирішити лише деякі проблеми кібербезпеки, ШІ відіграє важливу роль у підтримці зусиль з кібербезпеки та дотриманні нормативних вимог. Хоча ШІ є потужним інструментом в арсеналі кібербезпеки, важливо використовувати його в поєднанні з людським досвідом та постійними дослідженнями і розробками.

7. ВИСНОВОК

Отже, прогресивний сучасний бізнес прагне максимальної автоматизації та активного розвитку власного інформаційного середовища. Якісне здійснення цього неможливе без реалізації комплексної системи захисту інформації на підприємстві. Особливо, якщо компанія бере на себе відповідальність за особисті відомості, що надаються клієнтами. Загалом, для забезпечення інфобезпеки малого, середнього та великого бізнесу необхідно вдатися до комплексного підходу.

Список літератури

[1] Корпоративна кібербезпека та роль штучного інтелекту у захисті даних. BDO Україна. URL: https://www.bdo.ua/uk-ua/insights-2/information-materials/2024/corporate-cybersecurity-ai-role-in-data-protection.

[2] Кібербезпека та штучний інтелект. Web Academy. URL: https://web-academy.ua/blog/junior/cybersecurity-and-artificial-intelligence.

[3] Інформаційна безпека на підприємстві. Дніпровський державний аграрно-економічний університет. URL: https://dspace.dsau.dp.ua/bitstream/123456789/5273/1/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0.pdf.

[4] Що потрібно знати бізнесу про захист інформації: огляд технічних засобів. Yubikey Україна. URL: https://yubikey.com.ua/shcho-potribno-znaty-biznesu-pro-zakhyst-informatsii-ohliad-tekhnichnykh-zasobiv?srsltid=AfmBOori1z8prGNAPFQA-O2mMcAUhBpAUDGXO32PmpB3KcS7LAE2tgcj.

[5] Кібербезпека бізнесу – це не лише технічні заходи. Legal IT Group. URL: https://legalitgroup.com/kiberbezpeka-biznesu-tse-ne-lishe-tehnichni-zahodi/.

[6] Захист інформації на підприємстві. ResIT. URL: https://resit.com.ua/zachist-informacii-na-pidpriemstvi/.

[i] *Робота виконана під керівництвом к. т. н., доц. Євгенії Шабали*