**Владислав Цвєтков**

**(Рівне, Україна)**

**Інформаційна безпека**

Інформаційна безпека - це практика захисту інформації та інформаційних систем від несанкціонованого доступу, використання, розкриття, перекручення, модифікації або знищення. У сучасну цифрову епоху інформаційна безпека стала критично важливою проблемою як для організацій, так і для приватних осіб та урядів. Зростаюча залежність від цифрової інформації та взаємопов'язаність комп'ютерних систем збільшили ризик кібератак і витоку даних. У цій статті ми обговоримо важливість інформаційної безпеки, ключові загрози інформаційній безпеці та заходи, яких можна вжити для забезпечення інформаційної безпеки.

Інформація є цінним активом, який необхідний для функціонування будь-якої організації. Вона може включати в себе конфіденційні дані, такі як інформація про клієнтів, фінансові документи, інтелектуальну власність та комерційну таємницю. Втрата або компрометація такої інформації може мати серйозні наслідки, такі як фінансові збитки, юридичні зобов'язання, шкода репутації і навіть штрафи від регуляторних органів. Більше того, у сучасному взаємопов'язаному світі ризик кібератак та витоку даних багаторазово зріс, що робить інформаційну безпеку критично важливою проблемою.

Важливість інформаційної безпеки стала ще більш очевидною з розвитком віддаленої роботи. Оскільки працівники отримують доступ до конфіденційних даних з віддалених місць, організації повинні забезпечити, щоб їхні заходи інформаційної безпеки були достатньо надійними для захисту від кіберзагроз. Це призвело до посилення уваги до таких заходів безпеки, як багатофакторна автентифікація, віртуальні приватні мережі (VPN) та захист кінцевих точок.

Крім того, швидкий темп технологічного прогресу створив нові виклики для інформаційної безпеки. Нові технології, такі як штучний інтелект, хмарні обчислення та Інтернет речей (IoT), трансформують способи збору, зберігання та аналізу даних в організаціях. Однак вони також несуть нові ризики для безпеки, оскільки кіберзлочинці використовують вразливості в цих системах для отримання несанкціонованого доступу до конфіденційної інформації.

Для ефективного управління ризиками інформаційної безпеки організаціям необхідно застосовувати комплексний підхід, який включає не лише технічні заходи, але й політики, процедури та навчальні програми, спрямовані на підвищення обізнаності працівників у питаннях безпеки. Регулярні оцінки та аудити безпеки також мають вирішальне значення для виявлення та усунення потенційних вразливостей в інформаційних системах.

Зрештою, важливість інформаційної безпеки неможливо переоцінити. Вона має вирішальне значення для захисту репутації організації, забезпечення відповідності нормативним вимогам і збереження довіри клієнтів. Інвестуючи в надійні заходи інформаційної безпеки, організації можуть захистити свої цінні активи та зменшити ризики кіберзагроз у сучасному цифровому ландшафті, що постійно змінюється.

Існує кілька типів загроз інформаційній безпеці, зокрема:

*Шкідливе програмне забезпечення:* Шкідливе програмне забезпечення - це шкідливе програмне забезпечення, призначене для завдання шкоди комп'ютерній системі. Воно може приймати різні форми, такі як віруси, хробаки, трояни та програми-вимагачі. Шкідливе програмне забезпечення може потрапити в систему через інфіковані вкладення електронної пошти, завантаження з ненадійних джерел або вразливості в програмному забезпеченні.

*Фішинг:* Фішинг - це соціальна інженерна атака, яка полягає в тому, щоб обманом змусити користувачів розкрити конфіденційну інформацію, таку як імена користувачів, паролі або дані кредитних карток. Зазвичай це робиться через електронну пошту, телефонні дзвінки або текстові повідомлення. Фішингові атаки можуть бути витонченими, їх важко виявити, і вони часто покладаються на людську помилку.

*Внутрішні загрози:* Внутрішні загрози - це загрози, які надходять зсередини організації. Вони можуть бути навмисними або ненавмисними і можуть включати працівників, підрядників або партнерів, які мають доступ до конфіденційної інформації. Внутрішні загрози може бути важко виявити, оскільки вони можуть мати законний доступ до системи.

*Атаки на відмову в обслуговуванні (DoS-атаки):*DoS-атаки передбачають перевантаження комп'ютерної системи або мережі трафіком, що унеможливлює доступ до системи для законних користувачів. DoS-атаки можуть здійснюватися зловмисниками, які використовують кілька зламаних комп'ютерів, відомих як ботнет, для переповнення системи трафіком.

*Атаки типу "людина посередині" (Man-in-the-middle, MITM):* MITM-атаки передбачають перехоплення комунікації між двома сторонами і викрадення або модифікацію інформації, якою вони обмінюються. Це може бути зроблено зловмисниками, які отримали доступ до мережі, або за допомогою програмного забезпечення для перехоплення комунікації.

Для забезпечення інформаційної безпеки організації та окремі особи можуть вжити кілька заходів, зокрема:

*Впровадження контролю доступу:* Контроль доступу обмежує доступ до конфіденційної інформації лише уповноваженому персоналу. Це можна зробити за допомогою таких заходів, як паролі, двофакторна автентифікація та біометрична автентифікація. Контроль доступу може допомогти запобігти несанкціонованому доступу до конфіденційної інформації.

*Шифрування:* Шифрування передбачає перетворення конфіденційної інформації в закодований формат, який може бути розшифрований лише уповноваженими особами за допомогою ключа розшифрування. Це може запобігти несанкціонованому доступу до конфіденційної інформації, навіть якщо її перехоплять. Шифрування можна використовувати для захисту конфіденційних даних під час передачі, наприклад, даних, що передаються мережею, та даних у стані спокою, наприклад, даних, що зберігаються на жорсткому диску.

*Регулярне оновлення програмного забезпечення:* Регулярне оновлення програмного забезпечення має важливе значення для забезпечення безпеки комп'ютерних систем. Оновлення програмного забезпечення часто включають виправлення відомих вразливостей, які можуть бути використані зловмисниками. Якщо не оновлювати програмне забезпечення, системи можуть стати вразливими до атак.

*Навчання та обізнаність:* Програми навчання та підвищення обізнаності можуть допомогти працівникам та окремим особам зрозуміти важливість інформаційної безпеки та заходи, яких вони можуть вжити для її забезпечення. Це може включати навчання тому, як розпізнавати фішингові електронні листи, як створювати надійні паролі та як повідомляти про інциденти безпеки.

*Регулярне оцінювання безпеки:* Регулярні оцінки безпеки можуть допомогти організаціям виявити вразливості в їхніх системах інформаційної безпеки та усунути їх до того, як вони будуть використані. Оцінка безпеки може включати тестування на проникнення, оцінку вразливостей та аудит безпеки.

*Резервне копіювання:* Резервне копіювання може допомогти гарантувати, що конфіденційна інформація не буде втрачена у випадку кібератаки або витоку даних. Резервні копії слід зберігати надійно і регулярно тестувати, щоб забезпечити можливість їх відновлення в разі збою системи.

На додаток до цих заходів, організації та окремі особи можуть також розглянути можливість застосування підходу до інформаційної безпеки, заснованого на управлінні ризиками. Це передбачає виявлення потенційних загроз і вразливостей, оцінку ймовірності та впливу цих ризиків, а також впровадження засобів контролю для їхнього зменшення. Управління ризиками може допомогти організаціям визначити пріоритети у сфері інформаційної безпеки та ефективно розподілити ресурси.

Іншим важливим аспектом інформаційної безпеки є планування реагування на інциденти. Організації повинні мати план реагування на інциденти безпеки, такі як витік даних, атаки шкідливого програмного забезпечення та системні збої. План повинен включати процедури ідентифікації та локалізації інциденту, повідомлення зацікавлених сторін та відновлення нормальної роботи систем. Регулярне тестування і навчання допоможуть забезпечити ефективність і актуальність плану реагування на інциденти.

На завершення, інформаційна безпека є критично важливим питанням, яке вимагає уваги та дій як від організацій, так і від окремих осіб. Впроваджуючи контроль доступу, шифрування, оновлення програмного забезпечення, навчальні та інформаційні програми, регулярну оцінку безпеки, резервне копіювання, управління ризиками та планування реагування на інциденти, організації та приватні особи можуть допомогти захистити себе від кіберзагроз і забезпечити конфіденційність, цілісність та доступність своєї конфіденційної інформації.

Інформаційна безпека є критично важливою проблемою в сучасну цифрову епоху, коли зростає залежність від цифрової інформації та взаємозв'язку комп'ютерних систем. Втрата або компрометація конфіденційної інформації може мати серйозні наслідки, що робить інформаційну безпеку головним пріоритетом як для організацій, так і для окремих осіб. Існує кілька типів загроз інформаційній безпеці, серед яких шкідливе програмне забезпечення, фішинг, інсайдерські загрози, DoS-атаки та MITM-атаки. Для забезпечення інформаційної безпеки організації та окремі особи можуть вжити низку заходів, зокрема, впровадити контроль доступу, шифрування, регулярне оновлення програмного забезпечення, навчання та інформування, регулярну оцінку безпеки та резервне копіювання. Інформаційна безпека - це безперервний процес, який вимагає постійного моніторингу, оцінки та вдосконалення для адаптації до нових загроз.

**Література:**

1. Вітман, М. Е., та Матторд, Х. Дж. (2018). Принципи інформаційної безпеки (6-е вид.). CengageLearning.
2. Кізза, Я. М. (2016). Посібник з безпеки комп'ютерних мереж (4-е вид.). SpringerInternationalPublishing.
3. Комп'ютерна команда реагування на надзвичайні ситуації (CERT). (2022). Загальні вразливості кібербезпеки.
4. Національний інститут стандартів і технологій (NIST). (2021). Рамки кібербезпеки.
5. Міжнародна організація зі стандартизації (ISO). (2021). ISO/IEC 27001:2013 - Інформаційні технології - Методи забезпечення безпеки - Системи управління інформаційною безпекою - Вимоги.
6. Агентство Європейського Союзу з кібербезпеки (ENISA). (2021). Тренінг з кібербезпеки для працівників.
7. Інститут SANS. (2022). Тестування на проникнення.
8. Міністерство внутрішньої безпеки США. (2022). Агентство кібербезпеки та безпеки інфраструктури.
9. Інститут Понемон. (2021). Вартість звіту про витік даних.
10. Verizon. (2021). Звіт про розслідування витоку даних.

**Науковий керівник:**

викладач Черняк Тетяна Григорівна.