***Боднар Владислав Романович****, cтудент IV курсу бакалаврату,*

*Київський національний університет*

*будівництва і архітектури, Київ, Україна*

***Науковий керівник: Шабала Євгенія Євгенівна,***

*доцент кафедри кібербезпеки та комп’ютерної інженерії*

**Засоби захисту корпоративної інформації**

Важлива інформація завжди була вагомою здобиччю для зловмисників.

Корпоративна інформаційна система - це інформаційна система, яка

підтримує автоматизацію функцій управління і надає інформацію для поглиблення знань та прийняття управлінських рішень. В ній реалізована сучасна управлінська ідеологія, яка поєднує бізнес-стратегію підприємства і прогресивні інформаційні технології, зберігаються важливі корпоративні дані.[1] Після розвитку бізнесів в різних сферах та їх діджиталізації, корпоративна інформація стала запорукою успіху будь-якої організації. Тому захист даних та стабільність технологічної інфраструктури є першочерговим завданням для підприємств.

Інформація вважається захищеною, якщо зберігається:

* Цілісність - неможливість модифікації інформації неавторизованим користувачем;
* Конфіденційність - інформація не може бути отримана неавторизованим користувачем;
* Доступність - полягає в тому, що авторизований користувач може використовувати інформацію відповідно до правил, встановлених політикою безпеки не очікуючи довше заданого (прийнятного) інтервалу часу.[2]

Для забезпечення захисту корпоративної інформації компанії можуть використовувати різні методи вдосконалення систем.

Політика паролів і аутентифікація, шифрування. Аутентифікація - це процес

перевірки ідентичності користувача або пристрою. В компанії звичною практикою є VPN-з’єднання, яке не тільки шифрує дані, а й є частиною аутентифікації користувачів. Також, при реєстрації в систему важливим є придумати надійний пароль. Для цього використовується нативна підказка користувачеві, для забезпечення надійності паролів.

Антивірусне програмне забезпечення. Використання антивірусного

програмного забезпечення для виявлення та видалення шкідливого програмного забезпечення та вірусів, що можуть призвести до витоку інформації та пошкодження цілісності даних.

Резервне копіювання даних. Зашкодити можливо не тільки вкравши дані, а

й знищивши їх в першоджерелі або ж атакувавши з ціллю відмови в обслуговуванні серверів. Для швидкого відновлення системи зберігаються резервні копії даних та налаштування серверів.

Так як інформаційна безпека залежить також від цілісності апаратного

забезперчення, важливою є також фізична безпека. Захист фізичного доступу до обладнання і серверних приміщень, включаючи захисні системи контролю доступу та відеоспостереження.

Запобігання витоку інформації, її цілісність дуже важлива для установ,

компаній. Адже, при порушенні захищеності даних, вони неминуче зазнають проблем – фінансових, репутаційних та юридичних. Тому, необхідно, всіма можливими методами, деякі з них зазначені вище, захистити важливі дані.

**Література**

1. <https://studfile.net/preview/5064248/page:16/>
2. <https://uk.wikipedia.org/wiki/%D0%97%D0%B0%D1%85%D0%B8%D1%81%D1%82_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%97>