Рудюк Б.М., магістрант,
Єфіменко А.А., к.т.н., доцент
Державний університет «Житомирська політехніка»

СПОСОБИ ЗАХИСТУ ДАНИХ В УМОВАХ ВІДДАЛЕНОЇ ТА ГІБРИДНОЇ РОБОТИ

Поширення пандемії COVID-19 значно змінило робочі процеси в багатьох компаніях, змусивши їх швидко адаптуватися до нових умов. Перехід на віддалену та гібридну роботу став не лише вимогою часу, але й новим викликом для безпеки даних. У таких умовах захист інформації став пріоритетом, оскільки традиційні методи захисту, що базуються на централізованих мережах та фізичних межах офісу стали неефективними.

В умовах віддаленої та гібридної роботи важливим завданням є забезпечення конфіденційності та цілісності даних, що передаються через мережі та зберігаються на різноманітних пристроях, зокрема, персональних комп'ютерах, мобільних телефонах та інших гаджетах.

Одним із найбільш ефективних способів забезпечення безпеки є впровадження моделі Zero Trust, яка передбачає, що жоден пристрій чи користувач не можуть автоматично отримати доступ до корпоративних ресурсів. Кожен запит на доступ до ресурсів має бути перевірений і автентифікований на кожному етапі, що значно знижує ризики внутрішніх загроз і атак. Окрім того, використання багатофакторної аутентифікації (MFA) є важливим елементом захисту, оскільки кожен запит на доступ має супроводжуватися кількома рівнями підтвердження особи.

Іншим важливим методом є шифрування даних. Це дозволяє захистити інформацію навіть у разі її перехоплення або фізичного доступу до пристроїв. Застосування шифрування є ключовим для забезпечення конфіденційності в умовах, коли співробітники працюють з дому або в інших локаціях, що не підлягають контролю організації.

Не менш важливим елементом є моніторинг мережевої активності. Використання інструментів для виявлення та запобігання вторгненням дозволяє оперативно реагувати на будь-які підозрілі дії в мережі. Адаптація до постійно змінюваних умов кіберзагроз вимагає інтеграції новітніх систем, які використовують машинне навчання та штучний інтелект для автоматичного виявлення аномалій та підозрілих дій. Ці системи дозволяють своєчасно виявляти потенційні загрози, навіть якщо вони ще не були виявлені традиційними методами.

Крім того, в умовах віддаленої роботи компанії повинні звернути увагу на захист віддалених робочих місць за допомогою VPN, що забезпечує безпечне з'єднання між співробітниками та корпоративними ресурсами. Ці інструменти дозволяють захистити трафік від перехоплення через публічні мережі або нестабільні канали зв'язку, що часто використовуються в умовах віддаленої роботи.

Також важливим аспектом є управління доступом до даних. Це включає в себе не лише контроль за доступом до корпоративних ресурсів, а й ретельну перевірку прав доступу до конфіденційної інформації. Забезпечення мінімально необхідного доступу до інформації допомагає знизити ризики витоків даних, якщо пристрої чи акаунти співробітників будуть зламані.

Не менш важливим є впровадження навчання для співробітників, спрямованих на покращення їхньої обізнаності щодо сучасних кіберзагроз, таких як фішинг, соціальна інженерія та інших видів атак. Постійне навчання персоналу дозволяє зменшити вразливість організації до загроз, пов'язаних з людським фактором.

Відновлення даних після інцидентів також є важливим аспектом кібербезпеки. Регулярне резервне копіювання даних та впровадження стратегії відновлення після катастроф дозволяє організаціям оперативно відновлювати свою діяльність після зловмисних атак. Крім того, регулярне оновлення програмного забезпечення і антивірусних систем знижує ризики заразитись шкідливим програмним забезпеченням.

Загалом, забезпечення безпеки даних в умовах віддаленої та гібридної роботи вимагає комплексного підходу, що поєднує передові технології захисту, ефективне управління доступом та активну роль співробітників у підтримці інформаційної безпеки. Організації мають запроваджувати багаторівневі стратегії, які гарантують надійний захист даних у будь-яких умовах. Таким чином, забезпечення безпеки даних в умовах віддаленої та гібридної роботи є не просто викликом, а важливим аспектом успішного функціонування сучасних організацій, який потребує комплексного і системного підходу.

Список використаних джерел

1. Remote Work Security: Safeguarding Your Data and Privacy. RemotePass: Global HR & Payroll Platform | Hire, Pay, and Manage Teams Worldwide. URL: https://www.remotepass.com/blog/remote-work-security

2. Data Protection for Remote Workers. Dasera | Automated Data Security and Governance Controls. URL: https://www.dasera.com/blog/data-protection-for-remote-workers