Список використаних джерел:

1. Міністерство цифрової трансформації України. Офіційний сайт. – https://thedigital.gov.ua
2. Кіберполіція України. Аналітичні матеріали та новини. – https://cyberpolice.gov.ua
3. NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). Reports. – https://ccdcoe.org
4. Symantec. Internet Security Threat Report. – https://symantec.com
5. FireEye Mandiant. Cyber Security Reports. – https://www.mandiant.com
6. CERT-UA (Computer Emergency Response Team of Ukraine). Офіційні публікації. – https://cert.gov.ua
7. Закон України «Про основні засади забезпечення кібербезпеки України» (2017 р.).
8. Офіційний сайт Ради національної безпеки і оборони України – www.rnbo.gov.ua.
9. ENISA. Reports on Critical Infrastructure Protection.
10. Symantec. Internet Security Threat Report.
11. Zetter K. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon.* – 2014.

Стрельцова Кіра Юріївна
Студентка н.гр. 105_СПД ННІ права та психології НАВС

Науковий керівник:
Хахановський Валерій Георгійович
доктор юридичних наук, професор, професор кафедри інформаційних технологій ННІ права та психології НАВС

КІБЕРБЕЗПЕКА БІЗНЕСУ: ВІД МАЛОГО ДО ВЕЛИКОГО

Сьогодні кібербезпека стала однією з ключових умов стабільності бізнесу незалежно від його масштабу. Малі, середні та великі підприємства дедалі частіше стають мішенню кіберзлочинців, адже дані, ресурси та фінансові активи є об'єктом особливої цінності.

Мета даної роботи – розглянути виклики та підходи до забезпечення кібербезпеки бізнесу на різних рівнях його розвитку.

Під *кібербезпекою* розуміють комплекс заходів, спрямованих на захист інформаційних систем, мереж, даних і цифрових активів від несанкціонованого доступу, кібератак, витоку інформації та інших загроз. Для бізнесу кібербезпека має стратегічне значення, адже інциденти у сфері безпеки можуть призвести до фінансових збиків, втрати репутації, а також до юридичної відповідальності.

Серед найбільш поширених кіберзагроз для підприємств є:

- фішингові атаки та соціальна інженерія;
- віруси, шпигунське програмне забезпечення та програми-вимагачі;
- несанкціонований доступ до корпоративних даних;
- витік конфіденційної інформації через внутрішні помилки співробітників;
- DDoS-атаки, що паралізують діяльність компаній.

Кожна з цих загроз може завдати бізнесу значних збитків, особливо якщо не існує плану реагування.

Малі підприємства зазвичай мають обмежені ресурси, тому кібербезпека часто недооцінюється. Проте саме вони стають легкою мішенню для хакерів.

Основні кроки для захисту малого бізнесу:

- впровадження базових правил кібергігієни (складні паролі, двофакторна автентифікація);
- регулярне оновлення програмного забезпечення;
- навчання персоналу основам інформаційної безпеки;
- використання хмарних сервісів із вбудованим захистом даних.

Середні компанії володіють більшими інформаційними потоками та клієнтськими базами. Для них особливо важливим є:

- розробка політик безпеки та внутрішніх регламентів;
- впровадження систем моніторингу та виявлення інцидентів;
- сегментація корпоративної мережі;
- створення резервних копій і планів відновлення даних.

Завдяки системному підходу середній бізнес може не лише захистити свої активи, а й підвищити довіру клієнтів.

Великі корпорації часто стають мішенню цілеспрямованих атак, спрямованих на фінансову вигоду чи промислове шпигунство.

Тут необхідні комплексні рішення, а саме:

- створення окремих відділів кібербезпеки;
- використання інноваційних технологій (штучний інтелект для виявлення аномалій);
- постійні аудити та тестування на проникнення;
- співпраця з державними структурами та міжнародними організаціями.

У країнах ЄС та США кібербезпека бізнесу регламентується законодавством, що передбачає сувору відповідальність за витік персональних даних.

Прикладом цього є Загальний регламент із захисту даних (GDPR), який зобов’язує компанії дотримуватися високих стандартів безпеки.

Для України важливим є гармонізація власних законодавчих норм із міжнародними стандартами.

Майбутнє кібербезпеки тісно пов'язане з розвитком новітніх технологій:

- використання штучного інтелекту та машинного навчання;
- впровадження блокчейн-технологій для безпечних транзакцій;
- підвищення ролі кіберосвіти серед працівників;
- створення культури безпеки як невід'ємної частини бізнес-процесів.

Отже, кібербезпека є невід'ємним елементом сучасного бізнесу незалежно від його масштабів. Малі компанії повинні приділяти увагу базовим заходам захисту, середні – впроваджувати системні підходи, а великі корпорації – інвестувати у комплексні рішення та міжнародну співпрацю.

Тільки так, на наш погляд, можна зменшити ризики та забезпечити стійкість бізнесу у цифрову епоху.

Список використаних джерел:

1. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII.
2. Загальний регламент захисту даних (General Data Protection Regulation, GDPR). Regulation (EU) 2016/679.
3. National Institute of Standards and Technology (NIST). Cybersecurity Framework. U.S. Department of Commerce, 2020.
4. International Telecommunication Union. Global Cybersecurity Index 2021.
5. Symantec. Internet Security Threat Report. Vol. 24, 2022.
6. ENISA (European Union Agency for Cybersecurity). Cybersecurity Threat Landscape 2023.
7. Кудінов, С. С. Кібербезпека в умовах цифровізації бізнесу: виклики та рішення // Науковий вісник ХНУВС, 2022. С. 34-37.
8. Гаврилюк, О. П. Інформаційна безпека підприємств: проблеми та шляхи їх вирішення // Економіка і суспільство, 2021.
9. PwC. Global Digital Trust Insights 2024: Cybersecurity trends.
10. Cisco. Cybersecurity Annual Report 2023.