УДК 004.49

КІБЕРЗАГРОЗИ ТА БЕЗПЕКА: СУЧАСНИЙ СТАН

Барташевська Ю.М., канд. екон. наук, доцент, bartashevska@duan.edu.ua
Університет імені Альфреда Нобеля

Сучасний стиль життя всього світу та України – цифровізація усіх сфер життя. Тому завдання збереження критично важливих даних, функціонування операторів зв'язку, банківських систем та мереж є критично важливими, а кібербезпека сьогодні стала невід'ємною частиною нашого життя.

Новини про чергову скомпрометовану мережу стали звичними. А з пошуком «мережеві атаки», відкривається безліч посилань на статті про кібератаки, що здійснюються на державні установи та інші організації, витоки інформації тощо [1].

Збереження безпеки мережі вимагає пильності з боку фахівців із мережевої безпеки державних органів та комерційних структур, які є учасниками (користувачами) системи. Вони мають бути постійно в курсі нових мережевих загроз та атак, що розвиваються, а також вразливостей пристроїв і додатків.

Міністерство внутрішньої безпеки США та Національний центр кібербезпеки Сполученого Королівства відзначили, що вони відчувають величезне зростання фішингу, поширення шкідливого програмного забезпечення, реєстрації нових доменів, атаки на інфраструктури віддаленої роботи з використанням приманок на тему COVID-19.

При цьому витрати на кібербезпеку у світі сягають шалених цифр.

У 2020 році обсяг ринку інформаційної безпеки або кібербезпеки склав 156,24 млрд. доларів США. Очікується, що до 2026 року він досягне 352,25 млрд доларів, за середньорічного темпу зростання – 14,5%. Тенденції IoT (інтернету речей), BYOD («принеси свій власний пристрій»), AI (штучного інтелекту) та машинного навчання в інформаційній безпеці зростуть. За даними Центру стратегічних і міжнародних досліджень США і McAfee, кіберзлочини, які включають пошкодження та знищення даних, крадіжку грошей, втрату власності, крадіжку інтелектуальної власності та ін. складають 8% від усього світового ВВП. Впровадження M2M (міжмашинної взаємодії), IoT-з'єднань стимулюють ринок інформаційної безпеки, оскільки нові бізнес-моделі та програми орієнтовані зниження витрат і зростання кількості підключених пристроїв (автомобілів, лічильників, побутової електроніки та інших.).

Однак цифри у звітах про кіберзлочинність, зазвичай, сильно занижені, тому статистика досить далека від реальної картини. Згідно з дослідженнями, щорічно, більше 70 млн. людей у світі стають жертвами кіберзлочинів. Тобто, кожен сотий житель планети стає жертвою кіберзлочинців.

Трійка країн-лідерів з найбільшими втратами на рік від кібератак зараз виглядає наступним чином:

- США: збитки 28 мільярдів доларів;
- Бразилія: збитки понад 26 мільярдів доларів;
- Велика Британія: збитки 17,4 мільярда доларів.

Найбільш поширеними зараз є цільові атаки (DDoS-атаки і фішингові кампанії), онлайн-шахрайство з використанням підроблених веб-сторінок і троянських програм. Найбільш популярними у хакерів залишаються програми-вимагачі [2]. За допомогою них хакери шифрують файли жертв і вимагають викупу для їх розшифровки. Це може бути особливо руйнівним для бізнесу, оскільки може привести до втрати важливих даних. Зростає число політичних та ідеологічних кібератак. Мотивом такої атаки може бути бажання порушити роботу організації або уряду, або публічно спаплюжити їх ім'я. Іноді подібні атаки можуть бути дуже руйнівними.

Також очікується, що до 2025 р. у світі буде близько 30 розумних міст, 50% з яких будуть розташовані в Північній Америці та Європі. Це вимагатиме вживання ефективних заходів щодо інформаційної надійності.

Розглянемо ситуацію з кібербезпекою і кіберзахистом в Україні.

Так за загальнодержавним рейтинг кіберзахищеності у 2020 р. Україна займала 50 позицію (серед 108 країн) з індексом 0.569, демонструючи дуже високий рівень схильності до кіберзагроз (відповідно, дуже низький рівень кіберзахищеності). Про це свідчать дані дослідження PasswordManagers.co [3]. Це місце Україні «забезпечили» близько 1 мільйона випадків кіберзагроз. Серед яких – мережеві атаки, спроби мережевого сканування, спроби WEB-атак, фішинг, DDoS-атаки, поширення шкідливого програмного забезпечення (РНБО, [4]). А відповідно до Глобального індексу з кібербезпеки (GCI) за 2020 рік від ITU Україна займає лише 78 позицію із 182 країн індексу. У 2021 р. за Глобальний індексом з кібербезпеки для України становив 65.9.

Статистика за 2022 р. свідчать, що упродовж перших 1,5 місяців повномасштабної війни в Україні зафіксували 362 кібератаки. Це утричі більше, ніж у такий самий період попереднього року. Половина цих атак була спрямована на уряд, місцеві органи влади, сектор безпеки й оборони та комерційні організації, щоб викрасти дані та встановити шкідливий програмний код. Атаки на ІТ-компанії становлять лише 6% від загальної кількості інцидентів [5].

У 2023 р. ці дані стали ще більше. За даними Державного центру кіберзахисту Держспецзв'язку тільки у ІІІ кварталі 2023 р. зареєстровано 355 кіберінцидентів, що на 46% вище, ніж у другому кварталі того ж року. Основні сфери спрямування – фінансовий, урядовий, телекомунікаційний, освітній сектори, а також громадські організації.

Отже, статистика кіберзагроз в Україні та світі говорить про їх невпинне зростання, а нажаль – і збільшення втрат від них. За прогнозами спеціалістів у 2024 р. у світі очікується збільшення кількості кіберінцидентів мінімум на 15%,

а основними типами атак будуть: фішингові, DDoS-атаки та використання програм-вимагачів і додатків-вимагачів.

Список використаних джерел

1. Витрати на кібербезпеку. Очікування та реальність. URL: https://www.intrasystems.ua/novini/vytraty-na-kiberbezpeku-ochikuvannya-ta-realnist/
2. Рейтинг країн світу за рівнем схильності до кіберзагроз 2020. URL: https://10guards.com/ru/articles/global-cybersecurity-exposure-index-2020/
3. В Україні в 2020 році зафіксували 1 мільйон кібератак – РНБО. URL: https://ms.detector.media/kiberbezpeka/post/25227/2020-08-07-v-ukraini-v-2020-rotsi-zafiksuvaly-1-milyon-kiberatak-rnbo/
4. Вітченко В. Чи добре українська IT-індустрія захищена від кібератак? Аналіз перших місяців війни та поради для бізнесу від N-iX. URL: https://speka.media/kiberbezpeka/ci-postrazdala-it-industriya-vid-kiberatak-analiz-ta-poradi-poradi-biznesu-vr8009
5. Биков В.Ю., Буров О.Ю., Дементієвська Н.П. Кібербезпека в цифровому навчальному середовищі. Інформаційні технології і засоби навчання, 2019, Том 70, №2. С. 313-331.