КІБЕРБЕЗПЕКА ЯК ОДИН ІЗ КЛЮЧОВИХ АСПЕКТІВ СУЧАСНОГО ЖИТТЯ

Проценко Н.М., к.е.н., доц.
Грабельник В.М., здобувач РВО бакалавр
Державний біотехнологічний університет
м. Харків, Україна, pronatanic@gmail.com

Анотація: В умовах постійного зростання глобальних загроз в галузі інформаційного захисту інформації збільшення рівня кіберзлочинів повною мірою впливає на безпеку як на макрорівні, так й на мікрорівні, завдаючи істотних збитків об'єктам інформаційної інфраструктури. Тому виявлення факторів забезпечення кібербезпеки у всіх сферах життя суспільства є невідкладною необхідністю сьогодення.
Ключові слова: кібербезпека, кіберпростір, інформація, кіберзлочини, втрати, кібератаки

Реалії сьогодення такі, що кіберпростір – це вже не просто середовище спілкування людей, різноманітні ігри, сховища знань (бібліотеки) тощо. Кіберзасоби (кіберзброя) – це самостійний вид озброєнь, здатних завдати ефективного удару, який можна порівняти за результатами з ядерним ударом, і залишитися при цьому невиявленим і невидимим для противника. Тому питання кібербезпеки відіграють велику роль у сучасному житті і є дуже актуальними.

Відповідно до українського законодавства, кібербезпека – це захищеність життєво важливих інтересів людини й громадянина, суспільства та держави у процесі використання кіберпростору [1].

Зазначимо, що поняття кібербезпеки включає безліч проблем різного типу, а також ще більше число рішень. Загрози у кіберпросторі є найбільш серйозними для національної та економічної безпеки, з якими стикаються держави. Шкода, яку завдає кіберзлочинність, виміряється мільярдами та росте з кожним роком. Кібератаки стають засобом боротьби проти держави, руйнують комунікацію та економіку.

У сучасній економіці кіберзлочинність переходить у приватну та комерційну площину і безумовно кібербезпека найбільше пов'язана з Інтернет-безпекою. Основними об'єктами більшості кібератак стають комерційні організації. Мета таких нападів отримання відповідної інформації або отримання будь-яких преференцій. Наприклад, економіка Німеччини є дуже привабливою мішенню для злочинців і ворожих держав. Згідно з даними опитування Bitkom, яке включає понад 1000 компаній, у 2023 році збитки перевищали позначку у 200 млрд євро, і така ситуація спостерігається вже третій рік поспіль. Близько 52 % опитаних на запитання чи кібератаки загрожують існуванню їхньому бізнесу відповіли ствердно. Якщо порівняти 2022 і 2021 роки, то у 2022 році ця цифра становила 45 %, а у 2021 р. 9 %. З компаній, які зазнали атак в 2023 р., у 70 % були викрадені конфіденційні дані (у 2022 р. цей показник дорівнював 63 %); шпигунству за цифровими комунікація піддавалися 61 % компаній (відповідно попереднього року 57 %) [2]. За дослідженням, що проведено експертами антивірусної компанії McAfee

спільно з Центром стратегічних міжнародних досліджень, в середньому збитки від дій хакерів у всьому світі оцінюються в 600 мільярдів доларів щорічно [3].

Також важливою метою кіберзлочинців є особисті дані окремих фізичних осіб. Практично кожна людина, яка є користувачем Інтернету, розміщує в мережі та зберігає на своїх пристроях величезну кількість важливої інформації про своє приватне життя та професійну діяльність.

Фахівці з кібербезпеки стверджують, що хакери, використовуючи особисті селфі, знаходять досить багато інформації, яка дозволяє ідентифікувати особистість. Також для кіберзлочинців цікавими є історії браузера, IP-адреси та багато інших особистих документів (дані про освіту, сертифікати та ліцензії для ведення бізнесу тощо). Уся ця запозичена інформація може бути використана для отримання власної вигоди без на те згоди чи дозволу збоку людину.

У 2023 році компанія Panda Security, що спеціалізується на рішеннях для забезпечення інформаційної безпеки, повідомила про нову кіберзлочинну схему, жертвами якої стають користувачі системи інтернет-бронювання готелів Booking.com. Зловмисники крадуть персональні дані, а потім, використовуючи викрадені облікові відомості, звертаються до клієнтів платформи з проханням оплатити фіктивні рахунки. При цьому користувачі перенаправляються на підроблені веб-сайти, що призводить до крадіжки.

Серед найпоширеніших кіберзлочинів у США, що склали загальну суму втрат в розмірі $4 млрд в 2021 р., третє місто посідають втрати, які пов’язані з викраденням персональних даних ($51,829 млн) [2].

У 2022 році найбільш атакованим став Азіатсько-Тихоокеанський регіон: на нього припав 31 % від загальносвітового числа кібератак, 24 % успішних атак були спрямовані на приватних осіб. У липні 2023 року стало відомо про витік даних понад 300 мільйонів жителів Індонезії, ймовірно, із системи Dukcapil. Серед даних, що були вкрадені, ідентифікаційні номери громадян, контактні телефони, електронні адреси, домашні адреси [4]. На сьогоднішній момент індивідуальна кібербезпека для багатьох є однією з найактуальніших і хвилюючих тем.

Слід зазначити, що відбувається поступова зміна характерної ознаки вибору мети кіберзлочинців в середньостроковій перспективі спостерігається масове збільшення атак на сервери з метою їх дестабілізації. Разом з тим, можлива поява нового типу кібератак – це створення перешкод, щоб користуватися IT-системою було фізично неможливо. Тобто об’єктами кібератак стає не інформація, що зберігається в системі, а функціональність самої IT-системи. Зокрема, найбільш популярними є DoS-атаки, коли кіберзлочинці створюють надлишкове навантаження на мережі та сервери відповідного об’єкта. В разі успішних дій зловмисників втрати можуть бути величезними, адже DDoS-атаки фактично зупиняють роботу, доки атаку не буде виявлено й усунене. А це означає втрату продуктивності, продажів і зниження якості обслуговування клієнтів. А ще є репутаційний чинник, який може позначитися на бізнесі на місяці чи роки наперед [5].

Підводячи підсумки, варто підкреслити, що кібербезпека є складною і постійно мінливою областю. Вона вимагає постійної уваги та розвитку з боку організацій, державних органів та окремих користувачів, щоб забезпечити безпеку інформації та даних у нашому цифровому світі.

Для ефективного захисту від кіберзагроз необхідно застосування комплексного підходу, що поєднує технічні заходи, навчання персоналу та дотримання відповідних політик безпеки.

Важливим фактором захисту від кіберзагроз є усвідомлення всіх учасників цифрового простору, що безпека це спільна справа. Відсутність обміну даними кібератак на державні організації та суб'єкти приватного бізнесу, підприємців, фізичних осіб, відсутність детального дослідження та розробки адекватних інструментаріїв протидії, організованого обміну інформацією та системи консультацій збільшує ймовірність напрямів кіберзагроз та дій хакерів та інших кіберзлочинців. Компанії та організації повинні співпрацювати між собою та з урядовими структурами для обміну інформацією про загрози та нові методи захисту. Крім того, освітні програми з кібербезпеки для широкої аудиторії допоможуть підвищити обізнаність користувачів та знизити ймовірність успішних атак, пов'язаних із людським фактором.

У сучасному світі на всіх рівнях людської життєдіяльності необхідне чітке усвідомлення того, що, незважаючи на всі зусилля, кібербезпека є однією з найскладніших і найдинамічніших областей. Кіберзлодії постійно знаходять нові вразливості та розробляють нові методи атак, що потребує постійного вдосконалення та адаптації методів захисту. Тому майбутнє кібербезпеки залежатиме від готовності суспільства та індивідуальних користувачів протистояти загрозам та застосовувати передові технології для захисту даних та інформаційних ресурсів.

Список літератури

1. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. Ст. 1. URL: https://kodeksy.com.ua/pro_osnovni_zasadi_zabezpechennya_kiberbezpeki_ukrayini/1.htm.

2. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О. Довгань; упоряд. О. Довгань, Л. Литвинова, С. Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В.І.Вернадського. К., 2023. №9 (вересень). 351 с. URL: https://ippi.org.ua/sites/default/files/2023-9.pdf.

3. Світові збитки від кібератак. *Економічна правда*. URL: https://www.epravda.com.ua/ ua /news/2018/02/22/634346/.

4. The statistics portal. URL: https://www.statista.com/statistics/184083 /commonly-reported-types-of-cyber-crime-us/.

5. Белов Д. DDOS-атаки на вашу інтелектуальну власність: чим загрожують і як від них захиститися. *Дзеркало тижня*. URL: https://zn.ua/ukr/tech/ddos-ataki-na-vashu-intelektualnu-vlasnist-chim-zahrozhujut-i-jak-vid-nikh-zakhistitisja.html.