УДК 004.056.5

АНАЛІЗ КІБЕРАТАК ОСТАННІХ РОКІВ: УРОКИ ДЛЯ ЗАХИСТУ

Наталія Чернящук, Катерина Клещевник

ANALYSIS OF CYBERATTACKS OF RECENT YEARS: LESSONS IN SELF-PROTECTION

Nataliia Cherniashchuk, Kleshchevnyk Kateryna

Волинський національний університет імені Лесі Українки, просп. Волі, 13, Луцьк, 43025, Україна

Abstract. *This paper analyzes major cyberattacks of recent years, focusing on their impact, strategies used by attackers, and the key lessons learned for improving cyber defense. High-profile incidents such as the NotPetya attack (2017), the SolarWinds breach (2020), the Viasat disruption during the Russian invasion of Ukraine (2022), and ransomware campaigns like the Colonial Pipeline attack (2021) are examined to illustrate the evolving nature of cyber threats. The study emphasizes the vulnerability of critical infrastructure, the importance of supply chain security, and the growing role of state-sponsored cyber operations. It also highlights Ukraine's experience in cyber defense during hybrid warfare, underscoring the value of international cooperation, zero-trust models, proactive threat detection, and public cyber hygiene.*

У другому десятилітті XXI століття кібератаки стали серйозною загрозою як для держав, так і для приватного сектору. Вони перетворилися з поодиноких технічних інцидентів на інструмент стратегічного впливу в політиці, економіці та безпеці. Одним із переломних моментів у світовому розумінні масштабів кіберзагроз стала атака вірусу NotPetya в 2017 році, яка почалась з ураження українського програмного забезпечення для бухгалтерського обліку M.E.Doc і швидко поширилась на міжнародні компанії – Maersk, Rosneft, FedEx та інші.

Збитки перевищили 10 мільярдів доларів, що зробило NotPetya однією з найбільш руйнівних кібератак в історії. Уроком цієї атаки стало розуміння, що ланцюги постачання ІТ-продуктів є вразливим місцем і можуть використовуватись для масштабного ураження.

Протягом останніх років росія активно використовує кіберзброю проти України в умовах гібридної війни. У 2022–2023 роках Державна служба – спеціального зв’язку та захисту інформації України зафіксувала понад 2 500 кібератак, більшість з яких були спрямовані на критичну інфраструктуру, зокрема енергетику, транспорт, телекомунікації та урядові структури.

Однією з найбільш резонансних стала атака на систему супутникового зв’язку Viasat напередодні повномасштабного вторгнення РФ. Цей інцидент не лише спричинив втрату зв’язку для українських військових, а й вивів з ладу модеми по всій Європі. Уроком з цього випадку стало усвідомлення важливості резервних каналів зв’язку та диверсифікації залежності від окремих провайдерів.

Не менш показовою була атака на SolarWinds у США у 2020 році, яку приписують російському угрупованню APT29 (Cozy Bear). Хакери зуміли інфікувати програмне забезпечення для моніторингу мереж Orion, яким користувались понад 18 000 клієнтів, включаючи урядові агентства США.

Атака залишалась непоміченою понад 9 місяців. Вона стала уроком про вразливість до зловживань довірою в ІТ-ланцюгах та необхідність постійного моніторингу навіть

авторизованих систем. Це також стало імпульсом для переходу до моделі Zero Trust, яка базується на принципі «не довіряй – перевіряй».

Ще одним напрямом розвитку загроз стали програми-вимагачі (ransomware). У 2021 році атака на Colonial Pipeline у США паралізувала постачання палива на Східному узбережжі, а кіберугруповання DarkSide отримало викуп у розмірі понад 4 млн доларів у біткоїнах.

Ці події підтвердили, що навіть приватні компанії, які забезпечують критичні послуги, можуть стати об'єктом атак, і підкреслили потребу в міжвідомчій координації кіберзахисту. Окрема увага заслуговує на атаки, спрямовані на дестабілізацію громадської думки, зокрема через соціальні мережі.

Прикладом є діяльність російських «фабрик тролів», які у 2016–2020 роках активно втручались у вибори в США, ЄС та інших країнах через дезінформацію, маніпуляції з контентом і соціальну інженерію. Цей тип атак виявився важко відстежуваним і масовим, що створило потребу у нових регуляторних механізмах для онлайн-платформ.

Водночас, Україна за роки війни продемонструвала високий рівень адаптації та формування ефективної кібероборони. Успішна діяльність спільноти волонтерів-кіберзахисників, зокрема ІТ-армії України, які здійснювали атакувальні операції у відповідь, засвідчила важливість кібермобілізації суспільства. Також налагоджено співпрацю з такими партнерами, як Microsoft, Google, Amazon, які допомагають забезпечити стійкість до атак та захист хмарних даних.

Ключові уроки останніх років можна узагальнити наступним чином. По-перше, необхідне постійне оновлення нормативної бази та технічних стандартів у сфері кібербезпеки. По-друге, важливим є розвиток національного кадрового потенціалу через освітні програми, сертифікацію спеціалістів і стимулювання внутрішньої ІТ-індустрії.

По-третє, держава має інвестувати у кіберзахист критичної інфраструктури – через системи виявлення інцидентів, центри реагування (CSIRT/SOC), резервні канали комунікації. І, нарешті, має бути розвинена культура кібергігієни серед громадян – адже навіть найкращі технології без свідомої поведінки користувачів залишаються вразливими.

Протягом останніх років кібератаки перетворилися на потужний інструмент впливу в геополітичних конфліктах, економічному шантажі та інформаційній війні. Інциденти, що відбулися з 2017 року, продемонстрували зростаючу складність атак, їхню спрямованість на критичну інфраструктуру та використання державами як засобу досягнення стратегічних цілей.

Водночас Україна демонструє високий рівень адаптації та розвитку кібероборони. У 2022 році було створено ІТ-армію України – спільноту волонтерів, яка здійснює як захисні, так і наступальні кібероперації.

У 2023 році запущено платформу Brave1, яка об'єднує інноваційні компанії для розробки технологій, спрямованих на посилення обороноздатності країни. Серед розробок – системи радіоелектронної боротьби, захисту від дронів та інші інноваційні рішення. Також впроваджено систему ситуаційної обізнаності Delta, яка забезпечує інтеграцію розвідданих та координацію дій на полі бою.

Отже, аналіз кібератак останніх років свідчить про стрімку еволюцію загроз, зростаючу складність інструментів атаки та системність використання кіберпростору як полігона для геополітичного впливу.

Атаки типу NotPetya, SolarWinds, Colonial Pipeline, а також численні кібероперації проти України з 2022 року чітко демонструють, що кібервійна вже давно вийшла за межі технічної площини і стала ключовим елементом національної безпеки. Критична інфраструктура, державні установи, приватний сектор та навіть особисті пристрої громадян – усе це перетворилося на ціль у глобальному кіберпросторі.

З кожною новою атакою стає очевидним, що класичні підходи до кіберзахисту – вже недостатні. Вони потребують трансформації у напрямі Zero Trust архітектури, використання штучного інтелекту для виявлення аномалій, автоматизації аналізу загроз, а також розбудови систематичних процесів управління ризиками, з урахуванням фактору ланцюгів постачання та людського фактору. Український досвід оборони від кібератак в умовах війни доводить, що кіберстійкість можлива навіть за найскладніших обставин. Це досягається завдяки інтеграції зусиль держави, IT-волонтерів, приватного сектору, міжнародної співпраці та швидкому впровадженню інновацій.

Сучасні тенденції, зокрема використання програм-вимагачів як сервісу (Ransomware-as-a-Service), атаки на supply chain, націлення на інфраструктури 5G, хмарні середовища та штучний інтелект, вимагають нового рівня готовності. Кібербезпека повинна розглядатися як безперервний процес, де превентивні дії, навчання персоналу, прозора політика оновлень і чітка стратегія реагування – обов'язкові складові захисту.

Таким чином, уроки останніх років однозначні: країни, організації та окремі користувачі мають постійно оновлювати свої підходи до захисту в кіберпросторі, впроваджувати принципи кібергігієни на всіх рівнях і формувати цифрову культуру безпеки як основу стійкості у світі, де кібератака може бути потужнішою за ракетний удар.

Бібліографія

1. MIT Technology Review, "A major ransomware attack on MOVEit has hit dozens of victims already", 2023 https://www.technologyreview.com (дата звернення: 17.05.2025).
2. Kaspersky Securelist, "Operation Triangulation – iOS spyware campaign exposed", 2023 https://securelist.com/operation-triangulation (дата звернення: 17.05.2025).
3. The Guardian, "Marks & Spencer and Co-op targeted by cyber-attacks using fake staff calls", April 2025 https://www.theguardian.com (дата звернення: 17.05.2025).
4. Politico Europe, "France accuses Russia of cyberattacks ahead of 2024 Olympics", 2024 https://www.politico.eu (дата звернення: 17.05.2025).
5. BBC News, "British Library ransomware hackers post 600GB of data online", 2023 https://www.bbc.com/news (дата звернення: 17.05.2025).
6. BleepingComputer, "Niconico confirms data breach after ransomware attack", 2024 https://www.bleepingcomputer.com (дата звернення: 17.05.2025).
7. Europol, "LockBit ransomware group disrupted by international law enforcement operation", 2024 https://www.europol.europa.eu (дата звернення: 17.05.2025).