УДК 621.396

Олег Рустемович Черняк *(начальник управління)*
Олег Владиславович Федулов *(заступник начальника служби)*

Військова частина А0515

ТЕНДЕНЦІЇ РОЗВИТКУ КІБЕРЗАГРОЗ У СВІТОВОМУ ІНФОРМАЦІЙНОМУ ПРОСТОРІ

Для захисту інформаційних систем від кіберзагроз (атак) необхідно постійно проводити аналіз та оцінку ризиків їх існування в світовому інформаційному просторі, які впливають на конфіденційність, цілісність та доступність інформаційних ресурсів. Проведено аналіз і виявлення основних тенденцій розвитку кіберзагроз у світовому інформаційному просторі, за результатом якого можна дійти висновку, що тенденції розвитку кіберзагроз збільшуються та ускладнюються механізми їх розповсюдження.

Ключові слова: *кіберзагрози, кібератаки, безпека Інтернет.*

Вступ

На цей час доступ до світового інформаційного простору, який в загальному вигляді являє складну сукупність, що реально існує у вигляді глобальної сукупності процесів взаємодії людей, програмного забезпечення та сервісів Інтернет у мережах (включаючи підключення до них технічного обладнання), але яка при цьому не проявляється в будь-якій відомій матеріальній формі та надає можливості отримати перевагу в соціальній, політичній, військовій та економічній сферах. Водночас у глобальній системі пов'язаних мереж (Інтернет) є кіберзагрози (атаки), що впливають на порушення конфіденційності, цілісності, доступності інформації, а також порушення спостережності та керованості інформаційно-телекомунікаційних систем [1].

Глобальна мережа Інтернет є невід'ємною частиною світового інформаційного простору. Ресурси (сервіси) цієї мережі використовують державні органи (силові структури та розвідувальні служби іноземних держав), корпорації, громадяни, які залежно від намірів та мотивації можуть здійснювати:

збір та викрадення інформації з метою використання або перепродажу;

шпіонаж (промисловий) та (або) диверсії;

злом відділених мереж для доступу до інформації та використання їх ресурсів для здійснення кібератак;

порушення роботи мереж за допомогою кібератак та шкідливого програмного забезпечення;

виведення з ладу або використання у своїх цілях важливих об'єктів інфраструктури;

крадіжку персональних даних.

Таким чином, рівень кіберзагроз (атак) в глобальній мережі Інтернет є дуже високим та може реально впливати на інформаційні ресурси держав, корпорацій та фізичних або юридичних осіб.

Постановка проблеми

Проблема існування кіберзагроз (атак) у світовому інформаційному просторі, що впливають на конфіденційність, цілісність та доступність інформаційних ресурсів.

Аналіз останніх досліджень і публікацій

Упродовж останніх років питання регулювання кібернетичного простору вже не є виключно "внутрішньою справою" окремих держав, вони широко досліджуються міжнародними і регіональними інститутами та союзами. Наприклад, проблему кібербезпеки розглядає на міжнародному рівні Міжнародний союз електрозв'язку (МСЕ). На регіональному рівні слід відзначити Європейський центр дослідження проблем безпеки ім. Дж. К. Маршалла, який займається дослідженням питань міжнародної безпеки та оборони, приділяючи значну роль дослідженням питань кібербезпеки країн НАТО, та Центр передового досвіду НАТО з кіберзахисту (CCD COE, у м. Таллінн) [2], який розробив Стратегію кібербезпеки (Strategic Cyber Security) [3]. В Україні системну роботу у сфері кіберзахисту проводить Національний інститут стратегічних досліджень, який проводить дослідження та публікує наукові роботи [4].

Мета написання статті

Аналіз та виявлення основних тенденцій розвитку кіберзагроз у світовому інформаційному просторі.

Основний матеріал

Кіберпростір сьогодні можна розглядати як середовище обробки інформації державного та корпоративного призначення та являє деяку віртуальну сутність, яка не має конкретної матеріальної форми, але проявляється в об'єктивності взаємодії людей і організацій в мережі Інтернет, а також асоційованого з ним технологічного обладнання та мереж. Під безпекою кіберпростору або кібербезпекою мається на увазі безпека цієї віртуальної сутності, цього віртуального світового інформаційного простору. Кібербезпека у свою чергу опирається на такі компоненти (рис. 1):

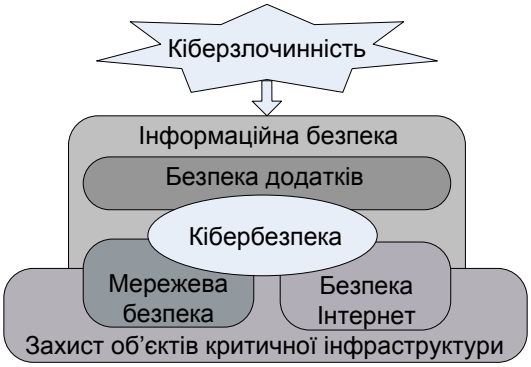

Рис. 1. Позиціонування кібербезпеки

інформаційна безпека – це заходи забезпечення конфіденційності, цілісності та доступності інформації для задоволення потреб користувачів;

безпека додатків – це менеджування ризиків, що застосовується не тільки до самих додатків (їх процесів, компонентів, програмного забезпечення та результатів), але і до даних (даних конфігурації, користувальницьких даних, організаційних даних), а також і до всіх технологій, активностей та акторів, залучених у життєвий цикл додатка;

мережева безпека – це технічний стан мережі, що досягається в процесі її розробки, створення, функціонування і модернізації та гарантує конфіденційність, цілісність і доступність інформації користувачів цієї мережі;

безпека Інтернет – розглядається як розширення поняття мережевої безпеки за рахунок включення до нього захищених Інтернет-залежних сервісів, систем і мереж;

захист ключових інформаційних систем об'єктів критичної інфраструктури розглядається в контексті критично важливих секторів, таких як енергетика, телекомунікації або, наприклад, водопостачання; захист критичної інформаційної інфраструктури передбачає забезпечення гарантії того, що подібні системи та мережі стійкі відносно ризиків інформаційної безпеки, мережевої безпеки, безпеки Інтернет, так само як і ризиків кібербезпеки [5].

Кіберпростір не належить нікому, кожен може знайти в ньому своє місце і мати в ньому свою частку. Персони чи організації в кіберпросторі можна поділити на дві групи: споживачі та провайдери (рис. 2).

Загрози, що існують у кіберпросторі, мають сенс лише в контексті їх прив'язки до активів. Актив являє собою деяку сутність, що має цінність для людини чи організації. Існують різні види активів, наприклад: інформація, комп'ютерне програмне забезпечення, фізичні об'єкти і предмети, послуги, люди та їх кваліфікації, навички та досвід, права та нематеріальні активи, такі як репутація (імідж). Іноді як актив визначають тільки інформацію або ресурси. Стандарт ISO/IEC 15408-1:2005 визначає активи як інформацію або ресурси, що захищаються відповідними заходами, асоційованими з цими активами. Активи можна поділити на два класи: особисті активи та активи організації.

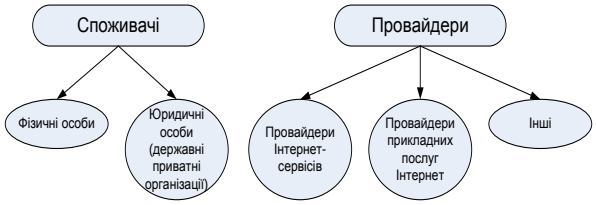

Рис. 2. Суб'єкти кіберпростору

Відповідно до активів загрози в кіберпросторі теж можуть бути розділені на два класи: загрози персональним активам та загрози активам організації.

Загрози персональним активам розглядаються, головним чином, як порушення їх недоторканності, приватності, пов'язані з витоком або розкриттям персональних даних. Наприклад, чорний ринок може стимулювати розкрадання і перепродаж персональних даних, зокрема, відомостей про кредитоспроможність.

Загрози активам організації найбільше впливають на онлайнові представництва організацій і онлайн-бізнес, які здійснюють зловмисники, наміри яких можуть виходити за рамки завдання звичайної майнової шкоди. Відомі факти шантажу організацій загрозою обвалення або порушення нормальної роботи важливих сторінок їх веб-сайтів. Також відомі факти викрадення (перереєстрація) доменних імен організацій і перепродаж їх стороннім особам з метою негативного впливу на імідж та бізнес жертви.

Для організацій існує ризик переслідувань за несанкціоноване розкриття персональних даних своїх співробітників, клієнтів, партнерів або постачальників, які можуть бути викрадені в результаті успішних атак на вразливості в захисті. Фінансові облікові дані організації можуть бути схильні до несанкціонованих спотворень через вразливості в системі авторизації та допуску.

В інформаційних системах державних органів міститься інформація не тільки з питань національної безпеки, оборони, розвідки, стратегічного планування та інших аспектів діяльності органів влади та управління, а й величезні масиви персональних даних, відомості про організації та суспільства в цілому [6].

Отже, порушники і агенти загроз – це окремі індивідууми чи його групи, або навіть держави, котрі грають певні ролі в здійсненні нападу або в його підтримуванні. Розуміння мотивів і спонукань (релігійних, політичних, економічних та ін.), можливостей (знань, розмірів фінансування тощо) і намірів (розваги, шпигунство та ін.) порушників і агентів загроз має вирішальне значення в оцінюванні ризиків, а також у створенні відповідних систем реагування.

Водночас необхідно зазначити, що під вразливістю розуміють слабку ланку в складі активу або системи управління, через яку може бути реалізована загроза. У контексті інформаційних систем документ ISO/IEC TR 19791:2006 визначає вразливості як дефекти,

недоліки чи прорахунки, допущені при проектуванні та реалізації інформаційної системи (включаючи систему безпеки) або існуючі в її оточенні, які можуть бути цілеспрямовано або ненавмисно використані для негативного впливу на активи організації та/або її діяльність.

На цей час значна частина кібератак в кіберпросторі здійснюється з використанням шкідливого програмного забезпечення, такого як програми-шпигуни, черв'яки та віруси, при цьому вихідна інформація часто збирається методами фішингу (виманювання у довірливих або неуважних користувачів мережі персональних або інших даних). Тактика нападу може бути вибудувана в руслі одного вектора кібератаки або у вигляді змішаної кібератаки по різних векторах. Механізм реалізації і просування кібератаки може бути організований, наприклад, на основі сумнівних веб-сайтів, неконтрольованих завантажень, розсилання спаму, віддаленого управління або заражених знімних носіїв. Всі кібератаки можна розділити на дві головні категорії: напад зсередини приватної мережі та напад зовні приватної мережі. Можливі варіанти комбінації кібератак зсередини і зовні приватної мережі.

Відомі механізми реалізації нападів, які будуються на основі маніпуляцій і фальсифікацій у популярних сьогодні соціальних мережах або на базі шкідливих файлів, впроваджених через легальні сайти. Люди схильні потенційно довіряти повідомленням, отриманим від джерел, які вони самі раніше прив'язали до своїх сторінок в соціальних мережах. Це дає зловмисникам можливість вибудувати шляхи кібератаки на основі маскування під легальний контакт.

Законні сайти можуть бути зламані і заражені шкідливими файлами, використовуваними як засоби для здійснення нападів. Люди схильні повністю довіряти часто відвідуваним ресурсам, адреси яких, як правило, збережені в закладках їх Інтернет-браузера, а ще більше – тим сайтам, які використовують механізми безпеки, такі як SSL (Secure Sockets Layer). Але перевірка автентичності та цілісності переданої або одержуваної інформації здійснюється "за місцем" і SSL в цьому плані не робить відмінностей між оригінальним файлом і файлом, спотвореним зловмисником, тим самим піддаючи користувача ризику бути атакованим.

Кібератаки зсередини приватної мережі звичайно ініціюються всередині мережі організації, як правило, в області локальної мережі, будучи справою рук співробітників або персоналу, який має доступ до комп'ютерів або мережі в межах організації або службових приміщень. Можливим варіантом початку кібератаки є зловмисне використання системним адміністратором своїх прав, зокрема, таких як, доступ до паролів користувачів. Однак, сам системний адміністратор може виявитися мішенню отримання інформації (логінів, паролів і т.д.), необхідної для початку цільової кібератаки. Для отримання паролів або іншої персональної інформації атакуючий може використовувати спеціальні засоби, наприклад, сніфери, або ж видавати себе за довірену особу в технології "людина посередині" ("man-in-the-middle").

Також на сьогодні одним з механізмів розкрадання особистих ідентифікаційних даних є створення і використання підробленої точки доступу (далі – ТД). У цьому випадку зловмисник може перебувати, наприклад, в аеропорту, кафе або іншому громадському місці, де пропонується вільний Wi-Fi доступ до Інтернету, маскуючись під законного власника безпроводової точки доступу, використовуючи Service Set ідентифікатори (SSID) службової території. Якщо користувач скористається такою підробленою ТД, зловмисник має можливість діяти як "man-in-the-middle" і отримати всі ідентифікаційні дані, активовані користувачем: ім'я облікового запису, пароль електронної пошти, інформацію про банківські рахунки та паролі доступу до них тощо. Для того щоб мати можливість розкрадати інформацію з незахищеної Wi-Fi мережі, достатньо лише перебувати поряд з мережею, наприклад, в автомобілі за межами службової території.

Комп'ютерна атака всередині приватної мережі може бути ініційована не тільки людиною, а й шкідливим програмним забезпеченням, впровадженим на будь-який комп'ютер цієї мережі. Найчастіше шкідливе програмне забезпечення розсилають у приватній мережі запити для виявлення інших комп'ютерів з метою їх подальшого несанкціонованого використання. Деяке шкідливе програмне забезпечення може ініціювати на заражених комп'ютерах режим прийому всіх мережевих пакетів ("promiscuous mode"), що забезпечує невибірковий режим прослуховування всього трафіка мережі.

Одним з найстаріших, але все ще дуже ефективних механізмів, є сканування портів. Усі порти, доступні на сервері, скануються для виявлення "відкритих" портів. Звичайно це є одним з перших кроків підготовки кібератаки на цільову систему.

З метою отримання даних для несанкціонованого входу в систему і звертання до додатків можуть використовуватися клавіатурні перехоплювачі – апаратні чи програмні засоби, які таємно відстежують всі дії користувача цільової системи і фіксують всі його маніпуляції з клавіатурою.

Найбільш поширеним видом кібератаки на цільову систему можна вважати розподілені DDoS-атаки на сервер додатків або на інше мережеве обладнання (відмова в обслуговуванні). Наприклад, великомасштабна DDoS-атака за допомогою бот-мережі може заблокувати доступ в кіберпростір на рівні країни. Необхідно зазначити, що з розвитком інформаційних систем потужність DDoS-атак постійно збільшується за рахунок використання більших ресурсів для їх здійснення.

Ще одним поширеним механізмом кібератаки на сервери в Інтернеті є атака переповнення буфера. Передаючи на сервер набагато більшу

кількість рядків символів, ніж це припустимо, можна вивести його в неконтрольований режим, що полегшує виконання шкідливого коду.

Іншим прикладом механізму кібератаки, який широко використовується зловмисниками сьогодні, є IP-Spoofing. Його зміст полягає в отриманні доступу до цільової системи за рахунок заміни в IP-повідомленнях власної IP-адреси на IP-адресу джерела, якому довіряє цільова система.

З поширенням peer-to-peer додатків, які забезпечують двом комп'ютерам в мережі можливість прямого обміну файлами через Інтернет, у зловмисників з'являються додаткові можливості маскування під обмін цифровими файлами форматів аудіо, відео, фото та ін.

Висновок

За результатом вищенаведеного аналізу кіберзагроз (атак) у світовому інформаційному просторі можна дійти висновку, що тенденції їх розвитку збільшуються, тобто ускладнюються механізми їх розповсюдження та реалізації (скритності та нових деструктивних властивостей).

До основних видів кіберзагроз можна віднести:

кібератаки на відмову в обслуговуванні;

крадіжку персональних даних та перепродаж цінної інформації;

атаки за допомогою шкідливого програмного забезпечення (розробники, які можуть бути представниками держави, корпорацій, злочинних угруповань тощо);

збір інформації та шпіонаж.

Виявлені тенденції розвитку кіберзагроз пропонуємо враховувати в ході створення комплексних систем захисту інформації в інформаційно-телекомунікаційних системах, а також національної системи кібербезпеки (рішення РНБО України від 08 червня 2012 року "Про нову редакцію Стратегії національної безпеки України", затверджене Указом Президента України від 08 червня 2012 року № 389/2012) [7][8].

Література

1. Голубенко О. Л. Інтернет – як поле бою в інформаційній війні / Петров О. С., Гарагуля М. В. // Вісник Східноукраїнського національного університету ім. В. Даля. – 2010. – № 9 (151), ч. 1. – С. 7–11. **2. Cyber** Security Strategy [Електронний ресурс] // Cabinet Office. – Режим доступу: http://www.ccdcoe.org/publications/books/Strategic_Cyber_Security_K_Geers.PDF. **3. NATO** Cooperative Cyber Defence Centre of Excellence [Електронний ресурс]. – Режим доступу : http://www.ccdcoe.org. **4. Дубов Д. В.** Майбутнє кіберпростору та національні інтереси України: нові міжнародні ініціативи провідних геополітичних гравців: аналіт. доп. / Д. В. Дубов, М. А. Ожеван. – К. : НІСД, 2012. – С. 22. **5. ISO/IEC 27032:2012**, Information technology Security techniques Guidelines for cybersecurity. **6. Конвенція** про кіберзлочинність [Електронний ресурс] // Верховна Рада України. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/994_575. **7. Указ** Президента України "Про рішення Ради національної безпеки і оборони України" від 8 червня 2012 року "Про нову редакцію Стратегії національної безпеки України" [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/389/2012/paran5#n5. **8. Президент** України поставив завдання прискорити ухвалення стратегічних документів сектора безпеки [Електронний ресурс] // Рада національної безпеки і оборони України. – Режим доступу : http://www.rnbo.gov.ua/news/1272.html. **9. The European** Network and Information Security Agency [Електронний ресурс]. – Режим досупу : http://www.enisa.europa.eu.

ТЕНДЕНЦИИ РАЗВИТИЯ КИБЕРУГРОЗ В МИРОВОМ ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

***Олег Рустемович Черняк** (начальник управления)*
***Олег Владиславович Федулов** (заместитель начальника службы)*
Воинская часть А0515

Для защиты информационных систем от киберугроз (атак) необходимо постоянно проводить анализ и оценку рисков их существования в мировом информационном пространстве, которые влияют на конфиденциальность, целостность и доступность информационных ресурсов. Проведен анализ и выявление основных тенденций развития киберугроз в мировом информационном пространстве, по результатом которого можно прийти к выводу, что тенденции развития киберугроз увеличиваются и усложняются механизмы их распространения.

***Ключевые слова:** киберугрозы, кибератаки, безопасность Интернет.*

CYBER THREATS TRENDS IN THE WORLD INFORMATION SPACE

***Oleg Cherniak** (Chief of a Department)*
***Oleg Fedulov** (Depute Chief of a Service)*

Military Unit A0515

To protect informational systems against cyber threats (attacks) risks must be constantly evaluated and assessed their existence in the global information space affect the confidentiality, integrity and availability of information resources. Upon the analysis and identification of the trends major development of cyber threats in the global information space made, it is possible to draw the conclusion about the trends progress of cyber threats and mechanisms of their proliferation become more complicated.

***Key words:** cyber threats, cyber attacks, Internet security.*