# 10.2. Основні загрози для веб-ресурсів

Безпека веб-ресурсів – є одним з найбільш гострих питань в контексті інформаційної безпеки. Як правило більшість сайтів, доступних в Інтернеті, мають різного роду вразливості і постійно піддаються атакам.

Основні типи загроз для інформаційної безпеки веб-додатків (сайтів):

1. **Загрози конфіденційності** - несанкціонований доступ до даних.
2. **Загрози цілісності** - несанкціоноване спотворення або знищення даних.
3. **Загрози доступності** - обмеження або блокування доступу до даних.

Основним джерелом загроз для інформаційної безпеки сайтам є зовнішні порушники. Зовнішній порушник - особа, що мотивована, як правило, комерційним інтересом, має можливість доступу до сайту компанії. Ця особа, зазвичай, не обізнана про дану інформаційну систему, але має високу кваліфікацію в питаннях мережної безпеки і великий досвід в реалізації мережних атак на різні типи інформаційних систем.

Основною загрозою безпеці сайту є хакерська атака. Вона може мати кінцеву мету, бути цільової атакою або носити безсистемний характер, за принципом - атакую ​​все підряд, що-небудь та зламається.

У першому випадку зловмисник може виявляти максимально можливу кількість векторів атаки для складання та реалізації потенційно успішних сценаріїв злому, у другому ж об'єкти атакують масово, звичайно використовують кілька поверхневих вразливостей.

## Види загроз

Загрози для безпеки пов'язані з кількома факторами:

**Вразливості сайтів або їх компонентів.** Вразливості сайтів, як правило, призводять до виконання коду на віддаленому сервері. Всі сервери використовують дані, передані користувачем при обробці запитів. Часто ці дані використовуються при складанні команд, що застосовуються для генерації динамічного вмісту. Якщо при розробці не враховуються вимоги безпеки, зловмисник отримує можливість модифікувати виконувані команди. До такого роду вразливостей відносяться, наприклад, SQL-injection.

**Використання механізмів перевірки ідентифікації.** Атаки, що скеровані на методи перевірки ідентифікатора користувача, служби або програми, або на методи, які використовуються веб-сервером для визначення того, чи має користувач, служба або додаток необхідні для вчинення дії дозволи. До такого роду атак відносяться – підбір паролів, обхід авторизації, небезпечне відновлення паролів, передбачуване значення сесії або її фіксація.

**Загрози безпеки відносяться до атак на самих користувачів, атаки на клієнтську частину.** Під час відвідування сайту, між користувачем і сервером встановлюються довірчі відносини, як в технологічному, так і в психологічному аспектах. Користувач очікує, що сайт надасть йому легітимний вміст і не очікує атак з боку сайту. Експлуатуючи цю довіру, зловмисник може використовувати різні методи для проведення атак на клієнтів сервера. Такого роду атаки можуть бути задіяні як в складних сценаріях атаки, так і в атаках на клієнтську частину, наприклад XSS.

**Витік або розголошення критичної інформації.** До розголошення інформації відноситься як дані безпосередньо про сайт, його компоненти, платформу та складові, так і витік конфіденційної інформації з сайту, через її неналежний захист. Це розкриття інформації, доступ до якої заборонено, або розкриття інформації в результаті невірного налаштування сайту або веб-сервера.

**Логічні атаки.** Логічні атаки спрямовані на експлуатацію функцій сайту або логіки його функціонування. Логіка веб-додатку є очікуваним процесом функціонування програми при виконанні певних дій, таких як: відновлення паролів, реєстрація облікових записів, транзакції в системах електронної комерції. Додаток може вимагати від користувача коректного виконання кількох послідовних дій для виконання певного завдання. Зловмисник може обійти або використовувати ці механізми в своїх цілях. До такого роду атак відносяться і атаки класу відмови в обслуговуванні, DoS.

## Види атак на веб-додатки

**Цільові атаки** - це атаки, спеціально націлені на сайт або групу сайтів, що об'єднані однією ознакою (сайти однієї компанії, що відносяться до певної сфери діяльності) або об'єднані кількома ознаками. Небезпека таких атак полягає саме в «замовному» характері. Виконавцями таких атак стають, як правило, зловмисники, що мають високу кваліфікацію в області безпеки веб-додатків (рис.1).



Рис. 1. Повідомлення про надання злочинних послуг

Метою таких атак, зазвичай, є отримання конфіденційної інформації, яка може бути використана недобросовісними конкурентами або злочинцями для отримання прибутку.

**Нецільові атаки** - це атаки, які проводяться фактично навмання, а її жертвами стають випадкові веб-сайти незалежно від популярності, розміру бізнесу, географії або галузі. Нецільова атака на сайт - це спроба отримання несанкціонованого доступу до веб-ресурсу, при якій зловмисник не ставить за мету зламати конкретний сайт, а атакує відразу сотні або тисячі ресурсів, відібраних за певним критерієм. Наприклад, сайти, що працюють на певній версії системи управління сайтом. Такого роду атаки намагаються охопити максимальну кількість сайтів при мінімумі витрат (рис.2).

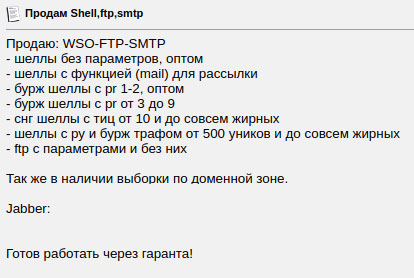


Рис. 2. Повідомлення про надання злочинних послуг

При вдалій спробі атаці зловмисник намагається отримати з цього користь: закріпитися на сайті, завантажити хакерський скрипт (Web Shell, Back Door), додати ще одного адміністратора, впровадити шкідливий код або отримати необхідну інформацію з бази даних.

Цільові атаки проводяться таємно, як правило досягають своєї мети. Нецільові атаки досить «гучні» і часто не досягають поставлених цілей, але, тим не менш, можуть доставити багато проблем для власника веб-ресурсу.

### Основні типи атак

Існує кілька видів атак на веб-сайти, які можуть використовувати зловмисники для отримання несанкціонованого доступу, пошкодження даних або порушення роботи веб-сайту.

* **Метод ін’єкцій.** Має багато різновидів. Наприклад, SQL-injection це втілення злочинного SQL-коду у запит веб-додатку до бази даних. Надає можливість прочитати вміст любих таблиць, знищити, додати або спотворити дані, працювати з локальними файлами та виконати любі команди на сервері, що атакується.
* **Міжсайтовий скриптинг (XSS, Cross-Site Scripting)**/ тип атаки на веб-додаток (клієнтська частина). У веб сторінку втілюється шкідливий код, що запускається, коли сторінка буде відкрита. Скрипт починає діяти і взаємодіє з сервером злочинця. Це може дозволити зловмиснику отримати доступ до сесійних даних, перехоплювати введені дані користувача або змінювати вміст веб-сторінок.
* **DDoS (Distributed Denial of Service).** При DDoS-атаках зловмисник використовує ботнет (мережа захоплених комп'ютерів) для перевантаження веб-сервера трафіком, що призводить до відмови в обслуговуванні легітимних користувачів. Це може призвести до недоступності веб-сайту або зменшення його продуктивності. В DDoS-атаках використовується або виникнення помилок, що призводять до відмови сервісу, або спрацьовування захисту, що приводить до блокування роботи сервісу, а в результаті і до відмови в обслуговуванні.
* **Атаки перебору паролів**. Зловмисник намагається здійснити перебір або вгадати паролі облікових записів користувачів за допомогою різних комбінацій чи словників.
* **Атаки крадіжки сеансів (Session Hijacking)**. Зловмисник намагається перехопити та використовувати ідентифікатори сеансів (session ID), щоб підмінити легітимну сесію користувача та отримати несанкціонований доступ до облікового запису. Дані, зокрема, логіни і паролі, можуть передаватися по мережі в незашифрованому вигляді, тоді хакер може отримати дуже багато інформації: хто, звідки і куди та які дані передавав.
* **Атаки на файлову систему**. Зловмисник намагатиметься отримати доступ до файлів та директорій веб-сайту, які не повинні бути доступні публічно. Це може призвести до витоку конфіденційних даних або зміни вмісту веб-сайту.

Це лише деякі з багатьох видів атак, і розробники сайтів повинні вживати заходів для захисту від цих загроз. Це має бути правильна фільтрація введення даних, використання параметризованих запитів до бази даних, оновлення та патчинг програмного забезпечення, використання сильних паролів, впровадження механізмів захисту від DDoS-атак і регулярне оновлення системи для усунення вразливостей. Важливо проводити регулярні аудити безпеки, щоб виявляти та усувати потенційні вразливості веб-сайту.

### Природа атак

Поширення атак на сайти пов'язано з двома основними факторами: недбале ставлення до безпеки сайту і низький поріг входу потенційних зловмисників.

У більшості випадків на сайтах не використовуються спеціальні засоби виявлення, моніторингу та захисту, а також немає відповідального персоналу та обізнаності про загрози безпеки сайту. Мало уваги приділяється якості коду і безпечному налаштуванню сайту і веб-сервера.

Поширення утиліт і сканерів безпеки сайтів обумовлює низький поріг входження потенційних зловмисників. А численні спільноти і форуми сприяють поширенню технік атак серед всіх бажаючих. Цьому сприяє широке і досить оперативне розголошення про виявлення нових вразливостей або технічні аспекти атак.

### Запобігання загроз

Існує низка заходів, які можуть бути вжиті для запобігання загрозам атак на веб-сайт.

* Регулярне оновлення всіх компонентів сайту, включаючи веб-сервер, бази даних та додатки до останніх доступних версій. Це допомагає закрити вразливості, які можна використовувати зловмисниками.
* Встановлення прав на доступ, які мінімізують можливості зловмисників. Обмежити привілеї користувачів та програм до того, що їм дійсно необхідно для виконання своїх завдань.
* Використання сильних паролів, які містять щонайменше 8 символів і включають комбінацію літер (у верхньому та нижньому регістрі), цифр та спеціальних символів. Рекомендується також увімкнути двофакторну автентифікацію для підвищення безпеки.
* Завжди перевіряти та фільтрувати введення даних від користувачів, щоб запобігти атакам на основі ін'єкцій, таких як SQL-ін'єкції та XSS. Використовувати механізми валідації даних на стороні сервера, щоб переконатися в безпеці переданих даних.
* Застосовувати заходи захисту від атак на відмову в обслуговуванні, такі як використання спеціалізованого мережного обладнання, CDN (Content Delivery Network) або послуг DDoS-захисту, які допомагають виявляти та обмежувати шкідливий трафік.
* З'єднання за допомогою протоколу HTTPS. Використовувати SSL/TLS сертифікати для шифрування з'єднання між сервером та клієнтом. Це забезпечує конфіденційність даних і захищає від атак перехоплення інформації.
* Здійснювати регулярні аудити безпеки: сканування на вразливості, аналіз журналів, моніторинг активності та інші дії для виявлення та реагування на потенційні загрози.
* Регулярно створювати резервні копії всіх важливих даних сайту. Це допоможе відновити працездатність та дані у разі успішної атаки або системного збою.
* Використовувати системи контролю доступу, щоб обмежити доступ до конфіденційних ресурсів лише для авторизованих користувачів. Встановити правильні дозволи на файли та директорії.
* Застосовувати системи моніторингу та реєстрації подій безпеки, які допоможуть виявити аномальну активність або спроби несанкціонованого доступу. Активний моніторинг може допомогти в реагуванні на інциденти та запобігання загрозам.
* Регулярно проводити тестування на проникнення до сайту, щоб виявити вразливості та слабкі місця в системі. Це дозволить вжити відповідних заходів для їх усунення.

Безпека веб-сайту - це безперервний процес, і важливо постійно оновлювати свої практики та вживати заходи для безпеки.

## Ботнет

Силу кібератак в Інтернеті можна порівняти з вибухом атомної бомби в реальності. Сьогодні недооцінювати серйозність хакерських зломів веб-ресурсів нерозумно і небезпечно. З такою напастю борються фахівці, на яких влада витрачає мільйони і мільярди доларів.

Ботнет (botnet) є мережею комп'ютерів, заражених шкідливим кодом, який дозволяє злочинним угрупованням дистанційно керувати «інфікованими» машинами без відома користувача.

Бот - це шкідлива програма, яка втілюється на комп’ютер і надає функції віддаленого керування кіберзлочинцям, а сам заражений комп'ютер перетворюється на «зомбі». Комп'ютер, який керує ботнетом, називається центром управління. Щоб не розміщувати в одному місці управління великим ботнетом, зловмисники розділяють його на кілька дрібніших, на випадок, якщо один з них вийде з з ладу. Ботнети можуть складатися від кількох сотень комп'ютерів до десятків або сотень тисяч комп'ютерів-зомбі (рис.3).

В певний момент за командою організатора атаки «зазомбовані» комп'ютери одночасно зв'язуються з сайтом, якому належить стати жертвою, і надсилають до нього певний запит. Ця дія сама по собі не може завдати шкоди сайту. Але через неочікувану величезну кількість запитів, якої не буває в нормі, комп'ютерна система припиняє роботу.

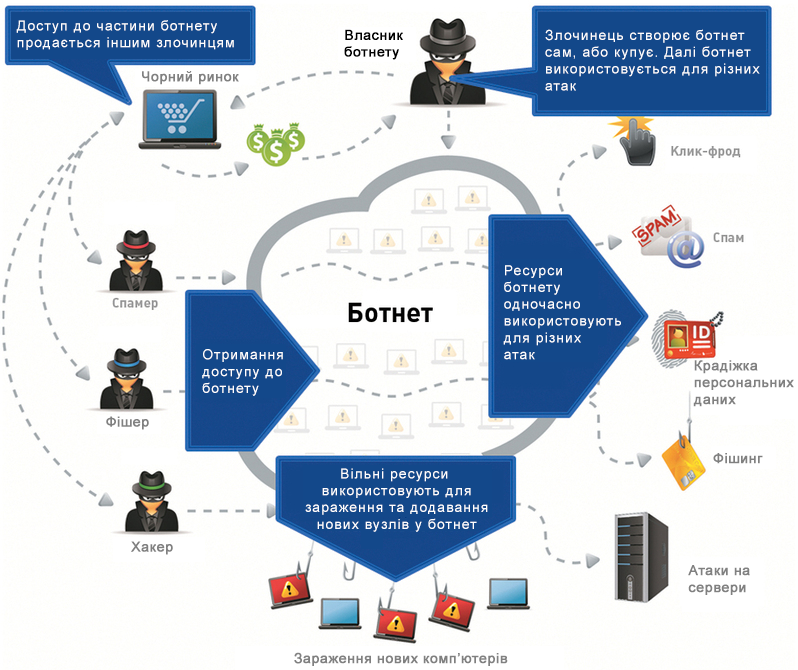


Рис.3. Мережа ботнет

Розробники ботів намагаються зробити так, щоб ці шкідливі програми довгий час не видавали своєї присутності на комп’ютері. Тому, багато власників інфікованих комп'ютерів не підозрюють про зараження. Виявлення зараження комп'ютера та його використання у ботнеті може бути складним завданням, оскільки зловмисники можуть вживати заходів для приховування своєї активності. Однак, є ознаки, щоб визначити можливе зараження комп'ютера та його участь у ботнеті:

* Незвичайна активність процесора та мережної активності. Якщо комп'ютер працює повільно або спостерігається високе завантаження процесора та мережної активності, це може бути ознакою того, що він використовується для виконання шкідливих завдань у фоновому режимі.
* Несподівана поведінка операційної системи. Якщо операційна система починає вести себе незвично, наприклад, з'являються помилки, раптові перезавантаження або закривання програм, це може вказувати на наявність шкідливого програмного забезпечення.
* Зміни у браузері. Якщо веб-браузер починає відкривати невідомі або підозрілі веб-сайти, змінює домашню сторінку або з'являються нові панелі інструментів та розширення, це може бути ознакою зараження.
* Неправильна робота антивірусного програмного забезпечення. Якщо антивірусне програмне забезпечення або захисний фаєрвол перестають коректно функціонувати, це може свідчити про те, що зловмисники впровадили шкідливе програмне забезпечення, яке блокує роботу захисних механізмів.
* Підозрілі мережні підключення. Якщо відбуваються незвичні мережні підключення або активність на маршрутизаторі, це може вказувати на те, що комп'ютер використовується в ботнеті для виконання команд зловмисників.

Боти проникають на чужі комп'ютери в різний спосіб. Найчастіше вони поширюються через сумнівні сайти, при завантаженні неперевірених плагинів для браузера, через електронні повідомлення, із запуском генераторів ключів, «кряків», патчів та іншого піратського програмного забезпечення. У разі підозри на зараження комп'ютера та його участь у ботнеті, рекомендується вжити таких заходів:

* Оновити антивірусне програмне забезпечення та виконати повне сканування системи.
* Ізолювати комп'ютер від мережі, щоб запобігти його взаємодії зі зловмисниками.
* Змінити всі паролі критично важливих облікових записів, таких як банківські або електронні платіжні системи.
* Звернутися до фахівця з комп'ютерної безпеки або ІТ-спеціаліста, щоб отримати допомогу у виявленні та видаленні шкідливого програмного забезпечення.

Важливо вживати заходів для запобігання зараженню комп'ютера, таких як встановлення надійного антивірусного програмного забезпечення, оновлення операційної системи та програмного забезпечення, а також обережність при відкриванні вкладень в електронній пошті або відвідуванні підозрілих веб-сайтів.

Ботнети виробляють атаки на сервери, здійснюють збір і передачу секретної інформації, розсилають спам, здійснюють фішинг і накрутку лічильників, при кліку на які виплачуються цілком реальні гроші. Всі перелічені дії ботнет може здійснювати одночасно.

### Поширені загрози від мережі ботнетів

**DDoS-атаки.** Метою є переповнення буфера атакованої машині, в результаті чого вона перестає відповідати на будь-які запити і просто «висне». DDoS-атаки широко використовуються хакерами для отримання доступу до атакованих комп'ютерів і запуску на них коду. Часто застосовуються недобросовісними конкурентами, оскільки DDoS-атака не є дорогим заходом, а усунення її наслідків може потребувати багато грошей і часу.

**Збирання секретної інформації.** Секретна інформація різного роду, що не призначена до широкого розголошення, завжди привертала кіберзлочинців. Бот на комп’ютері - це шпигун, який може надсилати з інфікованого комп'ютера паролі до різних сервісів, робити знімки екрану, виконувати пошук файлів з подальшим їх видаленням або завантаженням на віддалений сервер. Це номери кредиток, електронних гаманців, логіни, паролі та списки контактів до поштових скриньок чи месенджерів і багато іншого. Отримана інформація при цьому використовується як самими зловмисниками, так і продається на сторону.

**Спам-розсилки.** Якщо зловмисник отримає список контактів з поштової програми користувача, то його база для спам-розсилки збагатиться на кілька десятків чи сотень електронних адрес, але в ботнет кілька тисяч комп'ютерів і це вже суттєво. Є ймовірність, що комп'ютер користувача можуть занести до чорного списку як злісного поширювача спаму.

**Пошуковий спам.** Застосовується для підвищення рейтингу деяких сайтів в пошукових запитах. Чим більше відвідувачів на сайті, тим більше його власник отримає прибутку від реклами.

**Збільшення клік-лічильників.** Існують як окремі сайти, так і цілі мережі, які готові платити за перехід за їх посиланнями в надії, що користувач, який перейшов за посиланням здійснить в них покупку. Цим і користуються власники ботнетів, змушуючи комп'ютери жертв переходити за потрібними посиланнями і заробляючи при цьому непогані гроші.

**Фішінг.** Фішингом називають створення підробленої сторінки популярного проекту. Користувач прямує туди, і його просять авторизуватися і гроші з гаманців користувачів переходять до злочинців.

### Організація мережі ботнетів

Нажаль, організувати ботнет зовсім нескладно, в Інтернеті багато інструкцій щодо його створення. Але, насамперед, зловмисникам потрібно тим або іншим чином втілити бот на комп'ютер жертви, тому, слід бути уважними і не запускати додатків, які надіслано невідомими особами.

Використання ботнетів далеко не завжди здійснюється власником мережі: за придбання або оренду мережі ботнетів може заплатити якась рекламна компанія. Цілеспрямоване створення ботнетів на продаж є цілком прибутковим кримінальним бізнесом.

## Гучні кібератаки 21 століття

Кібератака (хакерська атака) - це шкідливе втручання в інформаційну систему компанії, злам сайтів і додатків, особистих акаунтів і пристроїв. Головні цілі - отримати вигоду від використання цих даних або шантажу власників. Є цілі хакерські групи, які зламують сайти, інфраструктури і сервіси, щоб заявити про себе. Через хакерські атаки щорічно страждають люди, корпорації та цілі країни; губляться мільярди грошей, а іноді і життя. Такі атаки можна порівняти з терористичними.

### Тенденції у кібератаках останніх років:

* Використання складних методів. Хакери використовують витонченіші методи для проведення кібератак. Вони використовують вразливість у програмному забезпеченні, соціальну інженерію та інші методи для отримання доступу до комп'ютерних мереж та даних.
* Націленість на критично важливі інфраструктури. Хакери спрямовують атаки на критично важливі інфраструктури, такі як енергетичні компанії, лікарні та урядові установи. Ці атаки можуть мати серйозні наслідки для суспільства.
* Міжнародна координація. Хакерські угруповання все частіше працюють разом, щоб проводити більш масштабні та складніші атаки. Вони можуть об'єднувати свої ресурси та знання, щоб отримати доступ до ширшого кола цілей.

Ці тенденції показують, що кіберзлочинність становить серйозну загрозу суспільству. Організації повинні приділяти більше уваги кібербезпеці, щоб захистити себе від кібератак.

### Найгучніші кібератаки останніх п'яти років:

* Nvidia 2022 рік. Хакери угруповання Lapsus$ вкрали вихідний код для деяких чіпів Nvidia, включаючи графічні процесори. Атака могла призвести до витоку конфіденційної інформації та порушення безпеки Nvidia.
* Garmin 2022 рік. Хакери угруповання LockBit використали вразливість у програмному забезпеченні Garmin для отримання доступу до комп'ютерних мереж компанії. Атака спричинила відключення сервісу Garmin Connect, який використовується для відстеження фізичної активності користувачів.
* Colonial Pipeline 2021 рік. Хакери угруповання DarkSide атакували паливну компанію Colonial Pipeline, що призвело до зупинення найбільшого магістрального нафтопроводу в США. Атака призвела до дефіциту палива в кількох штатах та викликала підвищення цін на бензин.
* Kaseya 2021 рік. Хакери угрупування REvil атакували компанію Kaseya, постачальника програмного забезпечення для управління ІТ-інфраструктурою. Атака поширилася на понад 1500 організацій, включаючи школи, лікарні та урядові установи.
* Microsoft Exchange 2021 рік. Хакери угруповання Hafnium використали вразливість у програмному забезпеченні Microsoft Exchange для отримання доступу до комп'ютерних мереж понад 100 000 організацій, включаючи урядові установи, приватні компанії та університети.
* Google 2021 рік. Хакери угруповання APT41 використали вразливість у програмному забезпеченні Google для отримання доступу до комп'ютерних мереж компанії. Атака дозволила хакерам отримати доступ до даних про користувачів Google та їх системи.
* Facebook 2021 рік. Хакери угруповання Lapsus$ вкрали вихідний код для деяких продуктів Facebook, включаючи Instagram та WhatsApp. Атака могла призвести до витоку конфіденційної інформації та порушення безпеки Facebook.
* SolarWinds 2020 рік. Хакери угруповання APT29, ймовірно пов'язані з російським урядом, атакували компанію SolarWinds, постачальника програмного забезпечення для управління інфраструктурою. Атака дозволила хакерам отримати доступ до комп'ютерних мереж понад 18 000 організацій, включаючи урядові установи, приватні компанії та університети.
* Microsoft 2020 рік. Хакери угруповання Fancy Bear використали вразливість у програмному забезпеченні Microsoft для отримання доступу до комп'ютерних мереж компанії. Атака дозволила хакерам отримати доступ до даних про працівників Microsoft та їх клієнтів.
* Twitter 2020 рік. Хакери угруповання Lapsus$ зламали акаунти Twitter кількох відомих людей, включаючи Білла Гейтса, Ілона Маска та Джо Байдена. Хакери використовували зламані облікові записи для поширення дезінформації та публікації образливих повідомлень.

Ці атаки показують, що кіберзлочинність може мати серйозні наслідки для організацій та їх клієнтів. Тому, кібербезпека є важливою для всіх організацій, незалежно від їх розміру чи галузі.

Війна в Україні і кібератаки: хакери щороку змінюють фокус

Говорячи про ситуацію з кібератаками від початку війни, вона вказала на те, що їхня інтенсивність постійно збільшується, але змінюється фокус зловмисників. На початку 2022 року російські хакери робили акцент на деструктивних кіберопераціях щодо критичної інфраструктури й намагалися отримати бази даних. Атакували логістику та проводили кампанії проти медіа з метою посіяти паніку серед цивільних. Водночас ці атаки не давали бажаного результату, бо українські IT-системи швидко відновлювались.

У 2023 році стратегія поступово змінилася. Хакери більше закріплювались у мережах, щоб приховано шпигувати та збирати якомога більше інформації. Наприклад, їх цікавив вплив ракетних ударів. У 2024 році спостерігається зміщення фокуса на кібершпигунство, пов’язане з театром бойових дій. Вони атакують постачальників послуг і намагаються якнайдовше залишатися непоміченими в організаціях, які можуть мати якийсь зв’язок з сектором оборони чи з критичною інфраструктурою.

Російські хакери з окупованого Криму, які працюють у складі ФСБ, спеціалізуються на розсиланні шкідливих програм поштою. Водночас є угруповання, які використовують витонченіший підхід до поширення шкідливого ПЗ. Їхні атаки спрямовані на представників сектору безпеки й оборони.

Є також угруповання, що атакують Україну з окупованого Луганська. Тут шкідливі програми надсилають через месенджери. Також постійною загрозою є фішинг, коли хакери надсилають листи з файлом чи посиланням, що веде на сторінку, схожу зі сторінкою входу на пошту чи на сторінку входу до якогось додатку.

Відомо про схему викрадення Telegram-акаунтів, коли користувачів просять, наприклад, проголосувати в якомусь конкурсі. В цій схемі потрібно авторизуватися за допомогою Telegram. Далі до акаунту користувача додається сторонній пристрій. В якийсь момент хакери завершують сесію користувача і він втрачає доступ до свого акаунту, тоді як хакери отримують до нього повний доступ. Надалі вони розпоряджаються акаунтом на власний розсуд — можуть зламувати інші акаунти, а можуть просити гроші на карту для власної наживи.

Найбільше Україну атакують російські хакери, що пов’язані з військовими структурами. Також до кібератак на Україну залучають комерційні хакерські групи.

### Найгучніші кібератаки на Україну 2023 року:

* У серпні 2024 року масштабної атаки зазнав monobank. Атака тривала три доби й була спрямована на те, щоб паралізувати його сервіси. Грошам клієнтів банку вона не загрожувала.
* Атака на енергетичні мережі України у січні 2023 року. Хакери угруповання Sandworm, ймовірно пов'язані з російським урядом, атакували енергосистему України, що призвело до відключення електрики у кількох регіонах країни.
* Атака на систему водопостачання України у лютому 2023 року. Хакери угруповання Sandworm атакували систему водопостачання України, що призвело до відключення водопостачання у кількох містах країни.
* Атака на сайти державних органів України у березні 2023 року. Хакери угруповання Killnet атакували сайти державних органів України, включаючи сайти Міністерства оборони, Міністерства закордонних справ та Служби безпеки України.

## Контрольні запитання

1. Перелічіть основні типи загроз для інформаційної безпеки веб-додатків.
2. З якими факторами пов'язані загрози для безпеки веб-додатків?
3. Перелічить основні види атак на веб-додатки.
4. Яка різниця між цільовими та нецільовими атаками?
5. Що має за мету DDOS атака?
6. Яку шкоду може спричинити розсилка спаму?
7. Які наслідки бувають після атак на сайти?
8. Які фактори сприяють поширенню атак на сайти?
9. Як можна запобігти загрозам атак?