# 8.1. Основні загрози для безпеки 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 і 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 відмову 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, 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).

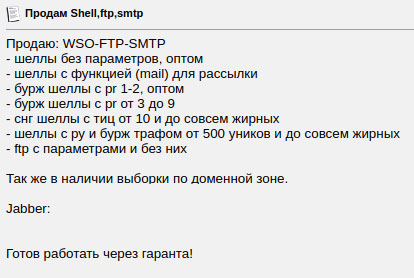


Рис. 2. Повідомлення про надання злочинних послуг

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

* **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.
* **DoS - (Denial of Service - Відмова в обслуговуванні)** - атака, що має за мету змусити сервер не відповідати на запити. Такий вид атаки не передбачає отримання деякої секретної інформації, але іноді буває допоміжною в ініціалізації інших атак. Наприклад, деякі програми через помилки в своєму коді можуть викликати виняткові ситуації, і при вимиканні сервісів здатні виконувати код, наданий зловмисником або атаки лавинного типу, коли сервер не може обробити величезну кількість вхідних пакетів.
* **DDoS - (Distributed Denial of Service)** - має таку ж мету що і DoS, але проводяться не з одного комп'ютера, а з кількох комп'ютерів в мережі. 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. DDoS використовується там, де звичайний DoS є неефективним. Для цього кілька комп'ютерів об'єднуються, і кожен здійснює DoS атаку на систему жертви. Разом це називається DDoS-атака.
* **Перехоплення пакетів.** Оскільки найчастіше дані, зокрема, логіни і паролі, передаються по мережі в незашифрованому вигляді, то при відповідним чином встановленому і налаштованому програмному забезпеченні, що називається сніфером, хакер може отримати дуже багато інформації: хто, звідки і куди, а також які дані передавав.
* **Атака за допомогою шкідливого програмного забезпечення.** На комп'ютер користувача з використанням різних методів (в тому числі і соціальної інженерії і дірок в програмному забезпеченні), надсилається або вірус, або троян, і, вже залежно від ступеня його шкідливості або передаються певні дані, або перехоплюється контроль над системою.
* **Мейлбомбінг (розсилка спаму)** - найстаріший тип атаки, коли на поштовий сервер надсилається велика кількість листів, внаслідок чого він не може обробити всю цю лавину і попросту падає. Було розроблено багато програм для здійснення спам-атаки, і навіть недосвідчений спамер міг заспамити скриньку недруга. При цьому в програми часто було закладено можливості анонімізації IP-адреси відправника та генерації тем повідомлень, тому, позбутися такого спаму звичайними засобами було досить важко. Але й зараз спам приходить на пошту в досить великих кількостях, всупереч антиспам-фільтрам та іншого програмного забезпечення.
* **Мережна розвідка.** При проведенні атаки хакер може отримати повний доступ до системи, дізнатися про її склад і встановлене програмне забезпечення, при цьому жодних дій деструктивного характеру він не виконує. Тому, атака і називається розвідкою.
* **Соціальна інженерія** заснована на жадібності, некомпетентності користувачів, а також бажанні хакерів показати власну значущість. Зловмисники можуть під самими різними приводами, втираючись в довіру, витягнути з користувача ті чи інші дані, зокрема, логін і пароль. При цьому користувач сам повідомляє їм ці відомості.

### Загрози від атак

* Загроза працездатності сайту та збереження даних користувача. Це призводить до фінансових і репутаційних втрат компанії.
* Хакери використовують сайт для атак на інші ресурси, для розсилки спаму або проведення DoS атак. Сайт блокують пошуковики і браузери, і він втрачає користувачів.
* Атака на сайт в корпоративному середовищі може бути точкою входу до корпоративної мережі компанії.
* Атаки на системи електронної комерції можуть бути використані для здійснення шахрайських дій, викрадення клієнтських баз тощо.
* Атаки можуть бути націлені на подальше «зараження» користувачів сайту, наприклад за допомогою засобів експлуатації вразливостей браузерів чи їх компонентів

### 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

Необхідно не забувати про дотримання базових заходів безпеки при розробці та підтримці роботи сайту, які необхідно виконувати РЕГУЛЯРНО, тоді ймовірність цілісності сайту збільшиться у багато разів. 100% гарантію звичайно ніхто дати не може, але виконуючи такі рекомендації, можна значно зменшити ймовірність несанкціонованого доступу до даних:

* Оновлювати CMS і всі її компоненти - не рідше 1 разу на рік.
* Систематично міняти паролі - не рідше разу на квартал.
* Відмовитися від застосування застарілих версій РНР.
* Налаштувати і застосовувати протоколи передачі даних HTTPS / HSTS.

## 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, а іноді і життя. Такі атаки можна порівняти з терористичними.

Кібератаки розрізняють за способом впливу:

* **Зловмисне вірусні програми, які заражають пристрій.** Вони блокують роботу пристрою або окремих сервісів, встановлюють програми для збору даних і стеження, копіюють і / або знищують файли.
* **Фішинг.** Розсилка повідомлень або електронних листів зі шкідливим кодом. При переході за посиланням шахраї отримують доступ до особистих і платіжних даних.
* **Кібератака через посередника (MitM).** Хакери перехоплюють дані і листування між двома людьми або пристроями. Це роблять за допомогою публічної Wi-Fi-мережі або шкідливого ПЗ.
* **«Відмова в обслуговуванні» (DDoS-атака).** Хакери ініціюють безперервний потік запитів або відвідувань сайту чи сервісу. В результаті ресурс перестає працювати.
* **SQL ін'єкція.** Шкідливий код впроваджується на сервер, який обробляє SQL-запити (Structured Query Language - структурована мова запитів), тобто запити до структурованих баз даних.
* **Zero-day (0-day).** Здійснення атак через вразливості, які самі розробники ще не виявили і не встигли усунути.
* **Тунелювання DNS.** Кібератака з застосуванням протоколу DNS для передачі стороннього трафіку HTTP і інших протоколів через порт 53. Так хакери отримують дані з системи і скеровують їх в своє середовище або навпаки.

### 1. WannaCry - наймасовіший вірус десятиліття

**Коли:** травень 2017 року.

**Кого або що атакували:** комп'ютери на ОС Microsoft Windows.

**Що сталося:**

WannaCry - шкідлива програма-вимагач, яка використовувала вразливість нульового дня в різних версіях Windows. Проникаючи в комп'ютери, вірус зашифровував весь вміст, а потім починав вимагати гроші за розблокування (рис.3). Однак розшифрувати файли було неможливо.



Рис.3. Віконце з вимогами вимагачів WannaCry

Вперше вірус виявили в Іспанії, а потім і в інших країнах. Найбільше постраждали Росія, Україна і Індія. Через WannaCry зупинилася робота банків, урядових організацій, аеропортів. У ряді британських лікарень не змогли провести термінові операції. Код вірусу виглядав занадто примітивним і начебто недописаним. Тому з'явилися версії, що розробник випадково випустив його завчасно, оскільки коди для розшифрування не працювали. Припускають, що спочатку WannaCry повинен був вразити всі пристрої на Windows.

Зупинити вірус вдалося досліднику Маркусу Хатчинса, який звернув увагу, що перед тим, як зашифрувати файли, програма надсилає запит на неіснуючий домен. Хатчинс зареєстрував цей домен, після чого WannaCry перестав завдавати шкоди. У створенні вірусу підозрюють Lazarus Group та інші угруповання, пов'язані з Агентством національної безпеки США: дані про вразливість були відомі тільки АНБ.

**Збиток:** вірус встиг заразити 500 тис. комп'ютерів в 150 країнах світу і завдати шкоди в $1млрд.

### 2. Petya / NotPetya / ExPetr - найбільший збиток від кібератаки

**Коли:** червень 2017 року.

**Кого або що атакували:** великі корпоративні мережі компаній і державних служб по всьому світу.

**Що сталося:**

Перша версія вірусу з'явилася в березні 2016 року, але серйозні кібератаки почалися в 2017р. Подібно до WannaCry, Petya і його пізні версії вражали комп'ютери на ОС Microsoft Windows. Вони зашифровували файли - точніше, базу даних з інформацією про всі файли на диску - і дані для завантаження ОС. Потім вірус вимагав викуп у біткоїнах (рис.4).

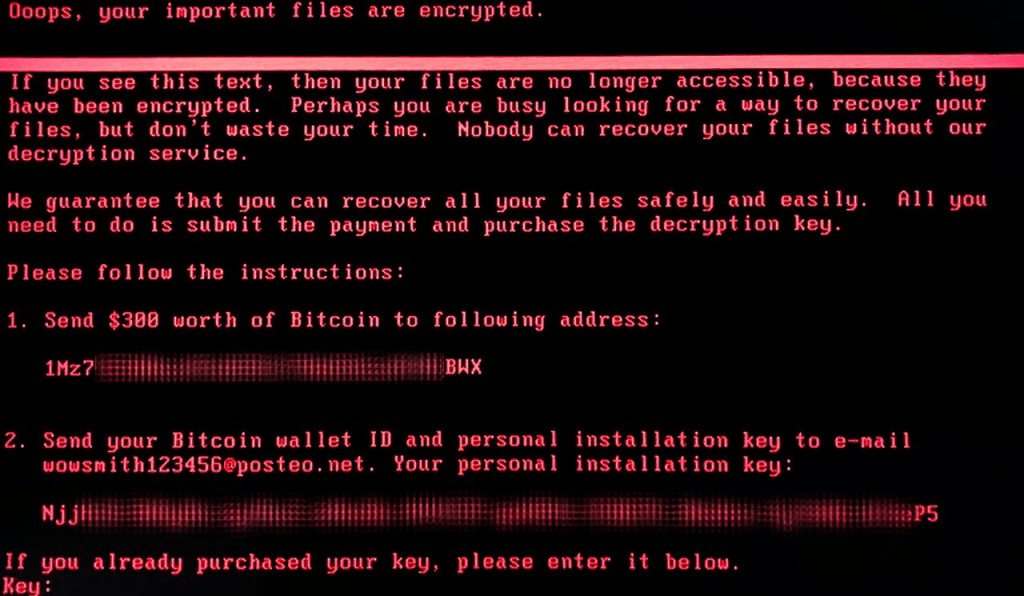


Рис.4. Екран ураженого вірусом NotPetya комп'ютера

Але коди для розшифрування не допомагали, а, навпаки, знищували все дані на твердому диску. При цьому вірус отримував повний контроль над всією інфраструктурою компанії, і захист від WannaCry проти нього вже не діяв.

Для створення NotPetya використовували коди хакерського угруповання Equation, викладені у відкритий доступ. У жовтні 2020 влада США звинуватила хакерське угруповання Sandworm, що складається із співробітників російського ГУ ГШ, в причетності до вірусу NotPetya і інших кібератак.

Найбільше від вірусу постраждала Україна, і від неї почалося зараження. Причина - в автоматичному оновленні бухгалтерської програми M.T.doc, якою користується більшість компаній і держорганів в країні.

**Збиток:** Вірус торкнувся компаній і держорганів Європи, США, Австралії, Росії, України, Індії, Китаю. Серед постраждалих - російські компанії «Роснефть» і «Башнефть», міжнародні корпорації Merck, Maersk, TNT Express, Saint-Gobain, Mondelez, Reckitt Benckiser. В Україні постраждало понад 300 компаній, включаючи «Запоріжжяобленерго», «Дніпроенерго», Київський метрополітен, українські мобільні оператори «Київстар», LifeCell і «Укртелеком», магазин «Ашан», Приватбанк, аеропорт Бориспіль. 10% пам'яті всіх комп'ютерів в країні виявилося стерто. Загальна сума збитку від діяльності хакерів склала більше $ 10 млрд.

### 3. Вибори в США - головний політичний скандал

**Коли:** липень 2016 року.

**Кого або що атакували:** сервери Національного комітету Демократичної партії США (DNC) і комітету Демократичної партії з виборів до Конгресу (DCCC).

**Що сталося:**

Хакери використовували шкідливе ПЗ для віддаленого управління серверами і передачі файлів, а також стеження за всіма діями користувачів в рамках мережі. Після кібератаки хакери вичистили всі сліди своєї активності.

Хакерам вдалося отримати доступ до електронної пошти кандидата в президенти від демократів Хіларі Клінтон та її команди. В результаті 30 тис. електронних листів були опубліковані на WikiLeaks, включаючи 7,5 тис. документів, відправлених самою Клінтон. Багато документів були секретними і стосувалися терористичних атак на консульство США в Бенгазі в 2012 році. Решта містили персональні дані членів і спонсорів демократичної партії, включаючи номери їх кредитних карт.

Американські експерти з інтернет-безпеки звинуватили в цих атаках діючі з Росії хакерські угрупування під назвою Cozy Bear і Fancy Bear.

**Збиток:** Історія з листуванням викликала розкол всередині демократів і сильно похитнула їхні позиції напередодні виборів. Скандал негативно вплинув на рейтинги Клінтон і завадив їй перемогти Дональда Трампа на президентських виборах.

Напередодні нових американських виборів в 2020 році вийшла доповідь Microsoft, де повідомляється про 200 хакерські атаки, що пов'язані з виборами. В числі головних винних називають Росію.

### 4. Злам Facebook - найгучніший витік даних з соцмережі

**Коли:** 2020 рік.

**Кого або що атакували:** персональні дані користувачів Facebook.

**Що сталося:**

У березні 2020 року британська компанія Comparitech повідомила про витік даних більш 267 млн. користувачів Facebook. Велика частина з них належить американцям. Їх могли використовувати для розсилки фішингових посилань.

У серпні 2020 року експерти з компанії DarkNet Data Leakage & Breach Intelligence (DLBI) виявили в Мережі персональні дані 150 млн. користувачів Facebook, Instagram і LinkedIn. На цей раз дані викрали з сервера в США, який належить китайській компанії Shenzhen Benniao Social Technology (socialarks.com). Вона продає рекламу і просування в соціальних мережах.

**Збиток:** Після перших витоків Федеральна торгова комісія США зобов'язала Facebook виплатити рекордні $5 млрд. штрафу. Це в 20 разів вище найбільших санкцій, які застосовувалися за витоку даних. Репутація самої компанії на тлі регулярних витоків сильно похитнулася - як і позиції на фондовій біржі.

### 5. Гучний злам акаунтів знаменитостей в Twitter

**Коли:** липень 2020 року.

**Кого або що атакували:** Twitter-аккаунти Білла Гейтса, Ілона Маска, Барака Обами, Джеффа Безоса, Каньє Уеста і інших відомих особистостей в США.

**Що сталося:**

У зламаних профілях зловмисники, від імені американських зірок, політиків і бізнесменів, закликали відправляти біткоїни на вказаний криптогаманець. Кожен переказ вони обіцяли повернути в подвійному розмірі. Постраждали також корпоративні акаунти Apple і Uber.

До цього в 2009 році зламували Twitter Барака Обами, в 2015-му - Дональда Трампа, а в 2019 році - гендиректора Twitter Джека Дорсі. Однак атака 2020 року стала наймасовішою.

**Збиток:** Всього було зламано понад 50 відомих акаунтів. У перші ж години після атаки шахраї отримали більше 300 переказів на суму понад $ 110 тис.

### 6. Stuxnet - найперша кіберзброя

**Коли:** 2009-10 роки.

**Кого або що атакували:** комп'ютери на ОС Windows.

**Що сталося:**

Мережний вірус Win32/Stuxnet вразив особисті комп'ютери, а також цілі автоматизовані системи управління виробництвом. Він використовував чотири уразливості «нульового дня» в ОС Windows, перехоплюючи і змінюючи потік даних промислових підприємств, електростанцій та аеропортів (рис.5).

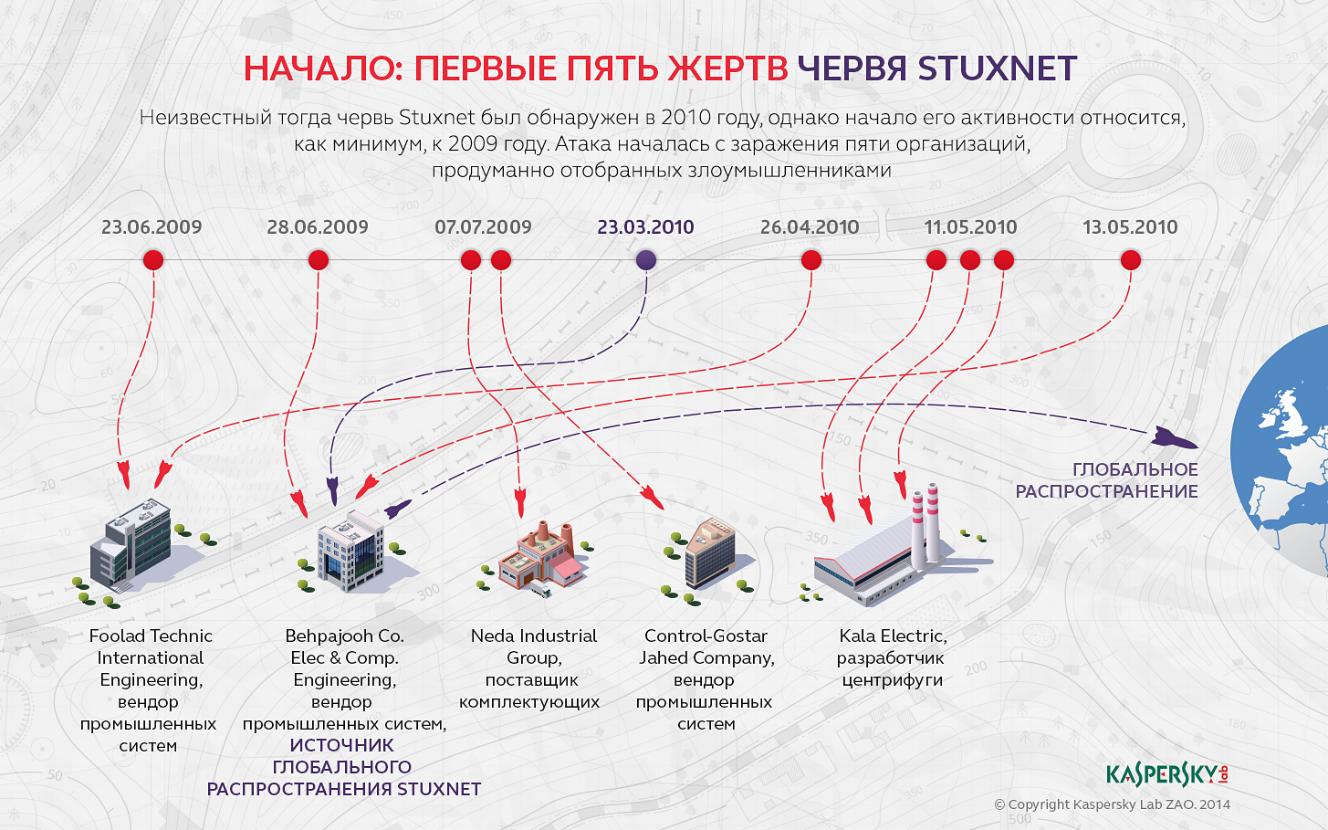


Рис.5. Поширення мережного вірусу Stuxnet

У коді фахівці знайшли сліди програми вразливості «нульового дня», явно написаної професіоналами. З'явилися версії, що Stuxnet був запущений з конкретною метою - атакувати блоки управління газовими центрифугами для отримання збагаченого урану на стратегічних об'єктах. Саме заводи, які їх випускали, стали ще однією мішенню шкідливого ПЗ. Зловмисники розраховували, що від них вірус пошириться на заводи з виробництва збагаченого урану в Ірані, щоб нанести удар по всьому ядерного проекту. Їх план спрацював.

У підсумку головними підозрюваними в кібератаці стали спецслужби Ізраїлю і США.

**Збиток:** Всього вірус встиг заразити 200 тис. пристроїв. Іранцям довелося позбутися 1 тис. Центрифуг для збагачення уранового палива, уражених Stuxnet. Решта блоки не постраждали, але ядерна програма Ірану була відкинута на кілька років назад.

### 7. Yahoo - наймасштабніший витік даних

**Коли:** 2013-14 роки.

**Кого або що атакували:** акаунти користувачів Yahoo.

**Що сталося:**

Зловмисники зламали акаунти користувачів Yahoo і вкрали їх особисті дані, включаючи адреси електронної пошти і номери телефонів. Злочинці діяли в два етапи - в 2013 і 2014 роках, при цьому Yahoo розповіла про це тільки в 2016-му.

Відповідальність за кібератаку покладено на двох співробітників ФСБ і двох хакерів з Росії і Канади. З них тільки канадець визнав свою провину і отримав п'ять років в'язниці.

**Збиток:** Всього постраждали 3 млрд облікових записів. Ринкова вартість Yahoo зменшилася на $350 млн. - саме стільки вона недоотримала в результаті операції з поглинання компанією Verizon.

### 8. Marriott - найсерйозніший удар по репутації

**Коли:** 2014-18 роки.

**Кого або що атакували:** мережа готелів Marriott International.

**Що сталося:**

У 2014 році хакери зламали систему Starwood Preferred Guest, де зберігалися дані про клієнтів готелів Marriott: імена і прізвища, номери паспортів, контактні та платіжні дані. Атака розкрилася лише чотири роки по тому. Підозри впали на угруповання з числа співробітників китайської розвідки, яка намагалася зібрати дані про громадян США.

**Збиток:** Постраждали близько 500 млн. клієнтів. Мережі довелося заплатити $ 124 млн штрафу за витік даних.

### 9. BlueLeaks - найгучніший витік даних з держорганів

**Коли:** червень 2020 року.

**Кого або що атакували:** правоохоронні органи і спецслужби США.

**Що сталося:**

Хакери з угруповання Anonymous отримали доступ до 269 Гб секретних даних правоохоронних органів і спецслужб США у вигляді більш 1 млн. файлів: відеоролики, електронні листи, аудіофайли, а також документи з планування та розвідки за останні десять років - включаючи ті, що підтверджують стеження за активістами Black Lives Matter. Файли передали групі хакерів-активістів DDoSecrets, яка опублікувала отриману інформацію.

У відповідь на це Twitter заблокував акаунт DDoSecrets, а в Німеччині заблокували сервер, на якому зберігалися дані BlueLeaks - за запитом від американської влади.

В січні 2019 року це угрупування опублікувало 175 Гб даних про таємні угоди Кремля, Російської православної церкви і участі Росії у війні на Донбасі.

**Наслідки:** Опубліковані документи викликали гучний скандал і звинувачення на адресу американських спецслужб, які у відповідь завели кримінальну справу. Їх дії щодо хакерів порівняли з переслідуванням WikiLeaks.

### 10. Найскандальніша кібератака російських хакерів

**Коли:** травень 2020 року.

**Кого або що атакували:** Агентство національної безпеки США.

**Що сталося:**

Хакери спробували зламати поштові сервери АНБ. Зловмисники використовували вразливість у агента пересилання повідомлень Exim, виявлену в червні 2019 року. Вона дозволяє злочинцеві відправляти шкідливий лист на сервер і відразу ж отримувати можливість віддалено запускати там свій код.

АНБ звинуватила в атаці хакерське угруповання Sandworm (Telebots, Voodoo Bear, Iron Viking і BlackEnergy), що пов'язане з Росією - те саме, що, ймовірно, запустило вірус NotPetya. Мін'юст США пізніше звинуватив їх в причетності до політичних подій в Грузії і Україні, а також у втручанні в вибори у Франції та атаці на комп'ютерну мережу Зимових Олімпійських ігор в Пхенчхані в 2018 році.

### Кібератака на Tesla

У 2016 році китайська хакерська група Whitehat Keen Security Lab зламала Tesla Model S через точку доступу Wi-Fi. Tesla швидко усунула вразливість, але потім хакери виконали це знову. Вони пропонували водіям підключитися до Wi-Fi, встановлювали шкідливе ПЗ і отримували повний доступ до систем управління.

У наступні роки виявлялися нові вразливості. Наприклад, можна було підключити свій ноутбук до мережного кабелю за панеллю приладів, запустити автомобіль за допомогою спеціальної програми та керувати ним. Завдяки щасливому випадку ніхто з водіїв не постраждав, хоча у зловмисників був доступ, в тому числі, до гальмівної системи. Це викликає, в свою чергу, багато питань до безпілотників, де контроль з боку водія мінімальний.

У серпні 2020 року російський хакер спробував впровадити шкідливе ПЗ в систему управління Tesla. Для цього він запропонував співробітникові компанії хабар у $ 1 млн. Однак затія провалилася, а самого хакера засудили на п'ять років.

### Кібератаки можуть вбивати

У 2015 році хакери зламали сайт Ashley Madison, призначений для знайомств заміжніх жінок і одружених чоловіків. В результаті атаки витекли дані 40 млн. користувачів. Деяким з них почали розсилати загрози з вимогою викупу в $ 1 тис. Деякі з постраждалих злякалися, що їх подружжя дізнається про зраду, і наклали на себе руки.

Другий випадок стався у вересні 2020 року. Зловмисники атакували ІТ-систему університетської клініки в Дюссельдорфі. В результаті 30 серверів і всі підключені пристрої - в тому числі апарати життєзабезпечення - на деякий час вийшли з ладу. Цього виявилося достатньо, щоб одна з пацієнток померла. Поліція завела кримінальну справу за фактом вбивства. Правда, пізніше в одному з видань з'явилося спростування: нібито смерть пацієнтки не була пов'язана з кібератакою.

### Кібератака на зірок

У 2014 році, в результаті кількох кібератак, хакери отримали доступ до фото та відео знаменитостей, які зберігалися в хмарі iCloud. Багато з них - включно з інтимними - потрапили в мережу: їх опублікували на ресурсі 4chan. У числі постраждалих опинилися Кім Кардашьян, Авріл Лавін, Кейлі Куоко, Дженніфер Лоуренс, Кірстен Данст, Ріанна, Скарлетт Йоханссон, Вайнона Райдер. Деякі поспішили заявити, що фото і відео підроблені.

### Психічна кібератака: злом клініки в Фінляндії

У вересні 2020 року кіберзлочинці зламали базу Vastaamo - одного з найбільших психотерапевтичних центрів в Фінляндії. Вони викрали особисті дані десятків тисяч пацієнтів, включаючи записи сесій з терапевтами. В обмін на дані хакери почали вимагати викуп в € 200-540 з кожного пацієнта і € 450 тис. з самого центру. Уряд Фінляндії зібрав екстрене засідання за участю міністра оборони. Однак зловмисників так і не спіймали, а дані пацієнтів виявилися в даркнеті.

## 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?

## Літературні джерела

1. Безпека веб-додатків <https://webcase.com.ua/blog/bezopasnost-web-prilozhenij/>
2. Що таке кібербезпека? <https://experience.dropbox.com/ru-ru/resources/cyber-security>
3. Вразливості сайтів <https://www.anti-malware.ru/threats/site-vulnerability>
4. Інструменти для перевірки безпеки веб-сайту: запобігання шахрайству та загрозам безпеці <https://www.webhostingsecretrevealed.net/ru/blog/web-tools/safety/>
5. Кібератаки https://www.tadviser.ru/index.php /Статья:Кибератаки
6. DDoS-атаки <https://www.orange-business.com/ru/blogs/kakie-bivayut-ddos-ataki-i-pochemu-zaschischatsya-slozhnee-iz-goda-v-god>
7. Захист сервера від DDoS-атак <https://itelon.ru/blog/zashchita-servera-ot-ddos-atak/>
8. Приклади атак XSS и способів їх послаблення <https://proglib.io/p/primery-atak-xss-i-sposobov-ih-ustraneniya-2021-03-13>
9. Гучні кібератаки 21 століття <https://trends.rbc.ru/trends/industry/600702d49a79473ad25c5b3e>
10. Статистика кібербезпеки за 2021 рік <https://www.websiterating.com/ru/research/cybersecurity-statistics-facts/>