УДК 004.056.57

Макеєв А.В.
*Кіровоградський національний технічний університет*

# Порівняння видів кібератак та методів боротьби з ними

Кібератака (англ. cyber-attack) — спроба реалізації кіберзагрози, тобто будь-яких обставин або подій, що можуть бути причиною порушення політики безпеки інформації або нанесення збитків автоматизованій системі. Можна констатувати, що в Україні в повному обсязі присутні всі ключові «класичні» кіберзлочини (шахрайство, здирництво, несанкціонований доступ до персональної інформації користувачів та автоматизованих баз даних, поширення порнографії, продаж зброї чи наркотиків тощо) і щороку їх кількість зростає.

Та так званих хакерів не лякає навіть те, що в Україні є кримінальна відповідальність за вище скоєні злочини: ст. 361 — несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку; ст. 362 — несанкціоновані дії з інформацією, яка оброблюється в ЕОМ (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї.

Щодо боротьби з кіберзлочинцями, в США компанії, що надають громадянам послуги бездротового зв'язку, прийшли до висновку, що потрібно почати впливати безпосередньо на людей. Для цього вводиться технологія CAS. Вона дозволить моніторити вихідний і вхідний трафік. Також однією з найбільших проблем е DoS та DDoS атаки, розподілені атаки на відмову в обслуговуванні (англ. DoS attack, DDoS attack, (Distributed) Denial-of-service attack) — напад на комп'ютерну систему з наміром зробити комп'ютерні ресурси недоступними користувачам, для яких комп'ютерна система була призначена. Одним із найпоширеніших методів нападу є насичення атакованого комп'ютера або мережевого устаткування великою кількістю зовнішніх запитів (часто безглуздих або неправильно сформульованих) таким чином атаковане устаткування не може відповісти користувачам, або відповідає настільки повільно, що стає фактично недоступним. Взагалі відмова сервісу здійснюється: примусом атакованого устаткування до зупинки роботи програмного забезпечення/устаткування або до витрат наявних ресурсів, внаслідок чого устаткування не може продовжувати роботу; заняттям комунікаційних каналів між користувачами і атакованим устаткуванням, внаслідок чого якість сполучення перестає відповідати вимогам;

Небезпека більшості DDoS-атак — в їх абсолютній прозорості і «нормальності». Адже якщо помилка в ПЗ завжди може бути виправлена, то повна витрата ресурсів — явище майже буденне. З ними стикаються багато адміністраторів, коли ресурсів машини (ширини каналу) стає недостатньо, або web-сайт піддається слешдот-ефекту. І, якщо різати трафік і ресурси для всіх підряд, то можна врятуватися від DDoS, у той же час, втративши велику частину клієнтів.

Виходу з цієї ситуації фактично немає, проте наслідки DDoS-атак і їх ефективність можна істотно понизити за рахунок правильного налаштування маршрутизатора, брандмауера і постійного аналізу аномалій в мережевому трафіку.

Щоб не попасти в безвихідь під час DDoS-атаки на системи, необхідно ретельно підготувати їх до такої ситуації: всі сервери, які мають прямий доступ в зовнішню мережу, мають бути підготовлені до простої і швидкої віддаленої роботи. Великим плюсом буде наявність другого, адміністративного, мережевого інтерфейсу, через який можна отримати доступ до сервера при зайнятому основному каналі. Програмне забезпечення, використовуване на сервері, завжди повинно знаходитися в актуальному стані. Всі дірки — пропатчені, оновлення встановлені. Це захистить вас від DoS-атак, багів у сервісах. Всі слухаючі мережеві сервіси, призначені для адміністративного використання, мають бути заховані брандмауером від всіх, хто не повинен мати до них доступу. Тоді той, що атакує не зможе використовувати їх для проведення DoS-атаки або брутфорса. На підходах до сервера (найближчому маршрутизаторі) має бути встановлена система аналізу трафіку (Netflow в допомогу), яка дозволить своєчасно дізнатися про атаку, що починається, і вчасно виконати заходи з її запобігання.

**Список використаних джерел**

1. *Про закони щодо несанкціонованого доступу [Електронний ресурс]. – Режим доступу: https://www.cybercrime.gov.ua/.*
2. *Головні поняття [Електронний ресурс]. – Режим доступу: https://ru.wikipedia.org/wiki/Кибервойна.*
3. *Щодо застережень Американських служб [Електронний ресурс]. – Режим доступу: http://svit24.net/.*