**Міністерство освіти і науки України**

**Національний університет водного господарства та природокористування**

**Реферат**

З дисципліни:”Інформаційні мережі”

на тему: ”Мережевий захист cisco”

Виконав:

студент групи КН-11інт

Трумкулов В.Т.

Перевірив:

Герус В.А.

Рівне - 2018

**Зміст**

[Вступ](http://masters.donntu.org/2013/fknt/zhadanov/diss/indexu.htm#p0)

1. [Мережеві](http://masters.donntu.org/2013/fknt/zhadanov/diss/indexu.htm#p1) атаки
2. [DDoS–атаки](http://masters.donntu.org/2013/fknt/zhadanov/diss/indexu.htm#p3)
3. [Засоби захисту від DDoS–атак](http://masters.donntu.org/2013/fknt/zhadanov/diss/indexu.htm#p4). Захист cisco

[Висновки](http://masters.donntu.org/2013/fknt/zhadanov/diss/indexu.htm#p5)

Список джерел

## Вступ

Ще кілька десятиліть тому комп'ютерні системи застосовувалися переважно одним користувачем і обмінювалися інформацією за допомогою кількох досить обмежених каналів.

Розробка нового принципу побудови мережі на основі комутації пакетів дозволили значно підвищити гнучкість і живучість системи. В даний час будь–яка діяльність, пов'язана з обміном інформацією не обходиться без використання комп'ютерних мереж. Пропускна здатність і охоплення найбільшої мережі – мережі Інтернет постійно зростає. Це дозволяє створювати багатокористувацькі, сильно розподілені додатки для роботи по всьому світу. Такі системи широко використовуються в областях кредитування, страхування, охорони здоров'я, права, військових додатків, зв'язку та багатьох інших.

Функціонування всіх цих додатків істотно залежить від захищеності інформаційних потоків, оскільки ефективне спільне використання інформаційних ресурсів дозволяє значною мірою підвищити якість обслуговування споживачів, продуктивність роботи бізнесу, роботи державних служб. Таким чином, для організацій і окремих користувачів характерна висока ступінь пов'язаності через відкриті мережі і залежність функціонування від їх безперебійної роботи.

Разом з цим широке впровадження мереж збільшило кількість потенційних зловмисників, що мають доступ до відкритих систем. Одним з небезпечних видів злочинної діяльності в мережі Інтернет є так звані мережеві кібератаки.

## 1. Мережеві атаки

Запобігання мережевим атакам – одне з найскладніших завдань у сфері захисту інформаційних систем. Більшість сучасних систем має розподілену структуру, в основі їх архітектури лежить використання мережевих технологій. І забезпечення працездатності таких систем залежить від здатності протистояти зловмисним діям, які спрямовані на порушення роботи як самої мережі, так і інформаційної системи, що функціонує в її рамках. Одним з найбільш небезпечних видів злочинної діяльності в мережі Інтернет є так звані мережеві атаки. Як свідчить статистика, наведена в Інтернет–джерелах, кількість мережевих атак продовжує зростати, методи, якими користуються злочинці, постійно розвиваються і удосконалюються, від одиничних спроб вони переходять до корпоративних розробок. У той же час сучасні системи виявлення вторгнень і атак ще не досконалі і недостатньо ефективні з точки зору безпеки рішень. Тому методи роботи в цьому напрямку необхідні і актуальні.

**2. DDoS–атаки**

Одним з найскладніших завдань у сфері захисту комп'ютерних систем є запобігання DDoS–атакам.

DDoS–атака (від англ. Distributed Denial of Service, розподілена атака типу «відмова в обслуговуванні») – атака на обчислювальну систему, виконувана з великої кількості комп'ютерів, з метою довести її до відмови. Тобто створити такі умови, при яких легітимні (правомірні) користувачі системи не можуть отримати доступ до надаваних системою ресурсів (серверів), або цей доступ ускладнений .

Спочатку, DDoS–атаки використовувалися для перевірки пропускної здатності каналу, однак, з часом кіберзлочинці усвідомили всі шкідливі можливості цієї технології і прийняли її на своє «озброєння». Тепер DDoS–атаки використовуються кіберзлочинцями в самих різних цілях: тиск на користувачів; блокування ключових вузлів мережі Інтернет; порушення працездатності інтернет – сервісів компаній, бізнес яких заснований на web–сервісах; в конкурентній боротьбі; в політичній конкуренції і т.д. Відповідно, прибутковість такого бізнесу досить висока. Наслідки DDoS – атак можуть призвести до втрати ключових ресурсів мережі, додатків і систем ведення бізнесу, втрати репутації, фінансових втрат і т.п. Так само DDoS–атаки можуть використовуватися для відволікання уваги при запуску інших шкідливих програм, наприклад, для викрадення конфіденційних даних.

Цілями таких атак є створення умов, за яких правомірні користувачі позбавляються можливості доступу до надаваних системою ресурсів (або цей доступ виявляється ускладненим). Сама по собі DDoS–атака виглядає як різке збільшення кількості трафіку на вузлі мережі що атакується.

Існує кілька варіантів класифікацій DDoS–атак за типами. Умовно виділяється кілька методик, що найчастіше використовуються кіберзлочинцями:

* руйнуючі – атаки, проведені таким способом, призводять до того, що вузол мережі стає повністю недоступним: зависає, знищується операційна система, конфігурація пристроїв тощо, такі атаки проводяться за допомогою вразливостей, що знаходяться в програмному забезпеченні;
* атаки на ресурси системи – при такій атаці формується велика кількість безглуздих або сформованих в неправильному форматі запитів до вузлів мережі або додатків, що призводить до значного зниження продуктивності комп'ютерної системи або мережного обладнання.

Метою такої атаки є відмова роботи системи через вичерпання її ресурсів. Ці атаки діляться на кілька видів:

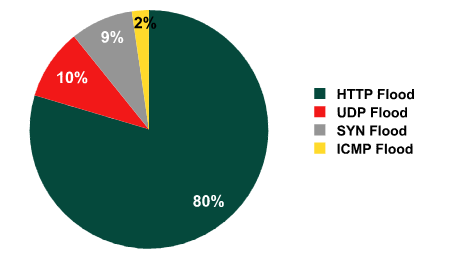
* HTTP GET – цілеспрямована, скоординована відправка на web–сервер жертви великої кількості запитів з «зомбі – мережі»;
* UDP – Flood (англ. Flood – повінь, затоплення) – цей тип атаки спрямований на канал зв'язку; на адресу системи що атакується надсилаються UDP запити великого розміру, при цьому відбувається швидке вичерпання смуги пропускання каналу зв'язку, що веде до системи що атакується, і пристрій, що працює по протоколу TCP, перестає відповідати;
* TCP SYN – Flood – при цьому типі атаки на вузол мережі що атакується надсилається велика кількість запитів на відкриття з'єднання, при цьому атакованому об'єкту доводиться витрачати всі свої ресурси на відстеження всіх цих частково відкритих з'єднань, що призводить до вичерпання кількості сокетів і пристрій перестає відповідати;
* ICMP – Flood – цілеспрямована, спеціалізована відправка великої кількості DNS запитів на DNS – сервер, при цьому DNS – сервер стає не доступний для великого кола користувачів, тому що його ресурси зайняті обробкою цих запитів.

Найчастіше, при проведенні DDoS–атаки використовується кілька типів атак, що, в значній мірі ускладнює протидію DDoS–атакам.

За даними Лабораторії Касперського найбільш популярним видом атаки являється HTTP–Flood (80%), коли на сайт що атакується одночасно відправляється безліч HTTP–запитів. Зловмисники використовують різні технології проведення атак цього типу. У 55% випадків атак типу HTTP–Flood боти намагаються звернутися до якоїсь однієї сторінки сайту; на другому місці з показником 22% знаходяться атаки на різні форми авторизації; третє місце (12%) зайняли атаки з використанням численних спроб скачування будь–якого файлу з сайту. І лише в одному випадку з 10 проводяться більш складні атаки, коли зловмисники намагаються замаскувати дії ботів під поведінку справжніх користувачів .

На другому місці з показником 10% розташувалися атаки типу UDP Flood. Боти, що здійснюють такі атаки, покладаються на «грубу силу», тобто генерують величезну кількість досить невеликих за розміром (наприклад, по 64 байти) сміттєвих пакетів.

На третьому і четвертому місцях у рейтингу популярності у зловмисників стоять атаки типу SYN Flood (8%) і ICMP Flood (2%) відповідно. Описана діаграма показана на рисунку 1.



*Рис. 1 – Типи DDoS–атак*

У більшості випадків, мережа, з якої виконується DDoS–атака, має організацію, що включає три рівні. Така мережа називається «кластер DDoS». Вгорі кластера знаходяться один або кілька комп'ютерів, з яких починається і координується атака. На другому рівні – головні (оброблювальні) комп'ютери, які безпосередньо передають сигнал про початок атаки на наступний рівень. Третій рівень – заздалегідь організована ботнет мережа.

Ботнет мережа – це мережа «комп'ютерів – зомбі», що потрапили під управління кіберзлочинців після зараження. Найчастіше бот у складі ботнета є програмою, потай встановленої на пристрій жертви і дозволяє зловмиснику виконувати якісь дії з використанням ресурсів зараженого комп'ютера. Зазвичай використовуються для несхвалюваних або нелегальних дій – розсилка спам–листів, добірка паролів на віддалених комп'ютерах і сервісах, використання при проведенні DDoS–атак .

Управління зазвичай отримують в результаті встановлення на комп'ютер невидимого не виявляємого користувачем у щоденній роботі програмного забезпечення без відома користувача. Відбувається зазвичай через:

* зараження комп'ютера вірусом через уразливість в програмного забезпечення (помилки в браузерах, поштових клієнтах, програмах перегляду документів, зображень, відео);
* використання недосвідченості або неуважності користувача – маскування під «корисний вміст»;
* використання санкціонованого доступу до комп'ютера (рідко);
* перебір варіантів адміністраторського пароля до мережевих ресурсів, що розділяються (зокрема, до ADMIN $, що дозволяє виконати віддалено програму) – переважно в локальних мережах.

При досить великій мірі вивченості процесу утворення ботнет мереж, протистояння кіберзлочинцям виявляється досить складним завданням.

Справа в тому, що зворотний шлях від жертви до кіберзлочинця простежити досить складно, тому найчастіше вони залишаються не розкритими. Через ці обставини і з'явився вид кримінального бізнесу в мережі Інтеренет – створення ботнет мереж і подальша передача або здача їх в оренду замовнику для проведення DDoS–атак і розсилки спам – листів.

Практично у всіх країнах світу DDoS–атаки є кримінальним злочином, але за гратами їх організатори виявляються надзвичайно рідко. У наші дні організацією DDoS–атак займаються не одинаки, а організовані злочинні групи. Їх розгалуженість, організаційна та географічна, дозволяє успішно протистояти діям правоохоронних органів.

Сучасні системи виявлення вторгнень і атак являють собою програмні або апаратно–програмні рішення, які автоматизують процес контролю подій, що протікають в комп'ютерній системі або мережі, а також самостійно аналізують ці події в пошуках ознак проблем безпеки, ці системи стали необхідним компонентом інфраструктури безпеки більшості організацій.

**3. Засоби захисту від DDoS–атак. Захист cisco**

Вважається, що немає необхідності в спеціальних засобах виявлення DDoS–атак, тому що сам факт атаки не помітити неможливо, однак, досить часто відзначаються атаки, результат яких видно тільки через деякий час.

Методи виявлення DDoS–атак поділяються на декілька груп:

* сигнатурні – засновані на якісному аналізі трафіку;
* статистичні – засновані на кількісному аналізі трафіку;
* гібридні – поєднують в собі переваги двох попередніх методів.

Традиційні технічні засоби захисту (наприклад, міжмережеві екрани і системи виявлення вторгнень (IDS)) не протидіють DDoS–атакам, тому що вони дозволяють лише або заборонити, або дозволити проходження мережевого трафіку на підставі аналізу різних полів мережевих пакетів. Однак, атака може бути успішно реалізована і в рамках дозволених полів мережевих пакетів. Також практично неможливо відрізнити коректно–сформований трафік від шкідливого, оскільки це ті ж самі запити, що і від звичайних користувачів, тільки генеруються в незрівнянно більшій кількості. Кіберзлочинці використовують ще одну технологію, звану IP–spoofing (від англ. Spoof – містифікація).

Цей метод полягає в проставленні у полі зворотної адреси IP–пакета невірної адреси і застосовується для приховування справжньої адреси атакуючого, з метою викликати у відповідь пакет на потрібну адресу і з іншими цілями. Деякі провайдери використовують технологію «Black–hole routing». Ця технологія дозволяє виявляти атаки на клієнта або діапазон IP адрес і забороняє вхід в мережу деяким IP адресами. Атака припиняється, але для клієнта це виглядає як повне відключення від мережі. Зрозуміло, що з великими клієнтами або важливими даними так вчинити неможливо, крім того, атакуючий може підставляти деякі важливі адреси (наприклад, адреси кореневих DNS).

Найефективнішим способом виявлення DDoS–атак є використання спеціально розроблених для придушення DDoS–атак рішень. Принцип їх роботи заснований на навчанні пристрою тому, що може бути розпізнано як коректно–сформований трафік та подальшим виявленням аномалій. При виявленні аномалій включаються механізми захисту різного рівня.

Одним із засобів боротьби з DDoS–атаками є комплексне рішення Cisco Clean Pipes.

Особливостями даного комплексу є швидке реагування на проведення DDoS–атаки, легка масштабованість, висока надійність і швидкодія. Комплекс Cisco Clean Pipes використовує модулі Cisco Anomaly Detector і Cisco Guard, а також системи статистичного аналізу мережевого трафіку, одержуваних з маршрутизаторів по протоколу Cisco Netflow.

У даному рішенні реалізується три рівня перевірок:

* фільтрація спуфінга;
* виявлення «зомбі–комп'ютерів»;
* блокування трафіку з атакуючої адреси.

Anomaly Detector, як випливає з назви, призначений для виявлення аномалій. Його завдання – навчання, а потім виявлення аномалій. Це пасивний елемент і через нього трафік не проходить.

Cisco Guard (фільтр) – розбирає трафік на шкідливу і легітимну складові. Якщо детектор виявляє аномалії, то необхідно пов'язати факт аномалії з DDoS–атакою. Для цього необхідно втрутитися в трафік і почати його аналізувати. При цьому детектор передає команду фільтру на контроль певної зони в мережі і весь трафік зони йде через нього, таким чином на фільтр потрапляє тільки трафік який містить атаку. Все інше проходить повз.

Така схема дозволяє зменшити відсоток помилкових спрацьовувань і збільшує продуктивність фільтра.

## Висновки

У рамках даної роботи було вивчено види мережевих кібератак, методи боротьби з ними. Дана область зараз найбільш розвивається, так як йде постійне суперництво між зловмисниками і організаціями, що забезпечують безпеку даних. Була підтверджена актуальність проблеми захисту і виявлення мережевих кібератак.

**Список джерел**

1. Безопастность сетей // [Электронный ресурс]. – Режим доступа: [http://ru.wikipedia.org/wiki/DoS](http://ru.wikipedia.org/wiki/DoS-%D0%B0%D1%82%D0%B0%D0%BA%D0%B0)
2. Безопастность сетей // [Электронный ресурс]. – Режим доступа: <http://www.intuit.ru/department/security/netsec/3/4.html>
3. Компьютерная сеть и ботнеты // [Электронный ресурс]. – Режим доступа: <http://alsiti.net/index.php?topic=396.0>
4. DDoS-атаки второго полугодия 2011 года // Лаборатория Касперского [Электронный ресурс]. – Режим доступа: <http://www.securelist.com/ru/analysis/208050745/>
5. Михайлюта С. Л., Степанушко И. В., Бабич Б. А., Ткаченко В. Ю., Лавринович В. С., Исследование сетевых DOS-атак, основанных на использовании протокола ICMP // Вісник Інженерної академії України. – К.: 2009. – № 2. – С. 146 – 149
6. Denial of Service Attacks // [Электронный ресурс]. – Режим доступа: <http://www.cert.org/tech_tips/denial_of_service.html>
7. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. 4 издание, 2010, 943с
8. Ефимов В.И. Система мультиплексирования разнесенного TCP/IP трафика / В.И. Ефимов, Р.Т. Файзуллин // Вестник Том. гос. ун-та. – 2005. – № 14. – С. 115 – 118.
9. Лукацкий А. В. Предотвращение сетевых атак: технологии и решения / А. В. Лукацкий. – СПб. : Экспресс Электроника, 2006. – 268 с.
10. Обзор механизмов реализации и обнаружения атак [Электронный ресурс]. – Режим доступа : <http://comp-bez.ru/?p=778>
11. Лукацкий А. В. Обнаружение атак / А. В. Лукацкий. – СПб. : БХВ-Петербург, 2003. – 256 с
12. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства / В. Ф. Шаньгин. – М. : ДМК Пресс, 2010. – 544 с
13. Котенко И. В., Степашкин М. В., Богданов В. С. Архитектуры и модели компонентов активного анализа защищенности на основе имитации действий злоумышленников // Проблемы информационной безопасности. Компьютерные системы. № 4. – СПб., 2005
14. Душкин А.В. Распознавание и оценка угроз несанкционированного воздействия на защищенные информационно-телекоммуникационные системы / А.В. Душкин // Информационные технологии. – 2008. – № 3. – С. 71 – 75.
15. Терновой О.С. Раннее обнаружение DDOS-атак методами статистического анализа /О.С. Терновой/ Перспективы развития информационных технологий. – Новосибирск, изд. «Сибпринт», С. 2012 – 212.