**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**КАЗАНСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМ. А.Н. ТУПОЛЕВА (КНИТУ-КАИ)**

**ИНСТИТУТ КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ И ЗАЩИТЫ ИНФОРМАЦИИ**

### КАФЕДРА СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**МЕТОДИЧЕСКИЕ УКАЗАНИЯ**

### К ВЫПОЛНЕНИЮ ЛАБОРАТОРНОЙ РАБОТЫ № 1

### ПО ДИСЦИПЛИНЕ

**«ПРОЕКТИРОВАНИЕ ЗАЩИЩЁННЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ»**

на тему

**«Анализ и классификация угроз информационной безопасности в ЗТКС»**

Составители:

доцент кафедры СИБ

Зиновьев П.А.

### Казань - 2015

**ЛАБОРАТОРНАЯ РАБОТА № 1**

**НАЗВАНИЕ работы:**

Анализ и классификация угроз информационной безопасности в ЗТКС.

**ЦЕЛЬ работы:**

Изучение методических основ анализа и классификации угроз информационной безопасности, а также анализа рисков их осуществления в рамках создаваемых ЗТКС.

**УКАЗАНИЯ к выполнению лабораторной работы № 1:**

Данная лабораторная работа проводится в форме интерактивной деловой игры, в ходе которой все присутствующие лица (т.е. студенты группы) являются активными участниками проектных подгрупп, проводящих анализ и актуализацию возможных угроз ИБ. Подобная задача наиболее часто встречается при разработке ЗТКС в целом или СЗИ в её составе. Роли участников деловой игры распределяются преподавателем, либо выбираются студентами самостоятельно.

# Теоретический материал

**1. Построение и анализ модели угроз**

Для того, чтобы составить модель угроз для заданной ЗТКС, нужно для каждого используемого в данной системе сервиса, или для каждого вида её обеспечений (технического, программного, информационного и др.) провести анализ потенциальных угроз ИБ. Комплексная методология обеспечения безопасности в рамках ЗТКС может служить эффективным руководством по разработке архитектуры системы обеспечения безопасности, помогая создать план определения характеристик, сопровождения и внедрения процессов обеспечения безопасности во всей сети. Созданную подобным образом архитектуру можно затем применить в рамках программы действия провайдера услуг в ЗТКС по обеспечению безопасности путем использования политик, процедур и технологий.

Так, по определению компании Cisco на сегодняшний день существуют следующие основные типы угроз для создаваемых ЗТКС:

* информационная разведка. Злоумышленники сканируют сеть для обнаружения уязвимых устройств (например, это могут быть открытые порты, отсутствие парольной защиты, уязвимости ОС) и атакуют обнаруженные жертвы;
* распределенные атаки типа «отказ в обслуживании» (DDoS) и атаки на инфраструктуру. Это атаки с использованием большого количества IP-пакетов, передаваемых в сеть. Целями атаки являются снижение быстродействия и надежности работы сети;
* взлом и захват сетевых устройств. Как правило, такие действия следуют за этапом информационной разведки и представляют собой несанкционированный доступ к тому или иному устройству с намерением нарушить его безопасность;
* кража сервисов и мошенничество. Угрозы данного типа заключаются в несанкционированном использовании сетевых ресурсов.

После идентификации и классификации угроз необходимо приступать к выработке мер по их нейтрализации. Для эффективной борьбы с угрозами необходимо понимание трех базовых принципов, а именно:

* предотвращение. Реализация известных защитных мер для предотвращения известных угроз. Средства предотвращения включают установку “заплат” в уязвимые системы, внедрение стандартных и усиленных образов системного программного обеспечения, использование межсетевых экранов или иных технологий разграничения доступа;
* мониторинг. Выявление потенциально опасных действий и действий, связанных с использованием известных уязвимостей; разграничение реальных действий злоумышленника и неадекватных действий пользователей с целью выделения реальных угроз, которые обнаруживаются в ключевых точках агрегации. Для выявления таких действия используются методы развертывания средств мониторинга вторжений, проведение анализа журналов серверов и межсетевых экранов, а также активный мониторинг вызовов операционной системы;
* ответные меры. Способность действовать на основании полученной информации с целью ограничить последствия подтвержденной реальной угрозы в режиме, приближенном к режиму реального времени. В числе применяемых методов – динамическое разграничение доступа, сброс пакетов, изменение конфигурации сетевого устройства, прерывание сеансов работы и блокирование некорректных системных вызовов.

Пример модели угроз представлен в Таблице 1.

Таблица 1.

| **№** | | **Угроза** | **Уязвимость** | **Источник** | **Способ реализации** | **Объект, на который реализуется угроза** |
| --- | --- | --- | --- | --- | --- | --- |
| **Угрозы для сервиса №1.** | | | | | | |
| 1 | | Информационная разведка(сканирование портов, уязвимости в ОС) для возможности реализации других угроз. | Доступность сети клиента для Администратора сети провайдера с PE маршрутизатора. | Внутренние нарушители – Администраторы провайдерской сети. | Возможность исследования сети клиента с PE маршрутизатора. | Частная сеть клиента. |
| 2 | | Распределенные атаки типа «отказ в обслуживании» (DDoS) | Доступность сети клиента для Администратора сети провайдера с PE маршрутизатора. Отсутствие системы фильтрации вредоносного трафика к клиенту. | Внутренние нарушители – Администраторы провайдерской сети. | Возможность отправки огромного количества пакетов с PE маршрутизатора | Частная сеть клиента. |
| **Угрозы для сервиса №2.** | | | | | | |
| 1 | | Информационная разведка(сканирование портов, уязвимости в ОС) для возможности реализации других угроз. | Отсутствие системы фильтрации подозрительного трафика к клиенту. | Внутренние нарушители – Администраторы провайдерской сети.  Внешние нарушители.  Вредоносное ПО. | Возможность исследования открытых портов маршрутизатора клиента путем удаленного сканирования. | Частная сеть клиента. |
| 2 | | Распределенные атаки типа «отказ в обслуживании» (DDoS) | Отсутствие системы централизованной очистки трафика. | Внутренние нарушители – Администраторы провайдерской сети.  Внешние нарушители.  Вредоносное ПО | Посылка огромного количества специально сформированных пакетов. | Частная сеть клиента. |
| 3 | | Перехват трафика | Наличие возможности перехватывать трафик с PE маршрутизатора | Внутренние нарушители – Администраторы провайдерской сети. | Запуск снифера на PE маршрутизаторе. | Частная сеть клиента. |
| **Угрозы для сервиса №3.** | | | | | | |
| 1 | | Распределенные атаки типа «отказ в обслуживании» (DDoS) | Доступность сети клиента для Администратора сети провайдера с PE маршрутизатора. Отсутствие системы фильтрации вредоносного трафика к клиенту. | Внутренние нарушители – Администраторы провайдерской сети | Возможность отправки огромного количества пакетов с пограничного PE маршрутизатора | Частная сеть клиента. |
| 2 | | Перехват трафика | Наличие возможности перехватывать трафик с PE маршрутизатора | Внутренние нарушители – Администраторы провайдерской сети. | Запуск снифера на PE маршрутизаторе | Частная сеть клиента. |
| 3 | | Информационная разведка(сканирование портов, уязвимости в ОС) для возможности реализации других угроз. | Отсутствие системы фильтрации подозрительного трафика к клиенту. | Внутренние нарушители – Администраторы провайдерской сети. | Возможность исследования открытых портов маршрутизатора клиента путем удаленного сканирования. | Частная сеть клиента. |
| **Угрозы для сервиса №4** | | | | | | |
| 1 | | Перехват пароля авторизации | Наличие возможности перехватывать трафик с PE маршрутизатора | Внутренние нарушители – Администраторы провайдерской сети. | Запуск снифера на PE маршрутизаторе | Клиент |
| 2 | | Перехват пароля для авторизации | Наличие возможности перехватывать трафик путем mac спуфинга. Не на всех коммутаторах настроен mac anti-spoofing. | Клиенты сервиса №4 | Подмена мак адреса | Клиент |
| **Угрозы информации для сервиса №5** | | | | | | |
| 1 | | Перехват трафика | Наличие возможности перехватывать трафик с PE маршрутизатора | Внутренние нарушители – Администраторы провайдерской сети. | Запуск снифера на PE маршрутизаторе | Частная сеть клиента. |
| 2 | | Перехват трафика | Наличие возможности перехватывать трафик путем mac-spoofing. Не на всех коммутаторах настроен port isolation. | Клиенты сервисов №№4-5 | Запуск снифера злоумышленником | Частная сеть клиента. |
| 3 | | Перехват паролей авторизации | Неправильный приоритет протоколов аутентификации на маршрутиза-торе. Некор-ректные настройки в связи с введением сервисов №№4-5 | Клиенты сервисов №№4-5 | Запуск снифера злоумышленником | Клиент |
| 4 | | Информационная разведка(сканирование портов, уязвимости в ОС) для возможности реализации других угроз. | Отсутствие системы фильтрации подозрительного трафика к клиенту | Внешние нарушители.  Вредоносное ПО | Возможность исследования открытых портов маршрутизатора клиента путем удаленного сканирования. | Частная сеть клиента. |
| 5 | | Распределенные атаки типа «отказ в обслуживании» (DDoS) | Отсутствие системы фильтрации подозрительного трафика | Внешние нарушители.  Вредоносное ПО | Возможность исследования открытых портов маршрутизатора клиента путем удаленного сканирования. | Частная сеть клиента. |
| **Угрозы для сервиса №6** | | | | | | |
| 1 | Распределенные атаки типа «отказ в обслуживании» (DDoS) | | Отсутствие системы фильтрации подозрительного трафика к клиенту | Внешние нарушители.  Вредоносное ПО | Возможность исследования открытых портов маршрутизатора клиента путем удаленного сканирования. | Частная сеть клиента. |
| 2 | Распределенные атаки типа «отказ в обслуживании» (DDoS) | | Исходящий канал для точки доступа достаточно узкий. 1 мбит. Нет политики QoS для исходящего трафика. | Клиенты сервиса №6 | Возможность DDoS атаки путем загрузки исходящего канала, например P2P трафиком. | Точка доступа WIFI |

**2. Выявление актуальных угроз и оценка рисков ИБ**

Оценка возможности реализации инцидентов ИБ и степени их воздействия на создаваемую ЗТКС осуществляется, чаще всего, на качественных шкалах. Для проведения такой оценки следует использовать таблицы 2, 3, 4.

Таблица 2. Качественная шкала для оценки возможности реализации события

|  |  |  |
| --- | --- | --- |
| **№** | **Уровень вероятности атаки** | **Описание** |
| **1** | A | Событие практически никогда не произойдет. Уровень соответствует числовому интервалу вероятности [0, 0.25) |
| **2** | B | Событие случается редко. Уровень соответствует числовому интервалу вероятности [0.25, 0.5) |
| **3** | C | Вероятность реализации события за рассматриваемый промежуток времени – около 0,5 |
| **4** | D | Скорее всего, событие произойдет. Уровень соответствует числовому интервалу вероятности (0.5, 0.75] |
| **5** | E | Событие почти обязательно произойдет. Уровень соответствует числовому интервалу вероятности (0.75, 1] |

Таблица 3. Качественная шкала для оценки ущерба

|  |  |  |
| --- | --- | --- |
| **№** | **Уровень ущерба** | **Описание** |
| **1** | N (Negligible) | Приводит к незначительным потерям материальных активов, которые быстро восстанавливаются, или к незначительному влиянию на репутацию компании |
| **2** | Mi (Minor) | Вызывает заметные потери материальных активов или к умеренному влиянию на репутацию компании |
| **3** | Mo (Moderate) | Приводит к существенным потерям материальных активов или значительному урону репутации компании |
| **4** | S (Serious) | Вызывает большие потери материальных активов и наносит большой урон репутации компании |
| **5** | С (Critical) | Приводит к критическим потерям материальных активов или к полной потере репутации компании на рынке, что делает невозможным дальнейшую деятельность организации |

Таблица 4. Оценка риска

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Вероятность атаки** | **A** | **B** | **C** | **D** | **E** |
| **Ущерб** |
| N (Negligible) | Низкий Риск | Низкий риск | Низкий риск | Средний риск | Средний риск |
| Mi (Minor) | Низкий Риск | Низкий риск | Средний риск | Средний риск | Высокий риск |
| Mo (Moderate) | Низкий Риск | Средний риск | Средний риск | Средний риск | Высокий риск |
| S (Serious) | Средний риск | Средний риск | Средний риск | Средний риск | Высокий риск |
| С (Critical) | Средний риск | Высокий риск | Высокий риск | Высокий риск | Высокий риск |

На основе данных таблиц определяется уровень ущерба для каждой выделенной угрозы (таблица 5):

Таблица 5. Оценка рисков ИБ

| **№**  **п/п** | **Сервис** | **Реализуемые угрозы** | **Вероятность реализации** | **Степень влияния** | **Уровень риска** |
| --- | --- | --- | --- | --- | --- |
| **1** | **2** | **3** | **4** | **5** | **6** |
| 1 | №1 | Информационная разведка | A | Negligible | Низкий |
| 2 | №1 | отказ в обслуживании(реализация DoS-атаки) | A | Serious | Средний |
| 3 | №1 | Перехват трафика | A | Minor | Низкий |
| 4 | №2 | отказ в обслуживании(реализация DoS-атаки) | С | Serious | Средний |
| 5 | №2 | Информационная разведка | C | Negligible | Низкий |
| 6 | №2 | Перехват трафика | A | Minor | Низкий |
| 7 | №3 | отказ оборудования (реализация DoS-атаки) | A | Serious | Средний |
| 8 | №3 | Перехват трафика | A | Negligible | Низкий |
| 9 | №3 | Информационная разведка | A | Negligible | Низкий |
| 10 | №4 | Перехват пароля авторизации | B | Moderate | Средний |
| 11 | №5 | Перехват трафика | A | Negligible | Низкий |
| 12 | №5E | Перехват пароля авторизации | E | Serious | Высокий |
| 13 | №5 | отказ в обслуживании (реализация DoS-атаки) | B | Serious | Средний |
| 14 | №5E | Информационная разведка | C | Negligible | Низкий |
| 15 | №6 | отказ в обслуживании(DoS-атака) | D | Serious | Средний |

Далее, используя таблицу 6, устанавливается уровень приемлемости рисков информационной безопасности.

Таблица 6. Уровень приемлемости риска

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Показатель уровня ущерба** | **Показатель вероятности реализации угрозы** | | | | |
| A | B | C | D | E |
| N (Negligible) | П | П | П | П | П |
| Mi (Minor) | П | П | П | Н | Н |
| Mo (Moderate) | П | Н | Н | Н | Н |
| S (Serious) | П | Н | Н | Н | Н |
| С (Critical) | П | Н | Н | Н | Н |

В конечном итоге осуществляется деление рисков информационной безопасности на приемлемые и неприемлемые (таблица 7).

Таблица 7. Приемлемые и неприемлемые риски

| **№ п/п** | **Приемлемые риски** | **Неприемлемые риски** |
| --- | --- | --- |
| 1 | №1. Информационная разведка | №2. Отказ в обслуживании (реализация DoS-атаки) |
| 2 | №1. Отказ в обслуживании (реализация DoS-атаки) | №3. Перехват пароля авторизации. |
| 3 | №1. Перехват трафика | №4. Перехват пароля авторизации |
| 4 | №2. Информационная разведка | №4. Отказ в обслуживании (реализация DoS-атаки) |
| 5 | №2. Перехват трафика | №5. Отказ в обслуживании(DoS-атака) |
| 6 | №2. Отказ оборудования (реализация DoS-атаки) |  |
| 7 | №3. Перехват трафика |  |
| 8 | №4.. Информационная разведка |  |
| 9 | №5. Перехват трафика |  |
| 10 | №6. Информационная разведка. |  |

По результатам проведённого анализа на следующем этапе создания СЗИ должны быть разработаны и реализованы меры по нейтрализации актуальных угроз в рамках проектируемой ЗТКС. Эти меры могут носить как технический, так и организационный характер.

**ЛАБОРАТОРНАЯ РАБОТА № 1**

**Название работы**

Анализ и классификация угроз информационной безопасности в ЗТКС.

**Цель**

Изучение методических основ анализа, моделирования и классификации угроз информационной безопасности, а также прогнозирования (анализа) рисков их осуществления в рамках создаваемых ЗТКС.

**ЗАДАНИЕ на выполнение лабораторной работы № 1:**

1. Изучить предлагаемый теоретический материал.
2. Ознакомиться с перечнем возможных угроз ИБ в соответствии с полученным заданием (так называемой «легендой») или, что является более предпочтительным, предложить собственный перечень угроз, выработанный самостоятельно на основе имеющегося опыта или априорных сведений практического характера.
3. Ознакомиться с порядком анализа и классификации угроз ИБ. Провести интерактивное обсуждение перечня возможных угроз с другими участниками своей рабочей группы с учётом распределения ролей. Провести анализ и классификацию возможных угроз.
4. Определить список наиболее актуальных угроз, оценить их степень их реального воздействия на создаваемую ЗТКС. Предложить рекомендации по их нейтрализации. Обосновать и защитить результаты анализа, ответить на вопросы.
5. Провести анализ рисков ИБ согласно списку наиболее актуальных угроз для проектируемой ЗТКС. Обосновать принятые решения в ходе их обсуждения с другими участниками своей рабочей группы с учётом распределения ролей.
6. Оформить отчёт по лабораторной работе в соответствии с заданием.
7. Ответить на вопросы преподавателя. Принять участие в общей дискуссии по результатам проведения данной деловой игры. По итогам деловой игры наиболее активные её участники премируются баллами в рамках существующей БРС.

### Контрольные вопросы

1. Для чего необходимо проводить анализ угроз при проектировании ЗТКС?
2. Какие основные типы угроз вы знаете?
3. Какие цели преследует классификация угроз ЗТКС?
4. Сформулируйте три базовых принципа борьбы с угрозами.
5. Для чего проводится мониторинг угроз?
6. Когда возникает необходимость в актуализации угроз ИБ?
7. Какова цель процедуры нейтрализации угроз в ЗТКС?
8. Для чего проводится оценка рисков ИБ в ЗТКС?
9. Охарактеризуйте качественную шкалу для оценки ущерба.
10. Охарактеризуйте таблицу для оценки уровня приемлемости риска.