СПбГЭТУ «ЛЭТИ»
ПЕРВЫЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ

Р.Р. Фаткиева

Основы построения защищенных компьютерных сетей

Виды нарушения сетевой безопасности

СПбГЭТУ «ЛЭТИ», 2021 г.

2. ВИДЫ НАРУШЕНИЙ СЕТЕВОЙ БЕЗОПАСНОСТИ

2.1 Обзор и анализ существующих стандартов в области обеспечения сетевого взаимодействия. Модель угроз и модель нарушителя информационной безопасности компьютерной сети

Отсутствие управления сетевой безопасностью приводит к формированию различных подходов к реагированию на тот или иной инцидент. При рассмотрении вопросов сетевой безопасности в настоящее время можно выделить два основных подхода:

Неформальный - комплекс вопросов построения защищённых сетей, который делится на основные направления, соответствующие угрозам, разрабатывается комплекс мер и механизмов защиты по каждому направлению.

Формальный основан на понятии политики сетевой безопасности и определении способов гарантирования выполнения её положений.

Неправильное применение этих механизмов регулирования и зон ответственности [1-13] дополнительно влечет нарушения сетевой. Проблема усугубляется тем, что имеется тенденция к использованию распределенной обработки данных, которая ослабляет эффективность централизованного контроля. Взаимодействие сетей общего пользования с частными сетями компаний, а также совместное использование информационных ресурсов затрудняет обеспечение безопасности и управление доступом к информации при нарушении работоспособности любой из подсистем.

Вследствие этого возникает необходимость оценки состояния сетевого взаимодействия в каждый момент времени для возможности управления состоянием безопасности. Однако в правовых актах отсутствуют методологические рекомендации по оценке информационной безопасности территориально распределенных сетей. Этот пробел, а также отсутствие иного четкого нормативного регулирования приводит к трудностям – при комплексной оценке комбинированных средств защиты и организационно-технических мер в отраслях критических технологий.

При формировании методологического подхода возникает сложность при выборе показателей и средств измерения. В законодательной базе [1-13] не

приводятся необходимые показатели защищенности, на основе которых возможно создание систем измерения и оценки информационной безопасности. Однако представленные методики не позволяют оценить систему как в целом, так и на каждом этапе жизненного цикла. В настоящее время отсутствует как перечень применяемых средств измерений и алгоритмов обработки их результатов. Также нет методов сравнения и выбора наилучшего варианта защиты при минимальных затратах на обеспечение безопасности. В связи с этим возникает необходимость создания частных моделей и методов нарушителей, механизмов функционирования сети и методов обеспечения ее безопасности. Для этого целесообразно рассмотреть возможные угрозы и уязвимости системы.

2.2 Сетевые атаки

Основными задачами, решаемыми в ходе оценки угроз безопасности и сетевых атак, являются [14]:

а) определение негативных последствий, которые могут наступить от реализации (возникновения) угроз безопасности информации;

б) инвентаризация систем и сетей и определение возможных объектов воздействия угроз безопасности информации;

в) определение источников угроз безопасности информации и оценка возможностей нарушителей по реализации угроз безопасности информации;

г) оценка способов реализации (возникновения) угроз безопасности информации;

д) оценка возможности реализации (возникновения) угроз безопасности информации и определение актуальности угроз безопасности информации;

е) оценка сценариев реализации угроз безопасности информации в системах и сетях.

Исходными данными для оценки угроз безопасности информации являются [14, рис 2.1]:

а) общий перечень угроз безопасности информации, содержащийся в банке данных угроз безопасности информации ФСТЭК России, а также отраслевые (ведомственные, корпоративные) модели угроз безопасности информации;

б) описания векторов (шаблоны) компьютерных атак, содержащиеся в базах данных и иных источниках, опубликованных в сети «Интернет» (CAPEC, ATT&CK, OWASP, STIX, WASC и др.);

в) документация на системы и сети;

г) нормативные правовые акты Российской Федерации, в соответствии с которыми создаются и функционируют системы и сети, содержащие в том числе описание назначения, задач (функций) систем и сетей, состав обрабатываемой информации и ее правовой режим;

д) технологические, производственные карты или иные документы, содержащие описание управленческих, организационных, производственных и иных основных процессов (бизнес-процессов) в рамках выполнения функций (полномочий) или осуществления видов деятельности обладателя информации, оператора (далее – основные (критические) процессы);

ж) результаты оценки рисков (ущерба), проведенной обладателем информации и (или) оператором.

Указанные исходные данные могут уточняться или дополняться с учетом особенностей области деятельности, в которой функционируют системы и сети.

Рис. 2.1

В ходе оценки угроз безопасности информации должны быть определены компоненты систем и сетей, несанкционированный доступ к

которым или воздействие на которые в ходе реализации (возникновения) угроз безопасности информации может привести к негативным последствиям – объекты воздействия [14] (рис 2.2)

Рис. 2.2

Для определенных информационных ресурсов и компонентов систем и сетей должны быть определены виды воздействия на них, которые могут привести к негативным последствиям. Основными видами таких воздействий являются, воздействия, представленные на рис. 2.3.

Рис. 2.3

При оценке угроз безопасности информации в системах и сетях, функционирующих на базе информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры, объекты воздействия определяются с учетом состава и содержания услуг (рис 2.4)

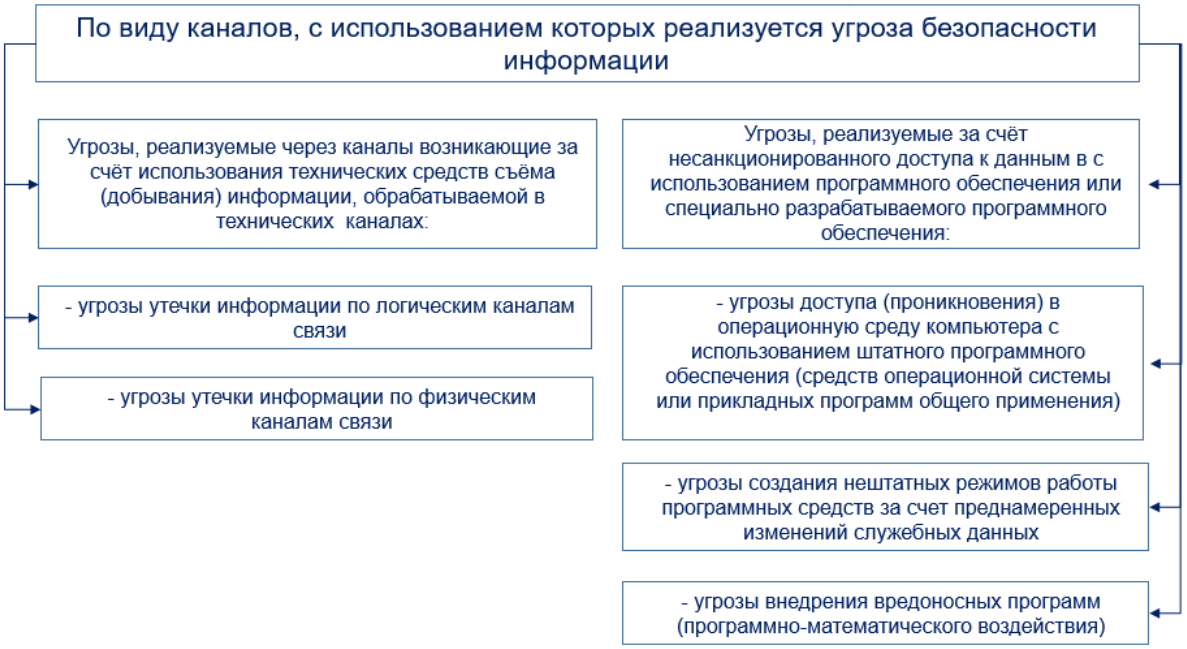

Рис. 2.4

В ходе оценки угроз безопасности информации должны быть определены возможные антропогенные источники угроз безопасности информации, к которым относятся лица (группа лиц), осуществляющие реализацию угроз безопасности информации путем несанкционированного доступа и (или) воздействия на информационные ресурсы и (или) компоненты систем и сетей, – актуальные нарушители (рис. 2.5)

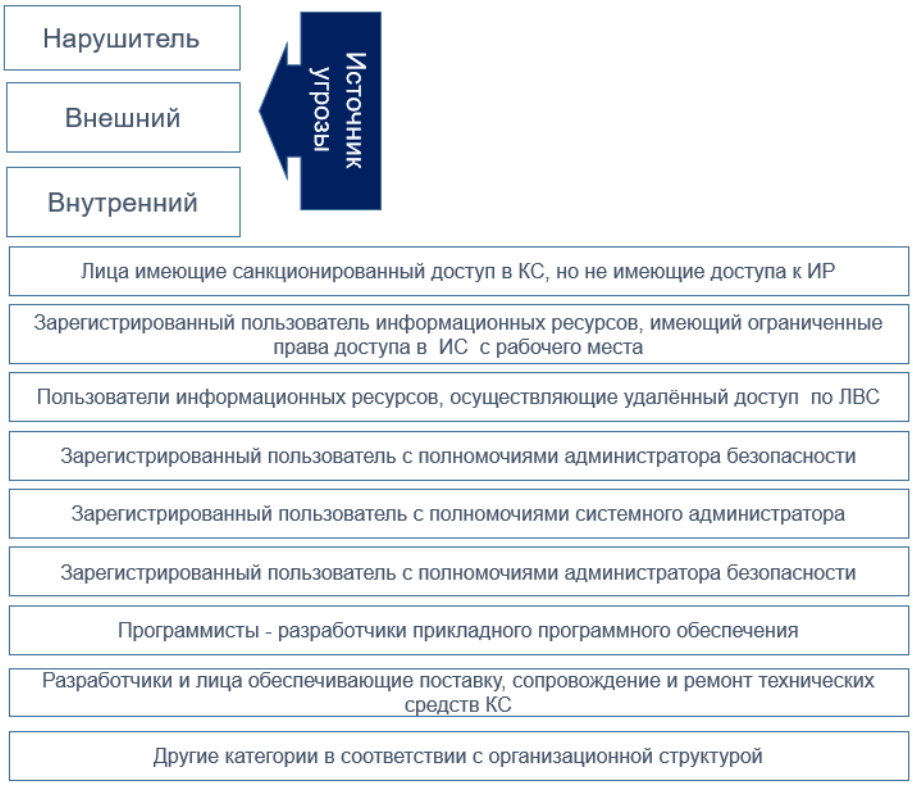

Рис. 2.5

В ходе оценки угроз безопасности информации должны быть определены возможные способы реализации угроз безопасности информации, за счет использования которых актуальными нарушителями могут быть реализованы угрозы безопасности информации в системах и сетях, – актуальные способы реализации (возникновения) угроз безопасности информации (рис 2.6)

Рис. 2.6

Атакой называется успешная или безуспешная реализация угрозы. Для осуществления атаки нарушитель разрабатывает сценарий, который состоящий из 3 этапов:

1. Разведка (сбор данных об атакуемой системе, выбор объекта, через который осуществляется атака, разработка сценария атаки).
2. Собственно атака (внедрение, повышение привилегий, использование ресурса). Наиболее сложное звено на данном этапе заключается в выборе в инструментального средства атаки. Выделяются следующие категории, представленные в таблице 1.

Таблица 1

Вид инструмента атаки	*Описание*
Пользовательская команда	Введение нарушителем команды в командной строке или графическом пользовательском интерфейсе
Сценарий или программа	сценарий или программа запущенные в пользовательском интерфейсе с целью воспользоваться уязвимостью компьютеров и сетей
Автономный агент	нарушитель использует программу или программный фрагмент, который вступает в действие независимо от

	пользователя с целью воспользоваться уязвимостью (вирусы, троянские кони)
Распределенные средства	нарушитель распределяет средства атаки по многим скоординированным узлам, с целью атаковать мишень одновременно из нескольких мест
Подслушивание данных	в тех местах, где электромагнитное излучение от несущего кабеля сетевого трафика или -компьютера "прослушивается" внешним устройством, или сетевой картой, компьютера, подключенного к сети.

3. Сокрытие следов и создание потайных ходов внедрение.

Противодействие атакам эффективно, как правило, лишь на первом этапе, для которого необходимо своевременно обнаруживать «бреши» (например обновлять антивирусную базу, или «бреши» ОС»). Для предотвращения разведки и собственно атаки необходимо осуществлять постоянный мониторинг системы.

2.3 Классификация сетевых атак

По принципу несанкционированного доступа:

- физический несанкционированный доступ;
- логический несанкционированный доступ.

По положению источника несанкционированного доступа:

- источник несанкционированного доступа, расположен в локальной сети. Данный вид атак как правило, осуществляется персоналом;
- источник несанкционированного доступа, расположен вне локальной сети. Это вид атак характерен для ситуации, когда объединяются отдельные сети, ориентированные на обработку конфиденциальной информации совершенно разного уровня секретности или разных категорий

В зависимости от источника:

- традиционные атаки:

атака один к одному- атака исходит из одного источника и достигает одной цели;

атака один ко многим- атака исходит из одного источника и достигает многих целей;

- распределенные атаки:

многие к одному – атака исходит из многих источников и достигает одной цели:

многие ко многим- атака исходит из многих источника и достигает 2 и более цели.

- гибридные атаки- использующие стратегии традиционных и распределенных атак

По режиму выполнения несанкционированного доступа:

- атаки, выполняемые при постоянном участии человека;
- атаки, выполняемые специально разработанными программами без непосредственного участия человека.

По типу используемых слабостей

- атаки, основанные на недостатках политики безопасности;
- атаки, основанные на ошибках административного управления компьютерной сетью;
- атаки, основанные на недостатках алгоритмов, реализованных в средствах защиты;
- атаки, основанные на ошибках реализации проекта системы защиты.

По пути несанкционированного доступа:

- атаки, с использованием прямого пути доступа к ресурсам;
- атаки с использованием скрытого пути доступа к ресурсам.

По объекту атаки:

- атаки на информацию, хранящуюся на внешних запоминающих устройствах;
- атаки на информацию, и протоколы передаваемые по линиям связи;
- атаки на информацию, обрабатываемую в основной памяти компьютера.
- атаки на политику безопасности и процесс административного управления;
- атаки на компоненты системы защиты;

По характеру воздействия:

- пассивное воздействие- не оказывает непосредственного влияния на систему (прослушивание канала связи в сети). При этом нарушитель не оставляет никаких следов.
- активное- оказывает непосредственное влияние на работу системы (изменение конфигурации, нарушение работоспособности и т. д.). Особенностью активного воздействия по сравнению с пассивным

является возможность его обнаружения, так как в результате его осуществления в системе происходят видимые изменения.

По цели воздействия

- нарушение конфиденциальности информации (перехват информации при прослушивании сети);
- нарушение целостности информации (искажение информации);
- нарушение работоспособности (доступности) системы (отказ в доступе легальным пользователям).

По условию начала осуществления воздействия

- атака по запросу от атакуемого объекта –условие начала осуществления воздействия является запрос от пользователя (DNS- и ARP-запросы в стеке TCP/IP);
- атака по наступлению ожидаемого события на атакуемом объекте (пятница 13)
- безусловная атака–осуществляется немедленно и безотносительно к состоянию системы и атакуемого объекта

По наличию обратной связи с атакуемым объектом

- с обратной связью – для более эффективной атаки, нарушителю требуется получение ответов, для реакции на изменения, происходящие на атакуемой системе;
- без обратной связи - атака, происходящая без реакции на поведение атакуемой системы (отказ в обслуживании (DoS)).

2.4 Механизмы реализации атак в сетях

Для каждой возможной угрозы безопасности информации определяется множество возможных сценариев ее реализации в интересах оценки эффективности принятых технических мер по защите информации (обеспечению безопасности), в том числе средств защиты информации. При этом множество сценариев определяется для каждого актуального нарушителя и уровней его возможностей в соответствии с полученными результатами инвентаризации систем и сетей, анализа уязвимостей и (или) тестирования на проникновение, проведенных с использованием автоматизированных средств ([14], рис. 2.7).

Рис. 2.7

2.5 Формирование требования к средствам защиты при построении защищённых компьютерных сетей

Оценка значимости угроз и атак позволяет сформировать основные требования к средствам защиты при реализации сетевого взаимодействия. В [12] к средствам обеспечения безопасности сетевого взаимодействия предъявляются следующие требования:

- обеспечению логической сегментации сети;
- ограничению трафика, проходящий между логическими сетями;
- контролю доступа к сети организации;
- регистрации трафика для последующего аудита;
- -сокрытия архитектуры внутренней сети, узлов и приложений;
- предоставлению возможности для упрощения выполнения действий по управлению сетью.

2.6 Основные этапы разработки проектных решений по системам обеспечения информационной безопасности на базе компьютерных сетей

Общий процесс достижения и поддержки необходимой сетевой безопасности можно кратко изложить процессом, состоящим из этапов:

1. Рассмотрение корпоративной политики информационной безопасности с целью получения подробностей о любых связанных с сетями рисках, которые всегда будут рассматриваться как высокие, и мерах,

средствах контроля и управления сетевой безопасностью, которые должны быть реализованы.

2. ***Определение области/контекста оценки рисков безопасности***, включающий сбор информации о текущей и (или) планируемой сетевой среде (рассмотрение корпоративной политики информационной безопасности на предмет формулировок о рисках: сбор и проверка информации о текущей и (или) планируемой сети (сетях), архитектуре, приложениях, видов соединений и другие характеристики для оценки рисков и определению того, что является возможным с точки зрения специализированной архитектуры/проекта сетевой безопасности); сбор информации об угрозах и уязвимостях сетевой инфраструктуры.

3. Идентификация и оценка рисков сетевой безопасности и соответствующих потенциальных областей действия мер и средств контроля и управления. На данном этапе производится осуществление оценки риска сетевой безопасности и проводимой руководством проверки с использованием информации о риске и оценки рисков, связанных с потенциальными нарушениями значимых предписаний и законов, касающихся сетевых соединений, которые определены соответствующими регулирующими или законодательными органами (рис 2.8).

Оценка риска сетевой безопасности должна проводиться в соответствии с рекомендациями, представленными в ИСО/МЭК 27001, ИСО/МЭК 27002 и ИСО/МЭК 27005. Для этого осуществляется:

- Определение степени значимости информации и услуг, выраженной с точки зрения потенциального неблагоприятного воздействия на основную деятельность организации в случае возникновения нежелательных инцидентов (оценка активов);

- идентификация и оценка вероятности или уровней угроз, направленных против информации и услуг;

- идентификация и оценка степени серьезности или уровня уязвимостей (слабых мест), которые могли бы быть использованы идентифицированными угрозами;

- оценка величины рисков, основывающихся на определенных последствиях потенциального неблагоприятного воздействия на операции деятельности организации и уровнях угроз и уязвимостей;

- идентификация аспектов специализированной архитектуры/проекта безопасности и оправданных потенциальных областей действия мер и средств контроля и управления безопасностью, необходимых для обеспечения того, чтобы оцененные риски оставались в допустимых пределах.

Рис. 2.7 [10]

4. Идентификация поддерживающих мер и средств контроля и управления безопасностью - технических и нетехнических - применяемых не только к сетям.

5. Рассмотрение вариантов специализированной архитектуры/проекта сетевой безопасности с учетом сетевых сценариев и вопросов сетевых «технологий», выбором и документированием предпочтительной специализированной архитектуры/проекта безопасности и связанных с ними мер и средств контроля и управления безопасностью.

6. Разработка и тестирование комплекса программных и технических средств и услуг по обеспечению безопасности;

7. Реализация и эксплуатация мер и средств контроля и управления безопасностью;

8. Мониторинг и проверка реализации (мониторинг и проверка мер и средств контроля и управления, необходимых для соблюдения соответствующих предписаний и законов, связанных с сетевыми соединениями, которые определены соответствующими регулирующими или законодательными органами (включая органы исполнительной власти).

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.06 № 149-ФЗ;
2. Федеральный закон «О государственной тайне» от 21.09.93 № 182;
3. Стратегия национальной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 31 декабря 2015 г. N 683;
4. Стратегия развития информационного общества в Российской Федерации на 2017–2030 гг. Утверждена Указом Президента Российской Федерации от 09.05.2017 № 203
5. ГОСТ Р ИСО/МЭК 15408-1-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.
6. ГОСТ Р ИСО/МЭК 15408-2-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности.
7. ГОСТ Р ИСО/МЭК 15408-3-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности.
8. ГОСТ Р ИСО/МЭК 15408 — Общие критерии оценки безопасности информационных технологий.
9. ГОСТ Р ИСО/МЭК 27002 — Информационные технологии. Практические правила управления информационной безопасностью. ГОСТ Р ИСО/МЭК 27001 — Информационные технологии. Методы безопасности. Система

управления безопасностью информации. Требования. Руководящие документы Гостехкомиссии России.

10. ГОСТ Р ИСО/МЭК 27033-1-2011. Национальный стандарт российской федерации. Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции.
11. ГОСТ Р ИСО/МЭК 27033-3-2014. Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления.
12. ГОСТ Р ИСО/МЭК 27033-4-2021 "Информационные технологии. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 4. Обеспечение безопасности межсетевого взаимодействия с использованием шлюзов безопасности" утвержден приказом Росстандарта от 19 мая 2021 года N 391-ст.
13. ГОСТ Р 56045-2021 "Информационные технологии. Методы и средства обеспечения безопасности. Рекомендации по оценке мер обеспечения информационной безопасности" утвержден приказом Росстандарта от 20 мая 2021 года N 421-ст.
14. Методический документ "Методика оценки угроз безопасности информации" (утв. Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г.)