ЛЕКЦИЯ №3 **Перечень опасных событий. Модели угроз, нарушителя и модель защиты**

ЛЕКЦИЯ №3 Перечень опасных событий. Модели угроз, нарушителя и модель защиты.

Для определения необходимых мер по обеспечению информационной безопасности информационно-телекоммуникационных систем необходимо обладать информацией о потенциальных нарушителях, их ресурсах, возможностях и реализуемых угрозах (на уровне предположений).

ЛЕКЦИЯ №3 Перечень опасных событий. Модели угроз, нарушителя и модель защиты.

Учебные вопросы:

1. **Типы нарушителей**
2. **Модель угроз**
3. **Модель защиты**

ЛЕКЦИЯ №3 Перечень опасных событий. Модели угроз, нарушителя и модель защиты.

Для формирования профиля возможных нарушителей необходимо выдвинуть гипотезы об их возможностях по реализации компьютерных атак (КА) на телекоммуникационное оборудование и систему управления телекоммуникационным оборудованием. Нарушителей будем обозначать H_1, H_2, … и т.д.

ЛЕКЦИЯ №3 Перечень опасных событий. Модели угроз, нарушителя и модель защиты.

При классификации будем исходить из того, что может быть 2 класса нарушителей - внешний нарушитель (группа нарушителей) и внутренний нарушитель (группа нарушителей)

H_1 - внутренний нарушитель (группа нарушителей). К данному классу относятся сотрудники предприятий, не являющиеся зарегистрированными пользователями и не допущенные к оборудованию, но имеющие санкционированный доступ в КЗ. (сотрудники различных структурных подразделений предприятий: энергетики, сантехники, уборщицы, сотрудники охраны и другие лица, обеспечивающие нормальное функционирование объекта информатизации).

H_2 - внутренний нарушитель (группа нарушителей). К данному классу относятся зарегистрированные пользователи сети связи, осуществляющие локальный доступ к оборудованию с рабочего места (сотрудники предприятий, имеющие право доступа к ТКО для выполнения своих должностных обязанностей).

H_3- внутренний нарушитель (группа нарушителей). К данному классу относятся зарегистрированные пользователи, осуществляющие удаленный доступ к ТКО по локальной или распределенной сети предприятий.

H_4- внутренний нарушитель (группа нарушителей). К данному классу относятся зарегистрированные пользователи с полномочиями администратора безопасности сегмента (фрагмента) сети связи.

H_5 - внутренний нарушитель (группа нарушителей). К данному классу относятся зарегистрированные пользователи с полномочиями системного администратора, выполняющего конфигурирование и управление программным обеспечением и оборудованием, включая оборудование, отвечающее за безопасность защищаемого объекта: средства мониторинга, регистрации, архивации, защиты от несанкционированного доступа.

H_6 - внутренний нарушитель (группа нарушителей). К данному классу относятся зарегистрированные пользователи с полномочиями администратора безопасности, отвечающего за соблюдение правил разграничения доступа, за генерацию ключевых элементов, смену паролей, криптографическую защиту информации.

H_7- внешний нарушитель (группа нарушителей). К данному классу относятся лица из числа программистов-разработчиков сторонней организации, являющихся поставщиками ПО

H_8 - внешний нарушитель (группа нарушителей). К данному классу относятся персонал, обеспечивающий поставку, сопровождение и ремонт оборудования.

H_9- внешний нарушитель (группа нарушителей). К данному классу относятся специалисты зарубежных специальных служб.

Необходимо отметить, что возможен сговор между внутренними и внешними нарушителями!

Далее необходимо выдвинуть гипотезы в виде общего перечня возможностей нарушителей. Такие возможности будем обозначать B_1, B_2, … и т.д.

ЛЕКЦИЯ №3 Перечень опасных событий. Модели угроз, нарушителя и модель защиты.

B1. Знание полного комплекта технической документации на ТКО и СУ ТКО.

B2. Знание типовых схем администрирования (как управляется ТКО).

B3. Знание принципов конфигурирования ТКО по стандартным протоколам управления и маршрутизации в сетях.

B4. Наличие исходных текстов (исходный код) ПО для ТКО

B5. Наличие готовых образцов ПО (скомпилированные) для ТКО.

B6. Наличие станции управления (ПЭВМ), подключаемой непосредственно к ТКО.

ЛЕКЦИЯ №3 Перечень опасных событий. Модели угроз, нарушителя и модель защиты.

В7. Наличие подключения к оборудованию, не являющемуся станцией управления ТКО, но входящей в состав сети связи.

В8. Наличие средств разработки и отладки средств вычислительной техники.

В9. Наличие распределенных вычислительных ресурсов сети, включая глобальные сети.

В10. Наличие аппаратно-программных средств перехвата паролей в информационном потоке.

В11. Наличие оборудования подключения к магистральному волоконно-оптическому кабелю и электрическому кабелю.

В12. Наличие технических средства передачи специализированных команд по сети электропитания, радио и иным каналам.

ЛЕКЦИЯ №3 Перечень опасных событий. Модели угроз, нарушителя и модель защиты.

При рассмотрении возможностей нарушителей необходимо также учитывать ограничения, т.е. полноту, достоверность и значимость таких сведений. Для этого необходимо выдвинуть гипотезы в виде общего перечня ограничений, их будем обозначать О1, О2 … и т.д.

ЛЕКЦИЯ №3 Перечень опасных событий. Модели угроз, нарушителя и модель защиты.

О1. Общедоступные источники информации (документация на ТКО, распространяемая на официальный сайтах, ресурсы сети – форумы, учебные пособия и т.д.)

О2. Общедоступное оборудование для организации КА (находящиеся в открытой продаже ПЭВМ и их комплектующие).

О3. Общедоступное программное обеспечение для организации КА (программы для определения уровня защищенности сетей связи).

О4. Конструкторская документация, имеющая ограничительные пометки (конфиденциально, строго конфиденциально и т.д.), а также объектовые схемы, инструкции и другие документы.

О5. Специализированное оборудования и программное обеспечение (специально разработанная ПЭВМ, контрольно-измерительное оборудование и др.);

Таким образом, набором (Н, В, О) можно задать профиль потенциального нарушителя. Данный профиль формируется путем анализа документации на оборудование (функциональные возможности), изучения рынка наложенных средств обеспечения информационной безопасности, исследованием теоретических основ организации компьютерных атак и т.д.

Перечень опасных событий

ЛЕКЦИЯ №3 Перечень опасных событий. Модели угроз, нарушителя и модель защиты.

Для формирования перечня опасных событий определим основные состояния защищенности ь информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.

ГОСТ Р 50922-2006 "Защита информации. Основные термины и определения" вводит понятие ИБ как состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность.

ЛЕКЦИЯ №3 Перечень опасных событий. Модели угроз, нарушителя и модель защиты.

- угрозы нарушения конфиденциальности информации, в результате реализации которых информация становится доступной субъекту, не располагающему полномочиями для ознакомления с ней;
- угрозы нарушения целостности информации, к которым относится любое злонамеренное искажение информации, обрабатываемой с использованием автоматизированных систем;
- угрозы нарушения доступности информации, возникающие в тех случаях, когда доступ к некоторому ресурсу АС для легальных пользователей блокируется.

Отметим, что реальные угрозы ИБ далеко не всегда можно строго отнести к какой-то одной из перечисленных категорий.

Выделяют два основных метода перечисления угроз:

- построение произвольных списков угроз. Возможные угрозы выявляются экспертным путём и фиксируются случайным и неструктурированным образом. Для данного подхода характерны неполнота и противоречивость получаемых результатов;

- построение деревьев угроз. Угрозы описываются в виде одного или нескольких деревьев. Детализация угроз осуществляется сверху вниз, и в конечном итоге каждый лист дерева даёт описание конкретной угрозы. ***Знание возможных угроз, а также уязвимых мест защиты, которые эти угрозы обычно эксплуатируют, необходимо для того, чтобы выбирать наиболее эффективные средства обеспечения безопасности.***

ЛЕКЦИЯ №3 Перечень опасных событий. Модели угроз, нарушителя и модель защиты.

К наиболее распространенным угрозам безопасности относят:

- несанкционированный доступ, который заключается в получении пользователем доступа к ресурсу, на который у него нет разрешения в соответствии с принятой политикой безопасности;
- отказ в обслуживании, который представляет собой преднамеренную блокировку легального доступа к информации и другим ресурсам;
- незаконное использование привилегий;

- «скрытые каналы». Представляют собой пути передачи информации между процессами системы, нарушающие системную политику безопасности. «Скрытые каналы» могут быть реализованы различными путями, в частности при помощи программных закладок;

- «маскарад». Под «маскарадом» понимается выполнение каких-либо действий одним пользователем от имени другого пользователя;

- «сборка мусора». После окончания работы обрабатываемая информация не всегда полностью удаляется из памяти оборудования. Данные хранятся на носителе до перезаписи, стирания, выключения и т.д.;

- «люки». Представляют собой скрытую, недокументированную точку входа в программный модуль. «Люки» относятся к категории угроз, появляющихся вследствие ошибок реализации какого-либо проекта (системы в целом, комплекса программ и т. д.);

- вредоносные программы. Эти программы прямо или косвенно дезорганизуют процесс обработки информации или способствуют утечке или искажению информации.

ЛЕКЦИЯ №3 Перечень опасных событий. Модели угроз, нарушителя и модель защиты.

К самым распространенным видам вредоносных программ относятся:

- «вирус» – это программа, которая способна заражать другие программы, модифицируя их так, чтобы они включали в себя копию вируса;

- «троянский конь» – программа, которая содержит скрытый или явный программный код, при исполнении которого нарушается функционирование системы безопасности.

- «жадная» программа – программа, которая захватывает (монополизирует) отдельные ресурсы вычислительной системы, не давая другим программам возможности их использовать;

- «бактерия» – программа, которая делает копии самой себя и становится паразитом, перегружая память компьютера и процессор;
- «логическая бомба» – программа, приводящая к повреждению файлов или компьютеров (от искажения данных – до полного уничтожения данных).

Также к классу вредоносных программ можно отнести «снифферы» (программы, перехватывающие сетевые пакеты), программы подбора паролей, атаки на переполнение буфера и т.д.

Перечисленные атаки зачастую используются совместно для реализации комплексных атак.

ЛЕКЦИЯ №3 Перечень опасных событий. Модели угроз, нарушителя и модель защиты.

Рассмотрим более подробно возможные компьютерные атаки на телекоммуникационное оборудование. В общем случае программное обеспечение любого современного телекоммуникационного оборудования состоит из следующих основных компонентов

- ***операционная система***, выполняющая функции по управлению программно-аппаратными средствами ТКО;
- ***встроенные средства управления***, представляющие собой интерфейсы передачи данных между операционной системой и внешними средствами управления (например, ПЭВМ управления);
- ***базовые протоколы передачи данных***, являющимися реализацией стандартных правил сетевого взаимодействия для обработки (приема/передачи) данных;

- ***надстройки базовых протоколов***, являющимися реализацией дополнительных функциональных возможностей протоколов сетевого взаимодействия, реализуемых различными фирмами-производителями;

- ***конфигурационные файлы***, представляющие собой текстовые файлы, содержащие всю необходимую информацию для штатного функционирования устройства (набор инструкций).

ЛЕКЦИЯ №3 Перечень опасных событий. Модели угроз, нарушителя и модель защиты.

Поэтому все попытки взлома защиты можно разделить на:

- кража пароля путем подглядывания за легальным пользованием во время ввода пароля на право работы с ОС; путем получения пароля из файла, в котором этот пароль был сохранен; путем кражи внешнего носителя парольной информации;

- подбор пароля путем: полного перебора всех возможных вариантов пароля; оптимизированного перебора вариантов пароля (по частоте встречаемости символов, с помощью словарей наиболее часто применяемых паролей, с использованием информации о конкретном пользователе и т.д.;

- сборка "мусора", а именно восстановление ранее удаленных объектов;

- превышение полномочий, предоставленных в соответствии с действующей политикой безопасности, используя ошибки в программном обеспечении или в администрировании ОС;

- отказ в обслуживании (целью этой атаки является частичный или полный вывод ОС из строя), достигается захватом ресурсов, бомбардировкой запросами; использованием ошибок в программном обеспечении или администрировании.

- анализ сетевого трафика. Данный вид атаки направлен в первую очередь на получение пароля и идентификатора пользователя путем "прослушивания сети". Реализуется это с помощью «сниффера», которая перехватывает все пакеты, идущие по сети. И если, протокол передает аутентификационную информацию в открытом виде, то злоумышленник легко получает доступ к учетной записи пользователя;

- сканирование сети. Суть данной атаки состоит в сборе информации о топологии сети, об открытых портах, используемых протоколах и т. п. Как правило, реализация данной угрозы предшествует дальнейшим действиям злоумышленника с использованием полученных в результате сканирования данных;

- навязывание ложного маршрута сети. Данная атака стала возможной из-за недостатков протоколов маршрутизации (RIP, OSPF, LSP) и управления сетью (ICMP, SNMP), таких как слабая аутентификация маршрутизаторов. Суть атаки состоит в том, что злоумышленник, используя уязвимости протоколов, вносит несанкционированные изменения в маршрутно-адресные таблицы;

- внедрение ложного объекта сети. Когда изначально объекты сети не знают информацию друг о друге, то для построения адресных таблиц и последующего взаимодействия используется механизм запроса (как правило, широковещательный) - ответ с искомой информацией. При этом если нарушитель перехватил такой запрос, то он может выдать ложный ответ, изменить таблицу маршрутизации всей сети, и выдать себя за легального субъекта сети. В дальнейшем все пакеты, направленные к легальному субъекту, будут проходить через злоумышленника;

- атаки с использованием сетевых сканеров — тип атак, основанных на использовании сетевых сканеров — программ, которые анализируют топологию сети и обнаруживают сервисы, доступные для атаки;

- атаки с использованием сканеров уязвимостей — тип атак, основанных на использовании сканеров уязвимостей — программ, осуществляющих поиск уязвимостей на узлах сети, которые в дальнейшем могут быть применены для реализации сетевых атак;

ЛЕКЦИЯ №3 Перечень опасных событий. Модели угроз, нарушителя и модель защиты.

В соответствии с сформулированными выше моделями угроз безопасности и нарушителя определён перечень факторов, обусловливающих актуальные угрозы информационной безопасности

ЛЕКЦИЯ №3 Перечень опасных событий. Модели угроз, нарушителя и модель защиты.

Угроза	Содержание фактора	Описание угрозы
y1	Передача сигналов по проводным (оптико-волоконным) линиям связи	Создание условий для реализации угроз, создаваемых другими факторами
y2	Паразитное электромагнитное излучение, модулируемое информационными сигналами	Нарушение конфиденциальности ресурсов
y3	Дефекты, сбои и отказы, аварии ТКО и инженерных систем объектов и сооружений связи	Нарушение доступности ресурсов, конфиденциальности и целостности
y4	Дефекты, сбои и отказы программного обеспечения ТКО, узлов связи	Нарушение доступности ресурсов конфиденциальности и целостности ресурсов.
y5	Разглашение защищаемой информации лицами, имеющими к ней право доступа, через утрату носителя информации	Нарушение конфиденциальности ресурсов
y6	Неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации, путем несанкционированного изменения информации	Нарушение целостности ресурсов

ЛЕКЦИЯ №3 Перечень опасных событий. Модели угроз, нарушителя и модель защиты.

Угроза	Содержание фактора	Описание угрозы
y7	Несанкционированный доступ внутреннего нарушителя к информации путем подключения к техническим средствам и системам узла связи	Нарушение доступности ресурса, конфиденциальности
y8	Несанкционированный доступ внутреннего нарушителя к информации через маскировку под зарегистрированного пользователя	Нарушение конфиденциальности ресурса
y9	Несанкционированный доступ внутреннего нарушителя к информации путем применение вирусов или другого вредоносного программного кода	Нарушение доступности ресурса, конфиденциальности, доступности
y10	Несанкционированный доступ внутреннего нарушителя к информации путем хищения носителя защищаемой информации	Нарушение конфиденциальности ресурсов
y11	Несанкционированный доступ внутреннего нарушителя к информации путем нарушения функционирования ТКО	Нарушение доступности ресурса, конфиденциальности, доступности
y12	Ошибки пользователей и технического персонала эксплуатирующей организации	Нарушение доступности ресурса конфиденциальности, доступности.

ЛЕКЦИЯ №3 Перечень опасных событий. Модели угроз, нарушителя и модель защиты.

Угроза	Содержание фактора	Описание угрозы
y13	Доступ внешнего нарушителя к защищаемой информации с применением технических средств разведки	Нарушение конфиденциальности ресурсов
y14	Несанкционированный доступ внешнего нарушителя к защищаемой информации путем подключения к техническим средствам и системам	Нарушение конфиденциальности.
y15	Несанкционированный доступ внешнего нарушителя к защищаемой информации путем использования закладочных устройств	Нарушение доступности ресурсов, конфиденциальности.
y16	Блокирование доступа к защищаемой информации путем перегрузки средств вычислительной техники и телекоммуникационного оборудования ложными заявками на ее обработку, передаваемыми на 2-7 уровнях эталонной модели взаимодействия открытых систем	Нарушение доступности ресурса
y17	Искажение, уничтожение или блокирование информации внешним нарушителем с применением технических средств путем использования программных или программно-аппаратных средств при осуществлении компьютерной атаки	Нарушение доступности ресурсов и целостности

Модель защиты

ЛЕКЦИЯ №3 Перечень опасных событий. Модели угроз, нарушителя и модель защиты.

С учетом рассмотренных выше возможных действий нарушителя был определен перечень конкретных угроз состоянию информационной безопасности ТКО. Для противодействия определенным угрозам необходимо применение соответствующего комплекса организационно-технических мер.

Данные меры формируются путем анализа каждой сформированной угрозы с точки зрения ее устранения организационно-правовым (организация пропускного режима, наличие инструкций по настройке оборудования и т.д.) или техническим мероприятием (функциональная возможность программного продукта, к примеру, антивируса)

Перечень мероприятий по предупреждению, обнаружению и ликвидации последствий компьютерных атак на ТКО приведен в таблице 2

№ п/п	Наименование мероприятия
По предупреждению компьютерных атак	
1.	Обеспечение криптографической защиты информации управления и мониторинга ТКО
2.	Применение сертифицированных антивирусных средств (система сертификации ФСБ России)
3.	Организация постоянного обновления применяемых в системе управления ТКО антивирусных средств (баз данных антивирусных средств).
4.	Специальная проверка и специальные исследования ТКО или применение сертифицированного оборудования (системы сертификации ФСБ России или ФСТЭК России, Минобороны).
5.	Предотвращение создания условий для возникновения источников компьютерных атак при доступе физических лиц, не имеющих на это права: а) на узлы связи:
5.1	1) оснащение сооружений связи узлов связи техническими средствами защиты, включая ограждения и охранную сигнализацию;
5.2	2) организация контрольно-пропускного режима внутри сооружений связи узлов связи;
5.3	3) оснащение сооружений связи средствами контроля доступа, видеонаблюдения, запирающими устройствами;
	б) к оборудованию, не входящему в состав узлов связи:
5.4	1) размещение линий связи, исключающее возможность доступа к ним без использования каких-либо инструментов и механизмов;
5.5	2) применение мер технического характера по обнаружению несанкционированных подключений к линиям связи;
5.6	3) регулярный осмотр линий связи и ведение журнала осмотра

№ п/п	Наименование мероприятия
По предупреждению компьютерных атак	
6.	Предотвращение создания условий для возникновения источников компьютерных атак при несанкционированном доступе к программным средствам узлов связи:
6.1	а) аутентификация персонала при доступе;
6.2	б) разграничение прав доступа персонала различных категорий
7.	Обеспечение возможности автоматического блокирования передачи пакетов и блокирования линейных интерфейсов телекоммуникационного оборудования при обнаружении признаков сетевых атак
8.	Обеспечение, посредством системы подбора кадров для работы с ТКО, совокупности профилактических и оперативных режимных мероприятий, условий, при которых минимальна вероятность появления внутреннего нарушителя
9.	Организация надежного хранения носителей информации с резервными (архивными) копиями программного обеспечения и конфигурационных данных, исключающее их хищение, подмену, уничтожение
10.	Проведение ремонтных и профилактических работ только организациями, имеющими соответствующие лицензии, либо сотрудниками эксплуатирующих подразделений ТКО
11.	Восстановление программного обеспечения, конфигурационных данных и настроек телекоммуникационного оборудования с резервных (архивных) копий при приеме оборудования из ремонта
12.	Периодический инспекционный контроль объектов связи с целью оценки защищенности от компьютерных атак

№ п/п	Наименование мероприятия
По обнаружению компьютерных атак	
13.	Разработка и документирование процедур по реагированию при обнаружении компьютерных атак
14.	Регистрация и последующий анализ фактов (попыток) несанкционированного доступа к программным средствам и защищаемой информации
15.	Периодический контроль целостности программного обеспечения, конфигурационных данных и настроек
16.	Мониторинг параметров информационной безопасности ТКО, идентификация атак
По ликвидации последствий компьютерных атак	
17.	Разработка и документирование процедур по ликвидации возможных последствий компьютерных атак
18.	Восстановление программного обеспечения, конфигурационных данных и настроек телекоммуникационного оборудования с резервных (архивных) копий при обнаружении нарушения их целостности
19.	Обеспечение переключения телекоммуникационного оборудования на обходные (резервные) направления связи при блокировании линейных интерфейсов по признакам сетевых атак
20.	Разработка и документирование процедур по ликвидации возможных последствий компьютерных атак