Конспект по справочному материалы 14 практики.

Определение угроз безопасности информации. (Этапы).

1. Определение негативных последствий
    a. Анализ документации систем и сетей исходных данных.
    b. Определение негат. последствий от реализации угроз.
2. Определение объектов воздействий
    a. Анализ документации систем и сетей исходных данных.
    b. Инвентаризация систем и сетей
    c. Определение групп информационных ресурсов и компонентов систем и сетей
3. Оценка возможности реализации угроз и их актуальности
    a. Определение источников угроз
    b. Оценка способов реализации угроз
    c. Оценка актуальности угроз

Алгоритм определения угроз безопасности информации при ее обработке в ИС:

1. Сбор исходных данных для определения угроз безопасности информации.
2. Анализ возможных уязвимостей информационной системы.
3. Анализ возможных способов реализации угроз безопасности информации.
4. Анализ последствий от реализации угроз безопасности информации.
5. Формирование перечня актуальных угроз безопасности информации.

Банк данных угроз безопасности информации включает базу данных уязвимостей программного обеспечения, а также перечень и описание угроз безопасности информации, наиболее характерных для государственных информационных систем, информационных систем персональных данных и автоматизированных систем управления производственными и технологическими процессами на критически важных объектах. Доступ к банку данных угроз безопасности информации осуществляется через сеть «Интернет» (адрес: www.bdu.fstec.ru).

Информация по уязвимостям:

-идентификатор уязвимости;

-описание уязвимости;

-наименование программного обеспечения, в котором возможна уязвимость;
-версия программного обеспечения;
-базовый вектор уязвимости, определяемый с учетом национальных стандартов в области защиты информации;
-уровень опасности уязвимости;
-возможные меры по устранению уязвимости;
-статус уязвимости;
-наличие специальной программы для эксплуатации уязвимости;
-информация об устранении уязвимости разработчиком;
-источники, в которых опубликованы сведения об уязвимости;
идентификаторы иных систем описаний уязвимости

Информация по угрозам:
-идентификатор угрозы безопасности информации;
-описание угрозы безопасности информации;
-источник угрозы безопасности информации;
-объект, на который может быть направлена угроза безопасности информации;
-возможные последствия от реализации угрозы безопасности информации.

Источниками угроз несанкционированного доступа (НСД) являются нарушитель(внешний или внутренний), носитель вредоносной программы и аппаратная закладка.

Возможности нарушителей (модель нарушителя)
С учетом наличия прав доступа и возможностей по доступу к информации и (или) к компонентам информационной системы нарушители подразделяются на два типа:
внешние нарушители (тип I) – лица, не имеющие права доступа к информационной системе, ее отдельным компонентам и реализующие угрозы безопасности информации из-за границ информационной системы;

1. Специальные службы ин. государств.
2. Террористические, экономические группировки
3. Криминальные структуры.
4. Отдельные физ.лица хакеры
5. Конкурирующие организации
6. Бывшие работники

7. Лица поставляющие ПО

внутренние нарушители (тип II) – лица, имеющие право постоянного или разового доступа к информационной системе, ее отдельным компонентам.
Наибольшими возможностями по реализации угроз безопасности обладают **внутренние** нарушители.

1. Разработчики ПО
2. Поставщики вычислительных услуг, услуг связи
3. Лица настраивающие оборудование
4. Лица обеспечивающие функционирование систем и сетей
5. Авторизованные пользователи
6. Системные администраторы

Наибольшими возможностями по реализации угроз безопасности обладают внутренние нарушители. Возможности внутреннего нарушителя существенным образом зависят от установленного порядка допуска физических лиц к информационной системе и ее компонентам, а также мер по контролю за доступом и работой этих лиц. Внешний нарушитель рассматривается, если имеется подключение информационной системы к внешним информационно-телекоммуникационным сетям.

Оценка возможностей нарушителей

- Возможности по реализации угроз безопасности информации нарушителя с **базовым низким потенциалом**:

Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы, опубликованную в общедоступных источниках. Имеют возможность получить информацию о методах и средствах реализации угроз безопасности информации (компьютерных атак), опубликованных в общедоступных источниках, и (или) самостоятельно осуществляет создание методов и средств реализации атак и реализацию атак на информационную систему.

- Возможности по реализации угроз безопасности информации нарушителя с базовым **повышенным (средним) потенциалом**:

Обладают всеми возможностями нарушителей с базовым потенциалом. Имеют осведомленность о мерах защиты информации, применяемых в информационной системе данного типа. Имеют возможность получить информацию об уязвимостях отдельных компонент информационной системы путем проведения, с использованием имеющихся в свободном

доступе программных средств, анализа кода прикладного программного обеспечения и отдельных программных компонент общесистемного программного обеспечения. Имеют доступ к сведениям о структурно-функциональных характеристиках и особенностях функционирования информационной системы.

- Нарушителями с **высоким потенциалом** являются специальные службы иностранных государств (блоков государств).

Обладают всеми возможностями нарушителей с базовым и базовым повышенным потенциалами. Имеют возможность осуществлять несанкционированный доступ из выделенных (ведомственных, корпоративных) сетей связи, к которым возможен физический доступ (незащищенных организационными мерами). Имеют возможность получить доступ к программному обеспечению чипсетов (микропрограммам), системному и прикладному программному обеспечению, телекоммуникационному оборудованию и другим программно-техническим средствам информационной системы для преднамеренного внесения в них уязвимостей или программных закладок. Имеют возможность создания и применения специальных технических средств для добывания информации. Имеют хорошую осведомленность о мерах защиты информации, применяемых в информационной системе, об алгоритмах, аппаратных и программных средствах, используемых в информационной системе. Имеют возможность получить информацию об уязвимостях путем проведения специальных исследований (в том числе с привлечением специализированных научных организаций) и применения специально разработанных средств для анализа программного обеспечения. Имеют возможность создания методов и средств реализации угроз безопасности информации с привлечением специализированных научных организаций и реализации угроз с применением специально разработанных средств, в том числе обеспечивающих скрытное проникновение в информационную систему и воздействие на нее.

Модель нарушителей ФСТЭК

В зависимости от уровня возможностей нарушители подразделяются на нарушителей, обладающих:

1) базовыми возможностями по реализации угроз безопасности информации (Н1);

2) базовыми повышенными возможностями по реализации угроз безопасности информации (Н2)

3) средними возможностями по реализации угроз безопасности информации (Н3);
4) высокими возможностями по реализации угроз безопасности информации (Н4).

Классификация угроз;

- по типу ИСПДн
- по виду защищаемой информ.
- по видам возможных источников
- по способам реализации
- по используемой уязвимости
- по способам реализации
- по объекту воздействия
- по виду нарушаемого свойства

Анализ последствий от реализации угроз безопасности информации

- ➔ Нарушение конфиденциальности:
- ➔ Утечка информации.
- ➔ Несанкционированное копирование.
- ➔ Перехват информации в каналах передачи данных.
- ➔ Разглашение (публикация) защищаемой информации.
- ➔ Нарушение целостности (уничтожение, модификация, дезинформация):
- ➔ Воздействие на ПО и данные пользователя.
- ➔ Воздействие на микропрограммы, данные и драйверы устройств ИС.
- ➔ Воздействие на программы, данные и драйверы устройств, обеспечивающих загрузку ОС и СЗИ и их функционирование.
- ➔ Воздействие на программы и данные прикладного и специального ПО.
- ➔ Внедрение вредоносной программы, программно-аппаратной закладки и др.
- ➔ Воздействие на средства управления конфигурацией сети.
- ➔ Воздействие на СЗИ.
- ➔ Нарушение доступности:
- ➔ Нарушение функционирования и отказы средств обработки информации, средств ввода/ вывода информации, средств хранения информации, аппаратуры и каналов передачи данных.
- ➔ Нарушение и отказы в функционировании СЗИ.

В состав экспертной группы для оценки угроз безопасности информации рекомендуется включать экспертов (независимо от того, реализуются ли функции обладателя информации, заказчика и оператора в рамках одной или нескольких организаций) от:

-подразделения по защите информации (обеспечения информационной безопасности);
-подразделения, ответственного за цифровую трансформацию (ИТ-специалистов);
-подразделения, ответственного за эксплуатацию сетей связи;
-подразделения, ответственного за эксплуатацию автоматизированных систем управления;
-подразделений обладателя информации или оператора, ответственного за выполнение основных (критических) процессов (бизнес-процессов).

В состав экспертной группы должны входить не менее трех экспертов. Экспертную оценку рекомендуется проводить в отношении следующих параметров:
а) негативного последствия от реализации угроз безопасности информации;
б) целей нарушителей по реализации угроз безопасности информации;
в) сценария действий нарушителей при реализации угроз безопасности информации.

Оценку параметров рекомендуется проводить опросным методом с составлением анкеты, в которой указываются вопросы и возможные варианты ответа в единой принятой шкале измерений («низкий», «средний», «высокий» или «да», «нет» или иные шкалы). При этом вопросы должны быть четкими и однозначно трактуемыми, предполагать однозначные ответы.
Опрос экспертов включает следующие **этапы**:

1. каждый эксперт проводит оценку оцениваемого параметра (рекомендуется не менее двух раундов оценки), результаты которой заносятся в таблицу;
2. после оценки каждым из экспертов отбрасываются минимальные и максимальные значения; определяется среднее значение оцениваемого параметра в каждом раунде;
3. определяется итоговое среднее значение оцениваемого параметра.

Методика определения угроз безопасности информации в информационных системах от 5 февраля 2021 г.

Методика применяется для определения угроз безопасности информации, реализация (возникновение) которых возможна в системах и сетях, отнесенных к государственным и муниципальным информационным системам, информационным системам персональных данных, значимым объектам критической информационной инфраструктуры Российской Федерации, информационным системам управления производством, используемым организациями оборонно-промышленного комплекса, автоматизированным системам управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды.

Содержание:

Описание

Раздел «Общие положения» содержит:

- назначение и область действия документа;
- нормативные правовые акты, методические документы, национальные стандарты, используемые для оценки угроз безопасности информации и разработки модели угроз;
- наименование обладателя информации, заказчика, оператора систем и сетей;
- подразделения, должностные лица, ответственные за обеспечение защиты информации (безопасности) систем и сетей;
- наименование организации, привлекаемой для разработки модели угроз безопасности информации (при наличии).

Раздел «Описание систем и сетей и их характеристика как объектов защиты» содержит:

- наименование систем и сетей, для которых разработана модель угроз безопасности информации;
- класс защищенности, категория значимости систем и сетей, уровень защищенности персональных данных;
- нормативные правовые акты Российской Федерации, в соответствии с которыми создаются и (или) функционируют системы и сети; назначение, задачи (функции) систем и сетей, состав обрабатываемой информации и ее правовой режим;
- основные процессы (бизнес-процессы) обладателя информации, оператора, для обеспечения которых создаются (функционируют) системы и сети;
- состав и архитектуру систем и сетей, в том числе интерфейсы и взаимосвязи компонентов систем и сетей;
- описание групп внешних и внутренних пользователей систем и сетей, уровней их полномочий и типов доступа (в состав групп пользователей включаются все пользователи, для которых требуется авторизация при доступе к информационным ресурсам, и пользователи, для которых не требуется авторизация (например, предоставлен доступ к сайту без прохождения авторизации);
- описание внешних интерфейсов и взаимодействий систем и сетей с пользователями (в том числе посредством машинных носителей информации, средств ввода-вывода, веб-приложений), иными системами и сетями, обеспечивающими системами, в том числе с сетью «Интернет»;
- информацию о функционировании систем и сетей на базе информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры, о модели предоставления вычислительных услуг, о распределении ответственности за защиту информации между обладателем информации, оператором и поставщиком вычислительных услуг, об условиях использования информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры поставщика услуг (при наличии).

Раздел «Возможные негативные последствия от реализации (возникновения) угроз безопасности информации» содержит:

- описание видов рисков (ущербов), актуальных для обладателя информации, оператора, которые могут наступить от нарушения или прекращения основных процессов;

- описание негативных последствий, наступление которых в результате реализации (возникновения) угроз безопасности информации может привести к возникновению рисков (ущерба).

Виды ущербов:

- Физ. лицу
- Юрид. лицу, ИП
- Государству с определенных областях и сферах

Раздел «Возможные объекты воздействия угроз безопасности информации» содержит:

- наименования и назначение компонентов систем и сетей, которые непосредственно участвуют в обработке и хранении защищаемой информации, или обеспечивают реализацию основных процессов обладателя информации, оператора;
- описание видов воздействия на компоненты систем и сетей, реализация которых нарушителем может привести к негативным последствиям.

Возможные объекты воздействия:

1. Разглашение персональных данных граждан:
    a. База данных информ. системы, содержащая идентификационные данные граждан.
    b. АРМ пользователя
    c. Линия связи основного сервера и резервного сервера ЦОД-а
    d. Веб приложение информ. системы обрабатывающей идентиф. данные
2. Хищение денежных средств со счета организации
    a. Банк-клиент
    b. АРМ финансового директора
    c. Эл. почта финансового директора
    d. АРМ главного бухгалтера
3. Срыв запланированной сделки с партнером
    a. АРМ руководителя
    b. Эл. почта руководителя
4. Загрязнение окруж.среды
    a. Коммутационный контроллер
    b. Программируемый логический контроллер
    c. АРМ оператора
5. Непредоставление гос.услуг
    a. Веб приложение гос. услуг

b. Система управления сайтом
c. Сервер балансировки нагрузки на сайт
d. Сервер приложения портала госуслуг
e. Сервер баз данных портала

Раздел «Источники угроз безопасности информации» содержит:

- характеристику нарушителей, которые могут являться источниками угроз безопасности информации, и возможные цели реализации ими угроз безопасности информации;
- категории актуальных нарушителей, которые могут являться источниками угроз безопасности информации;
- описание возможностей нарушителей по реализации ими угроз безопасности применительно к назначению, составу и архитектуре систем и сетей

Раздел «Способы реализации (возникновения) угроз безопасности информации» включает:

- описание способов реализации (возникновения) угроз безопасности информации, которые могут быть использованы нарушителями разных видов и категорий;
- описание интерфейсов объектов воздействия, доступных для использования нарушителями способов реализации угроз безопасности информации.

Раздел «Актуальные угрозы безопасности информации» включает:

- перечень возможных (вероятных) угроз безопасности информации для соответствующих способов их реализации и уровней возможностей нарушителей;
- описание возможных сценариев реализации угроз безопасности информации; выводы об актуальности угроз безопасности информации.