ОПРЕДЕЛЕНИЕ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА

Чаговец С. Н.

ТулГУ, 2021

Задачи моделирования угроз

- Стадия создания информационной системы и информационно-телекоммуникационных сетей – для определения предъявляемых к ним требований безопасности информации;
- Стадия их эксплуатации - для выявления новых актуальных угроз и принятия решения о необходимости модернизировать систему защиты информации.

До 2021

- методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (2008 года);
- методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры (2007 года).

Новая методика 2021 г

- универсальна и работает со следующими типами объектов:
  - информационные системы (ИС);
- автоматизированные системы управления;
- информационно-телекоммуникационные сети;
- информационно-телекоммуникационные инфраструктуры центров обработки данных;
- облачные инфраструктуры.

Недостатки методики 2021 года

- Документ невозможно выполнить буквально.
- Методика не является пошаговой инструкцией
- Содержит лишь перечень основных этапов моделирования угроз и основных операций, без их подробной детализации.
- Способы выполнения этих операций эксперты выбирают сами.

Область применения методики

- информационные системы персональных данных;
- информационные системы управления производством, используемые в ОПК;
- муниципальные и государственные ИС;
- значимые объекты критической информационной инфраструктуры РФ;
- критически важные, потенциально опасные объекты с автоматизированными системами управления производственными и технологическими процессами.

Ситуация с прежними методиками

- Прежние методики перестали применять при подготовке документации;
- Модели угроз, разработанные с их применением, продолжают действовать;
- Корректировка только в случае изменения соответствующей инфраструктуры.

Этапы оценки угроз безопасности информации по обновленной методики:

1. Определение негативных последствий, к которым может привести реализация угроз безопасности информации;
2. Проведение инвентаризации информационных систем и сетей, выделение возможных объектов воздействия нарушителя;
3. Определение источников угроз, оценить возможности нарушителей;
4. Оценка способов реализации угроз безопасности информации;
5. Оценка возможности реализации угроз безопасности информации, определение актуальности таких угроз (+3 подэтапа);

1. Выявление источников угроз безопасности информации.

- Новая методика не включает в себя ряд факторов, не зависящих от человека:
  - угрозы безопасности, связанных с природными явлениями и стихийными бедствиями;
  - угрозы безопасности криптографических средств защиты;
  - угрозы безопасности, связанных с техническими каналами утечки данных.

- ! Право включения техногенных угроз в модель угроз ИБ остается за оператором систем и сетей или владельцем информации

1. Выявление источников угроз безопасности информации

- В результате определения источников угроз ИБ выявляются:
- а)
  - виды потенциальных нарушителей
  - возможные цели реализации ими угроз безопасности информации
  - возможности
- б)
  - категории потенциальных нарушителей

2. Оценка способов реализации угроз безопасности информации.

- На данном этапе определяются:

- а) виды и категории нарушителей, способных применить актуальные способы;

- б) актуальные способы осуществления угроз ИБ и типы интерфейсов объектов воздействия.

3. Оценка актуальности угроз безопасности информации.

- Угроза считается допустимой, если на этапах оценки были обнаружены следующие признаки:
  - присутствует объект воздействия угроз;
  - присутствует непосредственно нарушитель или другой источник угрозы;
  - обнаружены пути осуществления угрозы ИБ;
  - осуществление угрозы может привести к негативным последствиям.

Определение негативных последствий

- Моделирование угроз начинается с определения негативных последствий, которые могут всерьез заботить руководство организаций.
  - !!Это не означает, что специалист по информационной безопасности должен уметь самостоятельно определять, что именно заботит руководство
- Для формального соответствия методике достаточно определять негативные последствия на том уровне абстракции, который используется в **Приложении 4**

Определение негативных последствий

Примеры негативных последствий, реально мотивирующих руководителей:

- Крупная организация – единовременное хищение на сумму свыше 10 млн рублей или серия однотипных хищений на общую сумму свыше 500 млн рублей в течение года;
- Промышленное предприятие – вывоз готовой продукции без оформления учетных документов, остановка производственных процессов более, чем на сутки;
- Лечебное учреждение – искажение отчетности о деятельности, связанной с оборотом наркотических средств, неоказание дежурной больницей профильной для нее медицинской помощи, утечка данных из специальных регистров;
- Орган власти – неспособность в течение длительного времени оказывать государственные услуги в электронном виде, утечка данных из специальных регистров (например, регистра ВИЧ-инфицированных жителей муниципального образования).

Определение объектов воздействия

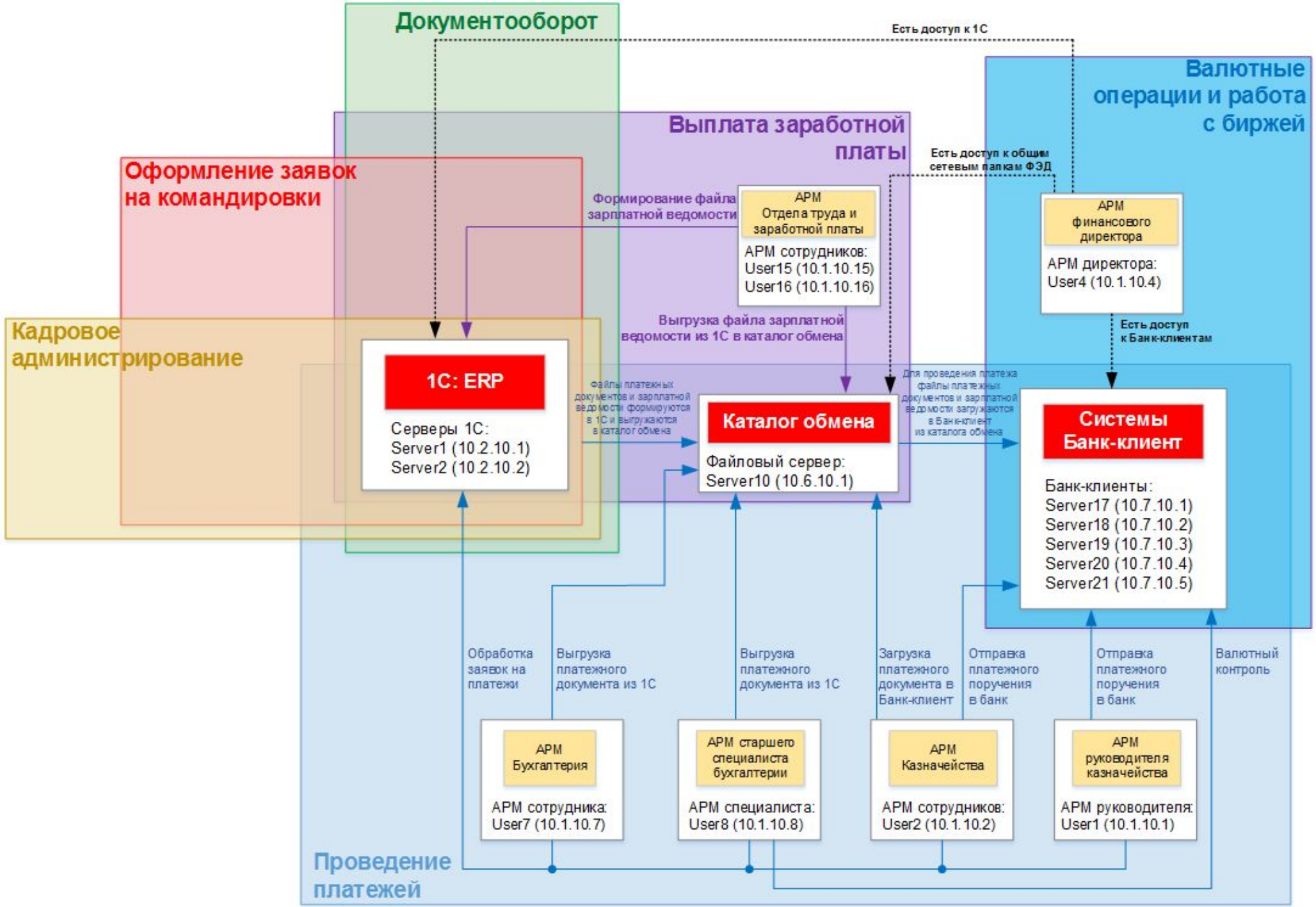
- Воздействие на какие именно объекты может привести к наступлению негативных последствий.
  - !!Методический документ не детализирует, как именно должны определяться объекты воздействия, оставляя это на усмотрение эксперта, проводящего анализ уязвимостей.
- Требуется использовать общий перечень угроз безопасности информации, опубликованный в банке данных угроз безопасности информации ФСТЭК России (https://bdu.fstec.ru);
- Требуется использовать низкоуровневые описания возможных способов воздействия, описанных в базах знаний CAPEC и Att&CK, а также в базах знаний типовых атак на веб-приложения WASC и OWASP.

Определение объектов воздействия

- Анализ угроз информационной системы не должен ограничиваться лишь только компонентами информационной системы, которыми управляет ее оператор.
- Например: Облако (облачные сервисы) – оценивает поставщик облачных услуг.

Пример детализации

- Выбираем моделируемое негативное последствие, например – хищение денежных средств с расчетного счета предприятия.
- Опрашиваем руководителей функциональных подразделений и определяем бизнес-процессы, в рамках которых выполняются платежные операции. (БП: оплата поставщикам, выплата заработной платы, оплата командировочных расходов, прямые финансовые операции и т. п.)
- Для каждого бизнес-процесса определяем какие именно операции могут быть скомпрометированы нарушителем для наступления моделируемого негативного последствия. Например, один из способов хищения денежных средств в бизнес-процессе выплаты заработной платы является добавление несуществующего работника в модуле кадрового администрирования.
- Для каждой операции, которые могут быть скомпрометированы нарушителем, определяем компоненты информационной системы, которые используются при выполнении таких операций.
- Для каждого такого компонента определяем, можно ли добиться моделируемого негативного последствия воздействием на такой объект. Так, нарушитель может добавить несуществующего работника, если получит контроль над сервером кадрового администрирования, сервер системы управления базами данных, который используется модулем кадрового администрирования, и т. п.


Документооборот
Есть доступ к 1С
Валютные операции и работа с биржей
Выплата заработной платы
Есть доступ к общим сетевым папкам ФЭД
Оформление заявок на командировки
Формирование файла зарплатной ведомости
АРМ Отдела труда и заработной платы
АРМ сотрудников:
User15 (10.1.10.15)
User16 (10.1.10.16)
АРМ финансового директора
АРМ директора:
User4 (10.1.10.4)
Выгрузка файла зарплатной ведомости из 1С в каталог обмена
Есть доступ к Банк-клиентам
Кадровое администрирование
1С: ERP
Серверы 1С:
Server1 (10.2.10.1)
Server2 (10.2.10.2)
Файлы платежных документов и зарплатной ведомости формируются в 1С и выгружаются в каталог обмена
Каталог обмена
Файловый сервер:
Server10 (10.6.10.1)
Для проведения платежа файлы платежных документов и зарплатной ведомости загружаются в Банк-клиент из каталога обмена
Системы Банк-клиент
Банк-клиенты:
Server17 (10.7.10.1)
Server18 (10.7.10.2)
Server19 (10.7.10.3)
Server20 (10.7.10.4)
Server21 (10.7.10.5)
Обработка заявок на платежи
Выгрузка платежного документа из 1С
Выгрузка платежного документа из 1С
Загрузка платежного документа в Банк-клиент
Отправка платежного поручения в банк
Отправка платежного поручения в банк
Валютный контроль
АРМ Бухгалтерия
АРМ сотрудника:
User7 (10.1.10.7)
АРМ старшего специалиста бухгалтерии
АРМ специалиста:
User8 (10.1.10.8)
АРМ Казначейства
АРМ сотрудников:
User2 (10.1.10.2)
АРМ руководителя казначейства
АРМ руководителя:
User1 (10.1.10.1)
Проведение платежей

Определение объектов воздействия

- Формируется перечень компонентов информационных систем, которые могут являться целью нарушителя, стремящегося добиться наступления моделируемого негативного последствия.
  - !! перечень неполон: кроме компонентов самой информационной системы, есть ряд объектов инфраструктуры, получение контроля над которыми тоже позволяет нарушителю решить стоящую перед ним задачу.

- Финальный перечень объектов воздействия должен включать в себя как компоненты информационной системы, так и объекты ИТ-инфраструктуры предприятия.

Определение источников угроз безопасности информации

- Определение источников угроз безопасности информации является частью моделирования угроз,
  - !!Более логичным будет - определение их до моделирования, сразу же после определения возможных негативных последствий
- Методика определяет основные виды нарушителей (спецслужба иностранного государства, террористическая группировка, …). Этот перечень не является исчерпывающим и при необходимости может дополняться.

Определение источников угроз безопасности информации - определение видов нарушителя

- Основные задачи:
  - сформулировать цель (т. е. мотив) действий нарушителя
  - Принять решение о признании нарушитель данного вида актуальным (Приложение 6)
- Вид нарушителя определяет уровень его возможностей.
  - базовый (Н1),
  - базовый повышенный (Н2),
  - средний (Н3)
  - высокий (Н4)

(Приложение 8)

Виды нарушителя

- Н1 не является специалистом, он использует только известные уязвимости и бесплатные инструменты.
- Н2 также использует только свободно распространяемые инструменты, но является специалистом. Он способен находить и использовать уязвимости нулевого дня на атакуемых объектах.
- Н3 дополнительно к этому способен приобретать дорогостоящие инструменты и проводить лабораторные исследования по поиску уязвимостей нулевого дня в оборудовании и программных средствах, аналогичных используемым на атакуемых объектах.
- Н4 способен внедрять программные и аппаратные закладки в серийно изготавливаемое оборудование и программное обеспечение, может использовать побочное электромагнитное излучение, наводки и скрытые каналы, умеет проводить долгосрочные APT-атаки и обладает неограниченными ресурсами.

Виды нарушителя

- Методика задает прямое соответствие между негативными последствиями, целями нарушителей различных видов и их возможностями.
- Соответствие возможных негативных последствий целям нарушителей оставлено на усмотрение экспертов.
  - Пример: Так, для ИСПДн, предприятия розничной торговли для учета заказов покупателей, допустимо признать неактуальными угрозы со стороны спецслужб.

Оценка способов реализации угроз

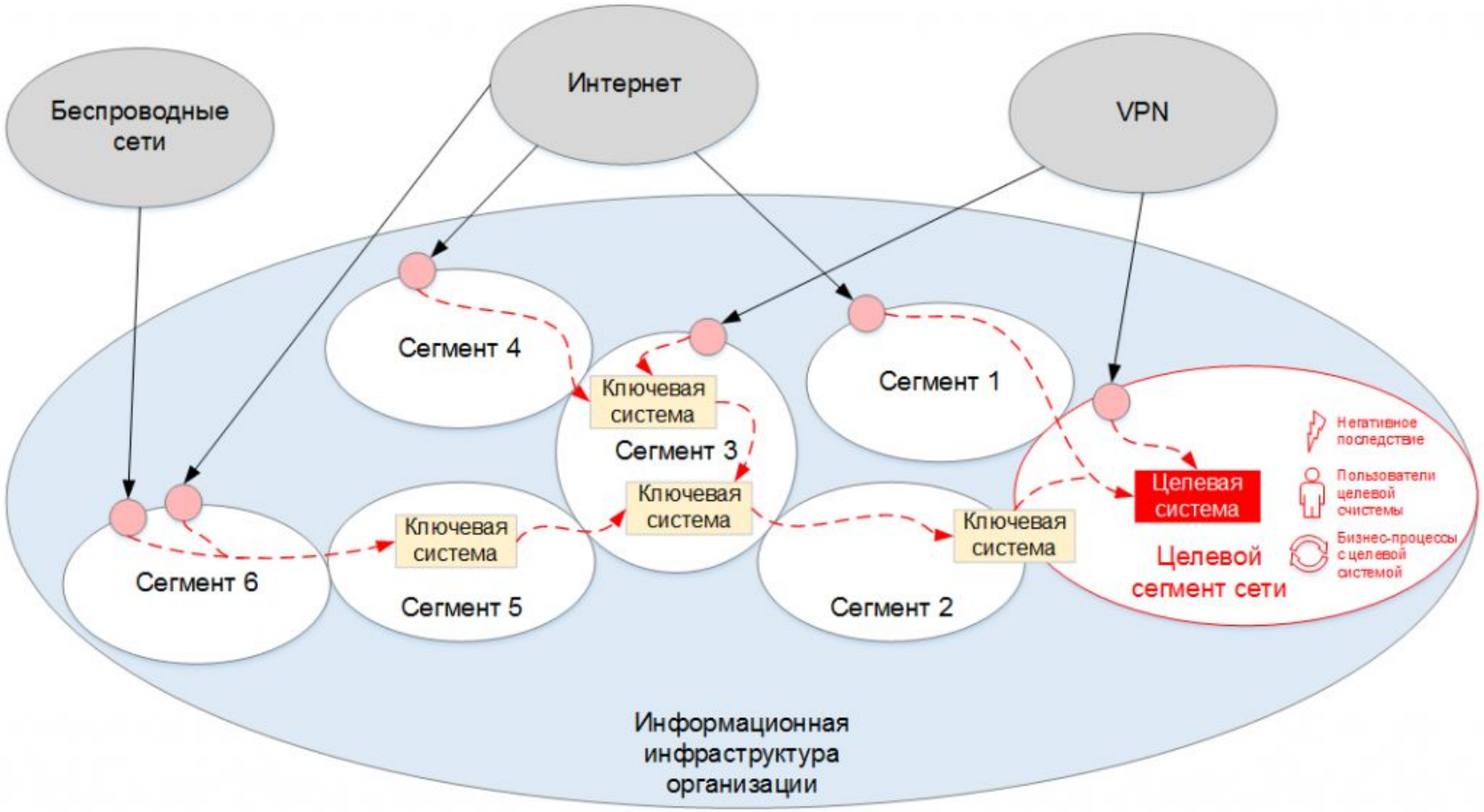
- Фактическая конкретизация понятие «угроза безопасности информации»:
  - угрозой называется потенциальная или реальная возможность наступления заданных негативных последствий в результате одного из заданных негативных воздействий на один из заданных объектов воздействия.

Оценка способов реализации угроз

- Если угроза признается возможной - оценка возможности выбранного нарушителя практически реализовать угрозу, рассмотрев возможные сценарии реализации угрозы.

- *На практике это означает оценку того, может ли нарушитель из заданных стартовых условий “пройти” по ИТ-инфраструктуре организации и получить практическую возможность реализовать угрозу.*

Оценка способов реализации угроз



Анализ угроз на разных стадиях жизненного цикла ИС

В соответствии с нормативными документами ФСТЭК России анализ угроз проводится на разных стадиях жизненного цикла ИС:

- на стадии создания системы;
- периодически на стадии эксплуатации системы.

- ! На стадии создания системы сценарий реализации угроз не может учитывать меры защиты: меры защиты еще не определены. Результаты анализа угроз – определение реализаций базовых и дополнительных мер защиты.
- На стадии эксплуатации - анализ угроз проводится:
  - с учетом реализованных мер защиты;
  - с учетом выявленных уязвимостей;
  - с использованием результатов тестирования на проникновения.

- Угроза признается актуальной, если есть хотя бы один сценарий ее реализации.

Заключение

Достоинства новой методики:

- универсальна и применима для широкого круга областей;
- наглядные примеры для выполнения каждого из подэтапов оценки потенциальных угроз;
- рекомендации о применении экспертного метода;
- нацеленность на оценку негативных последствий угроз.

Заключение

Недостатки

- сценарный подход к моделированию угроз требует от экспертов глубокого знания известных способов (техник, тактик) проведения компьютерных атак, а главное – времени.

- Самая серьезная проблема противодействия компьютерным атакам заключается в том, что зачастую даже типовые действия атакующего, часто оказывается сюрпризом для защищающейся стороны.