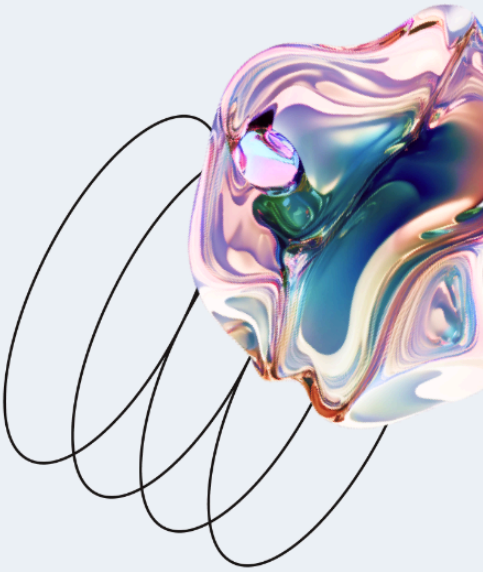
GeekBrains



Моделирование угроз и выбор мер защиты

Основы информационной безопасности

Оглавление

Введение

Сегодня мы продолжаем курс, посвященный основам обеспечения информационной безопасности (ИБ), а текущее занятие будет по теме: моделирование угроз и выбор мер защиты.

На этой лекции вы узнаете:

- Классы источников угроз, способы реализации угроз и уязвимостей
- Зачем нужна типизация кибератак (Cyber Kill Chain®, MITRE ATT&CK®)
- Варианты определения актуальных угроз
- Классы мер защиты и варианты их выбора и обоснования
- Актуальные на сегодня тенденции в части угроз и уязвимостей
- Наиболее популярные ИБ best practices и cybersecurity frameworks (ISO 27k series, CIS Controls, NIST CSF, OWASP).

Словарь терминов

Источник угрозы (безопасности информации) – субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации (ГОСТ Р 50922-2006).

Угроза (безопасности информации) – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации (ГОСТ Р 50922-2006).

Уязвимость – недостаток (слабость) программного (программно-технического) средства или системы и сети в целом, который(ая) может быть использован(а) для реализации угроз безопасности информации (ГОСТ Р 56545-2015).

Модель угроз (безопасности информации) – физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации (ГОСТ Р 53114-2008).

Моделирование угроз (безопасности информации) – систематический процесс анализа и оценки актуальности угроз безопасности информации как на этапе создания систем, так и в ходе их эксплуатации, в т.ч. при развитии (модернизации) и выводе из эксплуатации, а также формирование специального нормативного документа (опционально), адаптировано из методического документа «Методика оценки угроз безопасности информации», 2021.

Актуальная угроза (безопасности информации) – угроза реализация (возникновение) которой возможна в системах и сетях с заданной архитектурой и в условиях их функционирования, а также может привести к негативным последствиям (адаптировано из методического документа «Методика оценки угроз безопасности информации», 2021).

Меры защиты информации (control) – принятые правила, процедуры или механизмы, направленные на защиту информации (ГОСТ Р 59547-2021).

Эксплойт (exploit) – программа, фрагмент программного кода или последовательность команд, использующая (эксплуатирующая) уязвимости.

Патч (patch) – обновление и/или дополнение к программе(ам).

Классы источников угроз, классы способов реализации угроз и уязвимостей

Классификация позволит нам более системно подойти к рассмотрению источников угроз, способов их реализации и уязвимостей. Начнём с первичного понятия – источник угрозы, т.к. если его нет, то уязвимости и способы реализации угроз не имеют смысла.

Классы источников угроз

Источники угроз условно можно разделить на следующие классы:

- антропогенные (порождённые человеком):
    - внешний атакующий (хакер)
    - внутренний нарушитель (инсайдер)
    - внешний атакующий + внутренний нарушитель (сговор)
- технические (сбои, ошибки и т.п.)
- природные (наводнения, землетрясения и т.п.)
- социальные (терроризм, войны, эпидемии и т.п.)

В рамках данного курса продолжим рассмотрение только антропогенных источников угроз, с акцентом на внешнего атакующего (хакера).

Классы угроз (способов реализации)

Существует достаточно много вариантов классификации угроз, например:

- по видам защищаемой информации
- видам возможных источников угроз
- видам нарушений свойств защищаемой информации
- типам атакуемых систем
- способом реализации угроз
- используемым уязвимостям
- объектам воздействия

Но наиболее принятым и понятным является вариант классификации по способам реализации (возникновения) угроз, но, к сожалению, нет одного абсолютно верного варианта такой классификации. В рамках данного курса мы рассмотрим четыре варианта.

Первый вариант, основанный на методике ФСТЭК России [1], представляет собой следующий перечень классов возможных способов реализации угроз:

- использование уязвимостей (несанкционированные действия)
- внедрение вредоносного программного обеспечения (ПО)
- использование недекларированных возможностей ПО
- установка программных и/или программно-аппаратных «закладок»
- формирование и использование скрытых каналов (по времени, по памяти) для передачи данных
- перехват (измерение) побочных электромагнитных излучений и наводок (других физических полей)
- инвазивные способы доступа к информации, содержащейся в аппаратных средствах
- хищение аппаратных средств и/или физических носителей информации
- уничтожение аппаратных средств и/или физических носителей информации
- нарушение безопасности при поставках и/или услуг по установке, настройке, испытаниям, пусконаладочным работам (в т.ч. администрированию, обслуживанию)
- ошибочные действия в ходе создания и эксплуатации систем и сетей, в т.ч. при установке и/или настройке

Второй вариант, основанный на базовой модели угроз ФСТЭК России [2], представляет собой иерархически вложенный перечень классов возможных способов реализации угроз:

- угрозы утечки информации по техническим каналам:
    - угрозы утечки акустической (речевой) информации
    - угрозы утечки видовой информации
    - угрозы утечки информации по каналам побочных электромагнитных излучений и наводок (ПЭМИН)
- угрозы создания нештатных режимов работы – «отказы в обслуживании» (изменение служебных данных, игнорирования предусмотренных ограничений и т.п.)
- угрозы доступа (проникновения) в операционную среду:
    - угрозы непосредственного доступа
        - угрозы, реализуемые в ходе загрузки операционной системы (ОС)
        - угрозы, реализуемые после загрузки ОС, независимо от того, какое ПО запускается пользователем
        - угрозы, реализация которых определяется тем, какое ПО запускается пользователем, или фактом запуска любой из прикладных программ
    - угрозы удаленного доступа (сетевые атаки):
        - анализ сетевого трафика
        - сканирование сети
        - «парольная» атака
        - подмена доверенного объекта сети
        - навязывание ложного маршрута
        - внедрение ложного объекта сети
        - отказ в обслуживании
        - удаленный запуск приложений
    - угрозы программно-математического воздействия (внедрения вредоносного ПО)

Третий вариант классификации – это модель STRIDE от корпорации Microsoft:

- **S**poofing: подмена идентификационных данных
- **T**ampering: подделка (фальсификация) данных
- **R**epudiation: отказ от действий
- **I**nformation Disclosure: разглашение информации
- **D**enial of Service: отказ в обслуживании
- **E**levation of Privileges: повышение привилегий

Четвёртый вариант, основанный на стандарте безопасности сети электросвязи [3], представляет собой следующий перечень классов возможных способов реализации угроз:

- уничтожение информации и/или других ресурсов
- искажение или модификация информации
- мошенничество
- кража, утечка, потеря информации и/или других ресурсов
- несанкционированный доступ
- отказ в обслуживании

💡 На практике необходимо зафиксировать выбранный и используемый конкретной организацией вариант классификации угроз (реестр), который в т.ч. может быть комбинацией приведённых выше вариантов.

Классы уязвимостей

Уязвимости – это недостатки, которые атакующий использует в рамках реализации угроз. Их также можно классифицировать. Согласно ГОСТ Р 56546-2015 «Классификация уязвимостей информационных систем» [4] в основе классификации уязвимостей используются следующие классификационные признаки:

- область происхождения уязвимости
- типы недостатков ИС
- место возникновения (проявления) уязвимости ИС

По областям происхождения уязвимости:

- уязвимости кода (ПО)
- уязвимости конфигурации
- уязвимости архитектуры
- организационные уязвимости
- многофакторные уязвимости

По типам недостатков, связанных:

- с неправильной настройкой параметров ПО
- неполнотой проверки вводимых (входных) данных
- возможностью прослеживания пути доступа к каталогам

- возможностью перехода по ссылкам
- возможностью внедрения команд ОС
- межсайтовым скриптингом (выполнением сценариев)
- внедрением интерпретируемых операторов языков программирования или разметки
- с внедрением произвольного кода
- переполнением буфера памяти
- неконтролируемой форматной строкой
- вычислениями
- приводящие к утечке/раскрытию информации ограниченного доступа
- управлением полномочиями (учётными данными)
- управлением разрешениями, привилегиями и доступом
- аутентификацией
- криптографическими преобразованиями (недостатки шифрования)
- подменой межсайтовых запросов
- приводящие к «состоянию гонки»
- управлением ресурсами
- иные типы недостатков

По месту возникновения (проявления):

- уязвимости в общесистемном (общем) ПО
- уязвимости в прикладном ПО
- уязвимости в специальном ПО
- уязвимости в технических средствах (микропрограммных)
- уязвимости в портативных технических средствах
- уязвимости в сетевом (коммуникационном, телекоммуникационном) оборудовании
- уязвимости в средствах защиты информации

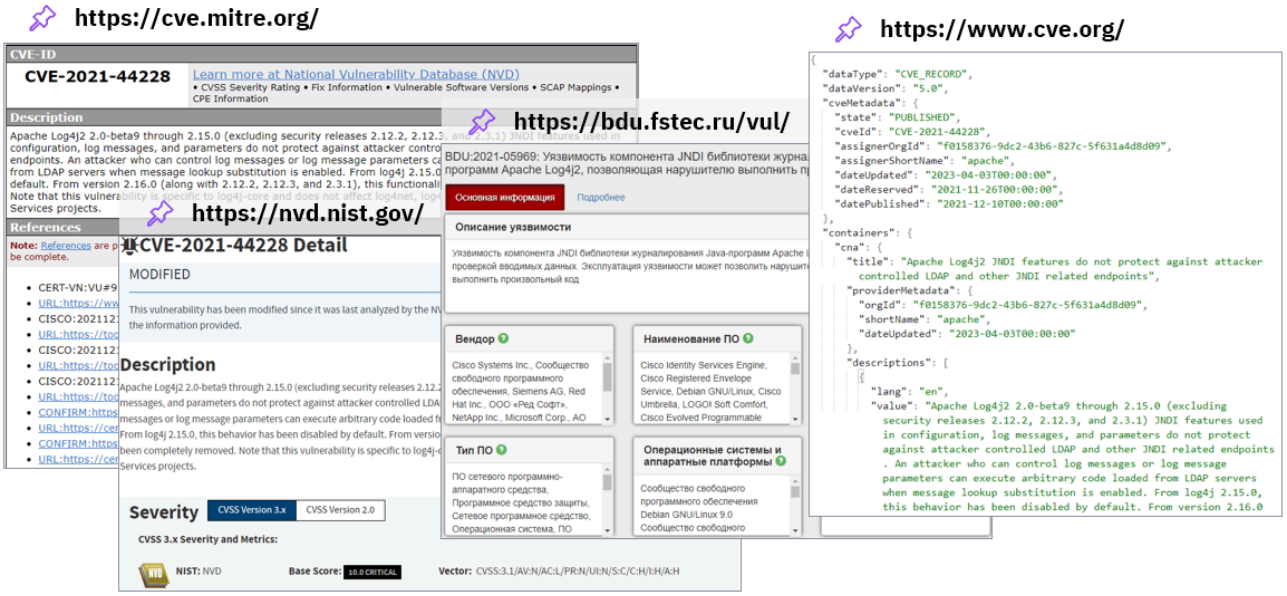
Говоря о классификации уязвимостей нужно так же затронуть так называемые **Common-понятия**:

- Common Weakness Enumeration (CWE™): перечень типов (классов) уязвимостей (ещё один вариант классификации)
- Common Vulnerabilities and Exposures (CVE®): каталог публичных уязвимостей
- Common Vulnerability Scoring System (CVSS): метод оценки опасности уязвимостей (severity)

Как раз по уровням опасности на практике чаще всего и классифицируют уязвимости:

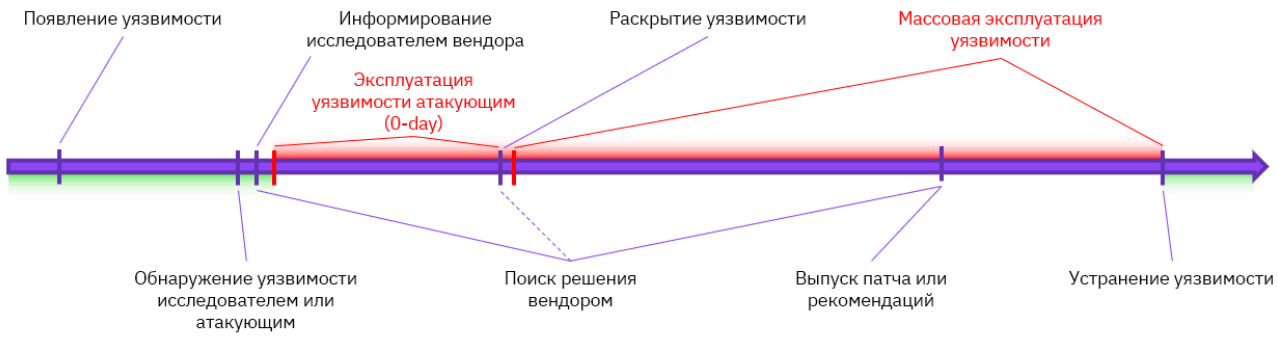
- согласно CVSS с учётом базовых метрик, не зависящих от времени и среды исполнения (вектора атаки, сложности атаки, необходимости взаимодействия с пользователем, требуемых привилегий в системе и др.), вре́менных метрик (состояния эксплойта и наличие патчей) и метрик окружения (контекст конкретной атакуемой системы) можно получить следующие варианты опасности:
  - critical: 9.0 - 10.0
  - high: 7.0 - 8.9
  - medium: 4.0 - 6.9
  - low: 0.1 - 3.9
  - none: 0.0
- согласно DREAD от корпорации Microsoft с учётом метрик потенциального ущерба, воспроизводимости атакующим, доступности эксплойта, масштабов влияния на пользователей и сложности обнаружения уязвимости атакующим можно получить следующие варианты опасности:
  - critical: 40 - 50
  - high: 25 - 39
  - medium: 11 - 24
  - low: 1 - 10

Сведения об уязвимостях аккумулируются в различных базах (реестрах) уязвимостей, в них могут использоваться свои варианты классификации уязвимостей. Примеры таких баз приведены на рисунке ниже:



💡 Недостаточно подписаться и/или использовать только одну базу (реестр) уязвимостей, т.к. они, к сожалению, не полностью перекрывают друг друга. Рекомендуется использовать профильные агрегаторы, например: https://vulners.com/.

Чтобы завершить блок про классы уязвимости предлагается взглянуть на их жизненный цикл:



Из которого видно, что уязвимости могут ещё подразделяться на уязвимости «нулевого дня» (0-day) и публично известные. В первом случае, об уязвимости никто не знает (ни разработчик ПО, ни ИБ-компании) – кроме того, кто её обнаружил, т.е. мер защиты против неё в моменте нет, и у разработчиков уязвимого ПО есть «ноль дней» на её исправление.

🔥 В связи с тем, что новые уязвимости обнаруживаются практически каждый день, а периодически еще и появляются новые способы реализации угроз, то ИБ-специалистам необходимо отслеживать сведения (тренды) об актуальных угрозах и уязвимостях.

Теперь рассмотрим, как отдельные уязвимости и способы реализации угроз «собираются» в успешные кибератаки.

Типизация кибератак

Стоит начать с того, что **типизация кибератак** – это выделение существенных и повторяющихся действий атакующих. Понимание типовой (условно «эталонной») кибератаки позволит нам лучше понять, как действуют атакующие, как следствие, мы сможем адекватнее моделировать угрозы.

Существует достаточно много вариантов типизации кибератак [5], но среди них можно выделить два стандарта де-факто:

- Cyber Kill Chain®
- MITRE ATT&CK®

Cyber Kill Chain®

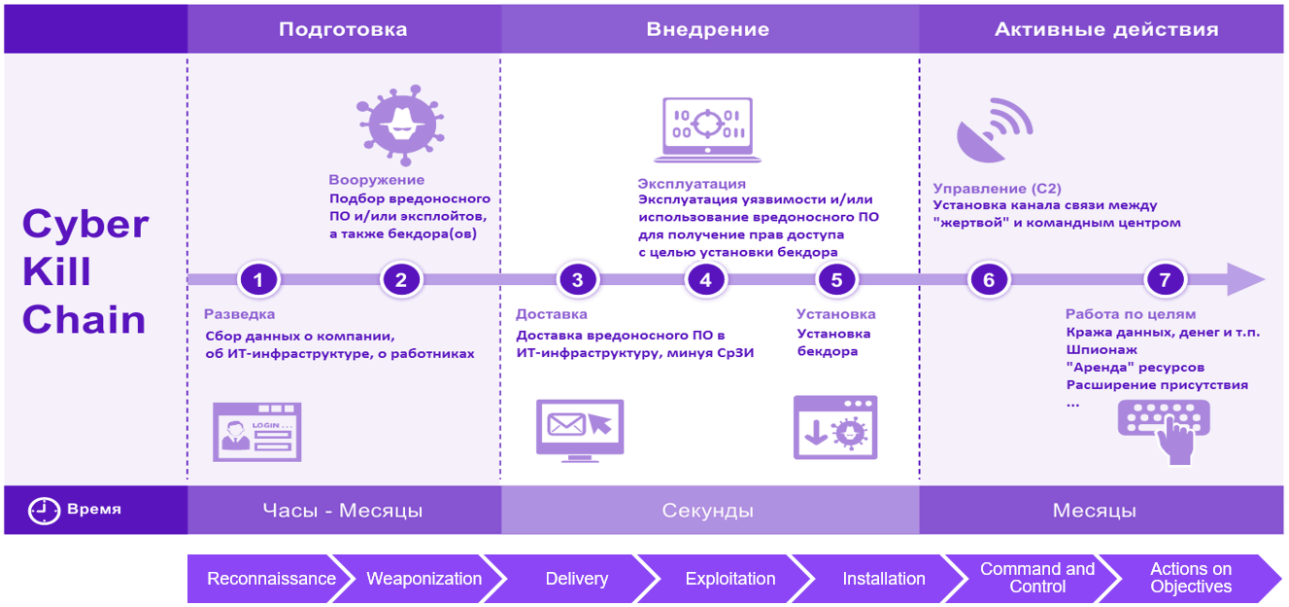
Это разработанная в 2011 году компанией Lockheed Martin семишаговая модель кибератаки (ныне framework), включающая:

- разведку (reconnaissance), где цель атакующего: собрать информацию о целях кибератаки
- вооружение (weaponization), где цель атакующего: подготовить нужное вредоносное ПО
- доставку (delivery), где цель атакующего: доставить подготовленное вредоносное ПО в ИТ-инфраструктуру, относящуюся к цели кибератаки, обходя средства защиты информации

> 💡 Обратите внимание, что кибератака может осуществляться не напрямую «вламываясь» в ИТ-инфраструктуру целевой организации, а через поставщика каких-то услуг для данной организации (supply chain cyberattacks) или часто посещаемые ресурсы работниками данной организации (watering hole cyberattacks).

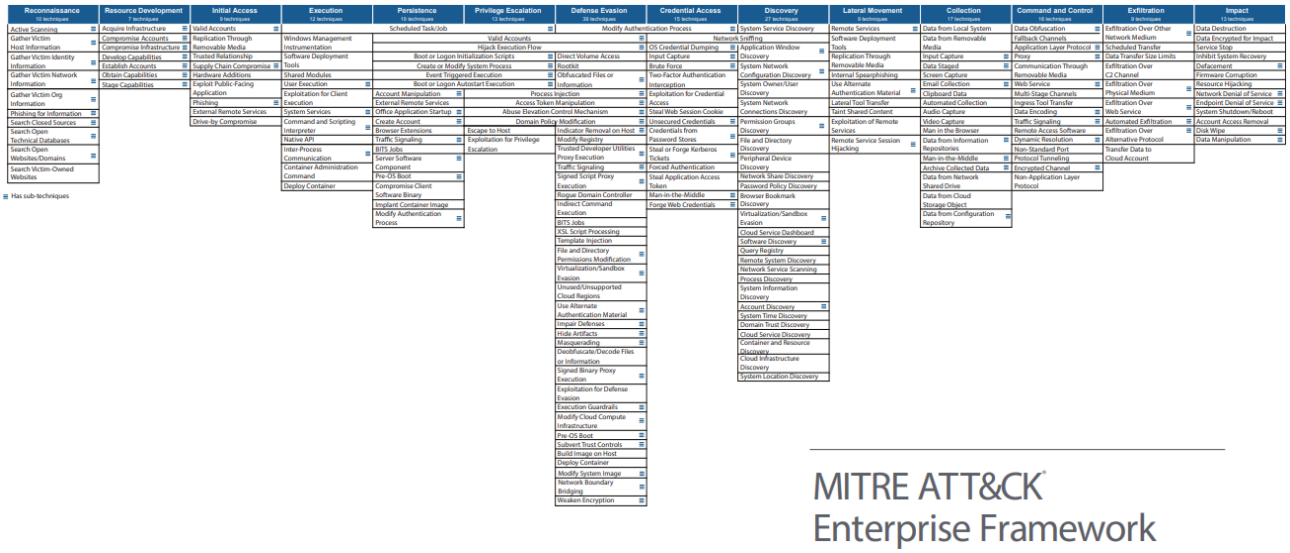
- эксплуатацию (exploitation), где цель атакующего: получить доступ на определенный хост с достаточными правами для установки бэкдора (специального вредоносного ПО, обеспечивающего скрытый канал взаимодействия с атакующим)
- установку (installation), где цель атакующего: установить бэкдор для взаимодействия с серверами управления атакующего

- управление и контроль (command and control), где цель атакующего: создать скрытый канал коммуникации между хостом-жертвой и серверами управления атакующего
- действия по целям (actions on objectives), где уже атакующий достигает цели кибератаки или переходит на новый виток «цепочки кибератаки»



MITRE ATT&CK®

Корпорация MITRE расширила (и продолжает расширять) модель Cyber Kill Chain® в рамках «матрицы» тактик, техник и общеизвестных фактов об атакующих (Adversarial Tactics, Techniques & Common Knowledge (ATT&CK®)).



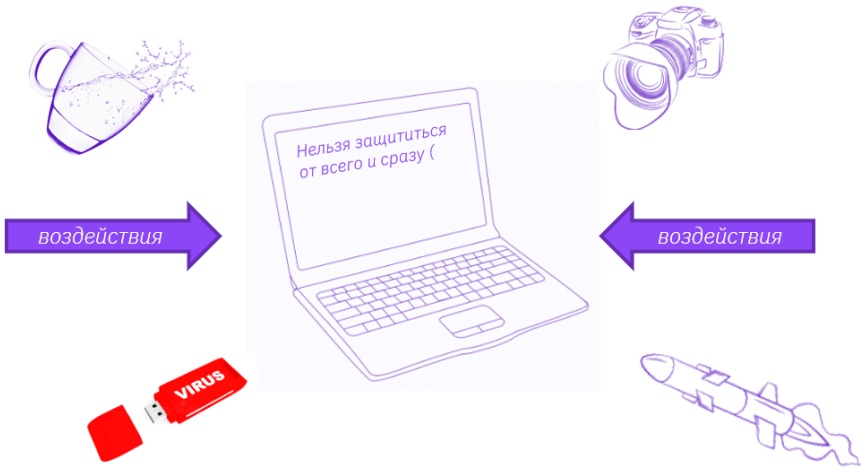
В рамках данной матрицы используется три взаимоувязанных понятия:

- тактика (tactic): отвечает на вопрос «почему/зачем?» атакующий выполняет действие
- техника и подтехника (technique and sub-technique): отвечает на вопрос «как?» атакующий выполняет действие (фактически речь о способах реализации угрозы)
- процедура (procedure): особенности реализации техники / подтехники (фактически особенности применения на практике способа реализации угрозы)

Нотация MITRE ATT&CK® и ссылки на неё при подготовке отчётов об инцидентах ИБ и эксплуатации ряда средств защиты информации и средств (контроля) анализа защищенности является повсеместной практикой. Стоит отметить, что даже ФСТЭК России в составе своей методики [1] так же оперирует понятиями тактики и техники, используя аналог матрицы MITRE ATT&CK®. В связи с этим необходимо быть готовыми работать с данным инструментом: https://attack.mitre.org/.

Варианты определения актуальных угроз

Стоит начать с того, что, к сожалению, нельзя защититься от всего и сразу, т.е. не бывает всеобъемлющих систем защиты информации.



Таким образом, нам нужно определить для себя приоритеты, а именно: от кого и от чего должна защищать создаваемая нами система защиты?

Как раз здесь нам помогут актуальные угрозы – угрозы реализация (возникновение) которых возможна в системах и сетях с заданной архитектурой и в условиях их функционирования, а также может привести к негативным

последствиям. В таком случае создаваемая нами система защиты должна быть нацелена на нейтрализацию или существенное затруднение реализации данных угроз.

В рамках определения актуальных угроз проводится моделирование по двум взаимосвязанным направлениям:

- моделирование нарушителя, чтобы понять:
  - кто атакует?
  - почему атакует (мотив)?
  - чем атакует (доступный бюджет атаки)?
- моделирование угроз, чтобы понять:
  - как атакует?
  - когда атакует (при каких условиях)?

Начнём с модели нарушителя, который в данном случае выступает антропогенным источником угрозы [6].

	УСЛОВНАЯ КАТЕГОРИЯ НАРУШИТЕЛЯ	ТИПОВЫЕ ЦЕЛИ	ВОЗМОЖНОСТИ НАРУШИТЕЛЯ
1	Автоматизированные системы*	Взлом устройств и ИТ-инфраструктур с низким уровнем защищенности для дальнейшей перепродажи или использования в массовых атаках	Автоматизированное сканирование
2	Киберхулиган/ энтузиаст-одиночка	Хулиганство, нарушение целостности ИТ-инфраструктуры	-//- Официальные и open-source-инструменты для анализа защищенности, публично доступные инструменты
3	Киберкриминал/ организованные группировки	Приоритетная монетизация атаки: шифрование, майнинг, вывод денежных средств	-//- Кастомизированные инструменты, доступное вредоносное ПО (приобретение, обфускация или разработка), доступные уязвимости, соц. инжиниринг
4	Кибернаемники/ Продвинутые группировки	Нацеленность на заказные работы – сбор информации, шпионаж в интересах конкурентов, последующая крупная монетизация, хактивизм, деструктивные действия	-//- Самостоятельно разработанные инструменты, приобретенные 0-day-уязвимости ПО
5	Кибервойска/ Прогосударственные группировки	Кибершпионаж, полный захват ИТ-инфраструктуры для возможности контроля и применения любых действий и подходов, хактивизм	-//- Самостоятельно найденные 0-day-уязвимости ПО и АО, разработанные и внедренные «закладки»

🔥 Зачастую моделируя нарушителя, используют «ярлыки»: спецслужбы, криминал, конкуренты, недобросовестные партнеры, обиженные работники и т.п., но на практике имеет значение только уровень финансово-технических возможностей нарушителя, а не его «социальный статус».

Варианты определения актуальных угроз условно можно разделить на следующие группы:

- анализ и оценка рисков ИБ, где моделирование угроз выступает составной частью данного процесса
- моделирование угроз “с нуля”
- адаптация существующих типовых или базовых моделей угроз
- использование готовых ТОП-ов (перечней) угроз

Слева направо снижается сложность реализации предлагаемого варианта, но при это возрастает и абстрактность получаемых результатов. Таким образом, потребуется найти баланс между доступными вашей команде ресурсами, в т.ч. временны́ми, и релевантностью получаемых результатов.

Давайте последовательно рассмотрим эти варианты, начиная с анализа и оценки рисков ИБ.

В первую очередь, стоит отметить, что **подход, базирующийся на риск менеджменте** (risk management), существует достаточно давно и активно развивался в области ИБ в середине 2000-ых. При этом, как сложившаяся практика, сейчас он представлен преимущественно в банковском секторе, где риски ИБ включены в состав операционных рисков, а также в международных компаниях.

Данный вариант хорош тем, что имеет устоявшиеся и понятные всем участникам процесса схемы реализации, где моделирование угроз – его составная часть. При этом он требует серьезных ресурсов на реализацию, в т.ч. участие различных подразделений, создание риск-комитета, а не просто «междусобойчик» ИТ- и ИБ-специалистов. Другими словами, для организаций, в которых есть культура риск менеджмента, это самый приоритетный вариант.

Второй вариант – это моделирование угроз с нуля. Здесь почти 15 лет «классикой» были методики ФСТЭК России, в первую очередь, на информационные системы персональных данных. А в 2021 году вышла единая методика оценки угроз безопасности информации, которая отменила действие упомянутых ранее документов. И сейчас она является основным документом в российской нормативно-правовой базе по данному вопросу. Её мы рассмотрим подробнее. Реализация данного варианта потребует участие ИТ- и ИБ-специалистов, а также представителей профильных бизнес-подразделений.

Третий вариант – это адаптация существующих типовых, в ряде случаев базовых, моделей угроз. Фактически этап моделирования сделан за нас, и мы можем выбрать модель, которая ближе всего к нам по входным параметрам, в первую очередь, по области применения.

И наконец, последний, четвёртый вариант – это использование уже готовых ТОП-ов угроз, например, ТОП-10 или ТОП-20. Источниками таких топов могут выступать различные исследовательские компании. Для российского сегмента наиболее авторитетные и релевантные публичные материалы предоставляются Лаборатория Касперского и Позитив Текнолоджиз.

Моделирование угроз по методике ФСТЭК России

Теперь давайте подробнее рассмотрим моделирование угроз согласно неоднократно упомянутой ранее методике ФСТЭК России [1].

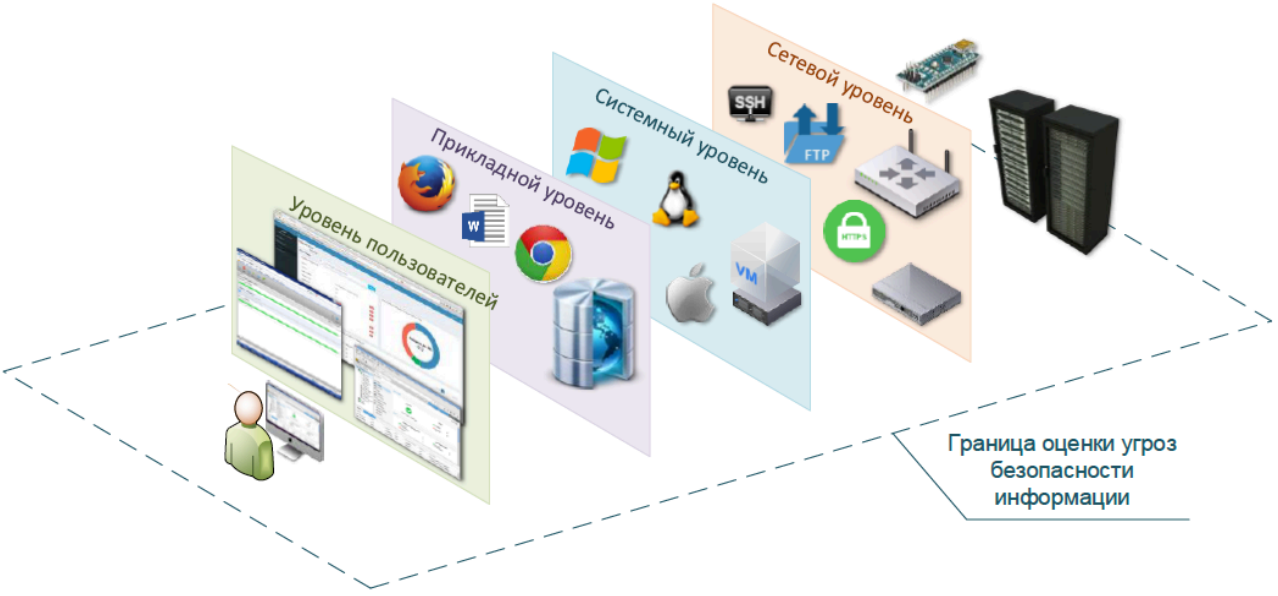
Начнём с **ограничений** данной методики:

- методика ориентирована на оценку антропогенных угроз
- проводится с использованием экспертного метода
- не рассматривается нарушение безопасности средств криптографической защиты информации
- не рассматриваются угрозы, связанные с техническими каналами утечки информации

Предусмотрена следующая последовательность проведения оценки угроз:

- определение негативных последствий:
    - анализ документации на основные (критические) процессы (бизнес-процессов)
    - определение негативных последствий от реализации угроз:

    - ущерб физическому лицу (физический, психологический, материальный и т.п.)
    - ущерб юридическому лицу, индивидуальному предпринимателю
    - ущерб государству в определённых сферах деятельности
- определение объектов воздействий (ресурсов и компонентов систем и сетей, несанкционированный доступ к которым (воздействие на которые) в ходе реализации (возникновения) угроз может привести к негативным последствиям):
    - анализ документации на системы и сети и иных исходных данных
    - инвентаризация систем и сетей
    - определение групп информационных ресурсов и компонентов систем и сетей:
        - информация (данные)
        - программно-аппаратные средства (серверы, ноутбуки и т.п.)
        - ПО
        - машинные носители информации
        - телекоммуникационное оборудование
        - средства защиты информации
        - привилегированные и непривилегированные пользователи
        - обеспечивающие системы (пожаротушение, кондиционирование и т.п.)



- оценка возможности реализации угроз и их актуальности:
    - определение источников угроз (внешние/внутренние нарушители признаются актуальными, когда возможные цели реализации ими угроз могут привести к определённым негативным последствиям):

        - с базовыми возможностями по реализации угроз (H1)
        - базовыми повышенными возможностями по реализации угроз (H2)
        - средними возможностями по реализации угроз (H3)
        - высокими возможностями по реализации угроз (H4)
    - оценка способов реализации угроз (способы признаются актуальными, когда возможности нарушителя позволяют их использовать для реализации угроз и имеются (созданы) условия, при которых такая возможность может быть реализована в отношении объектов воздействия)
    - оценка актуальности угроз (угрозы признаются актуальными, когда существует хотя бы один сценарий (последовательность возможных тактик и соответствующих им техник) её реализации)

> 💡 На практике можно воспользоваться онлайн «калькулятором» в составе Банка данных угроз (БДУ) ФСТЭК России: https://bdu.fstec.ru/threat-section/shaper-threats.

Альтернатива от MITRE

В качестве альтернативы «калькулятору» от ФСТЭК России рассмотрим «калькулятор» от корпорации MITRE, оперирующий техниками из уже знакомой нам матрицы ATT&CK®: https://top-attack-techniques.mitre-engenuity.org/calculator.

Его основное ограничение – это получение только ТОП-10 техник.

При расчёте данного ТОП-а учитываются следующие параметры:

- частота использования техники атакующим
- критичность техники для успеха всей атаки («узкое место» для атакующего)
- возможность обнаружения и митигации техники

Деревья атак

В завершении ещё затронем вариант моделирования угроз с использованием деревьев атак (attack trees). Фактически это метод визуального представления и анализа определённых способов реализации угроз. Он так же применяется в смежных областях, наиболее популярные - это деревья ошибок/отказов (fault trees) для различных систем.

Цель угрозы помещается в корне (дерево растёт сверху вниз), а ветви и листья – это различные способы (этапы) реализации угрозы. Лучше один раз увидеть, чем сто раз услышать.

Его главным преимуществом является наглядность. Однако, есть и недостаток: т.к. нужна отдельная схема на каждую цель, может возникнуть определённая сложность сопоставления схем между собой и получения итогового перечня актуальных способов реализации угроз.

Ключевые проблемы при моделировании угроз

- ☑ Моделирование угроз «для галочки» (отчитаться перед «проверяющими»).
- ☑ Одноразовое моделирование угроз (только на этапе создания системы).
- ☑ Моделирование в одиночку.
- ☑ Ментальные ловушки:
- «снаряд дважды в одну воронку не попадает»: мы уже подвергались данной кибератаке, значить такого больше не будет в ближайшее время
- «страшно или опасно?»: выставление приоритетов нарушителям/угрозам/уязвимостям на основе страхов, а не реальной ситуации и уровней опасности

Заключение по блоку определения актуальных угроз

Существует множество вариантов определения актуальных угроз – понимайте их достоинства и недостатки.

Используйте наиболее удобный Вам вариант определения актуальных угроз, приносящий воспроизводимые результаты.

Используйте удобный Вам вариант описания (если нет обязательных нормативных требований в этой части):

- объекты и связи в интерфейсе системы / программы
- объекты и связи на графической схеме (например, в формате vsdx или др.)
- текст в файле любого формата (например, в форматах docx, xlsx или др.)

На регулярной основе актуализируйте модель угроз.

Модель угроз – это теория, по возможности подтверждайте её практикой:

- тестирование на проникновения
- киберучения
- аудит ИБ

Классы мер защиты. Варианты выбора и обоснования мер защиты

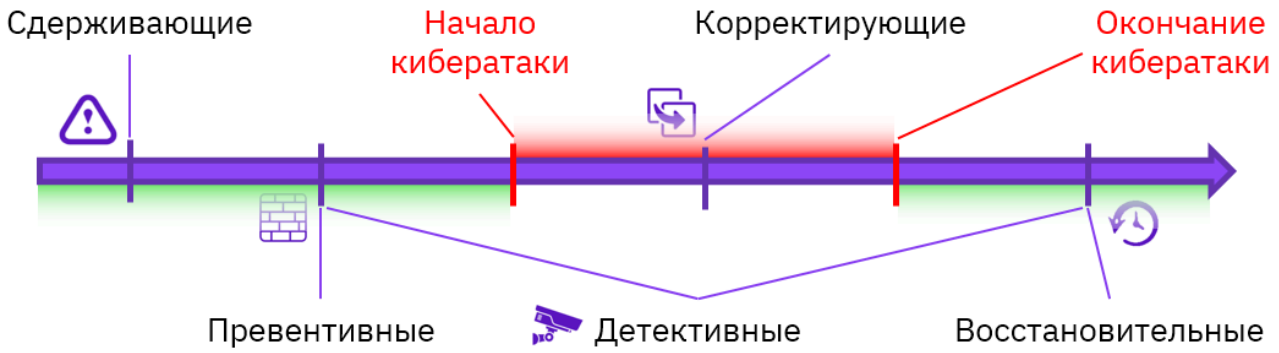
Стоит начать с того, что меры защиты информации (control) – это принятые правила, процедуры или механизмы, направленные на защиту информации, т.е. очень широкое понятие.

Меры защиты угроз условно можно разделить на следующие классы:

- сдерживающие, направленные на недопущение несанкционированных действий (например, любая вывеска «Объект находится под охраной», предупреждающий баннер в ПО или веб-браузере и т.п.)
- превентивные, направление на пресечение несанкционированных действий (например, любая система контроля доступа, межсетевой экран и т.п.)
- детективные, направление на обнаружение несанкционированных действий (например, система видеонаблюдения, журнал аудита ПО и т.п.)

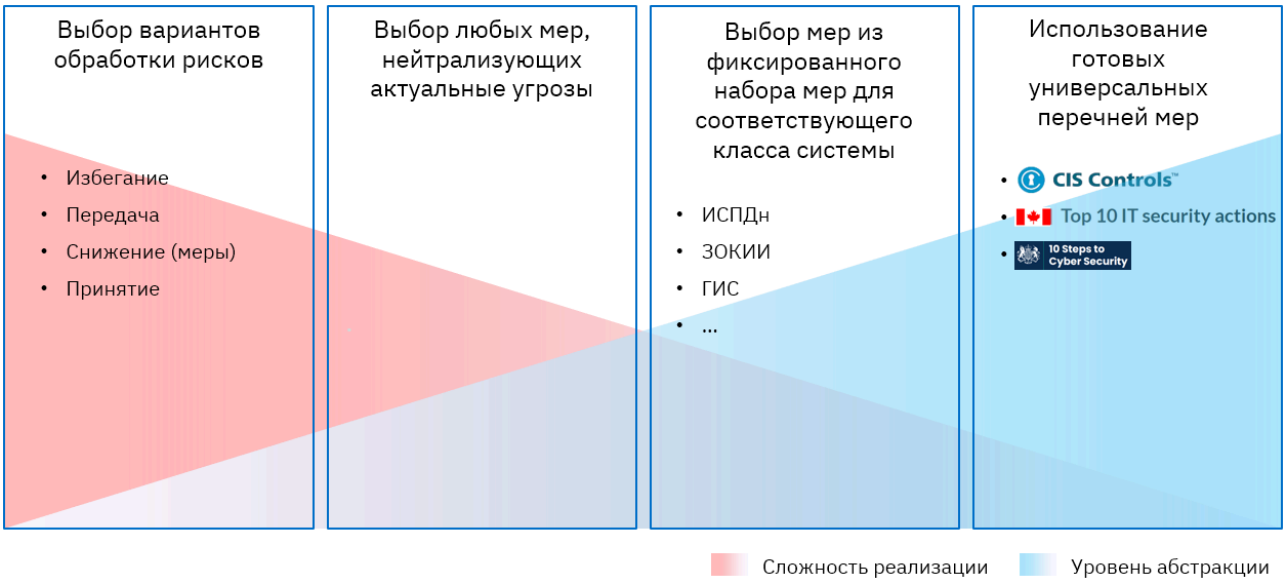
- корректирующие, направленные на изменение ситуации (например, вызов и действия охраны/полиции, лечение файла антивирусом, установка патча и т.п.)
- восстановительные, направленные на возврат к нормальному режиму работы (например, перезапуск сервисов, восстановление из резервных копий и т.п.)
- компенсирующие – как альтернатива любой другой мере, в случае если по какой-то объективной причине её нельзя применить (например, нет возможности повесить камеру видеонаблюдения (т.к. нет электропитания) – тогда периодический обход территории; нет возможности поставить антивирусное ПО (т.к. не совместим с ОС) – тогда блокировка USB-портов и доступ в сеть Интернет на ограниченный список веб-ресурсов и т.п.)

Применимость различных классов мер защиты с привязкой к началу и окончанию кибератаки условно можно отразить следующим образом:



Варианты выбора и обоснования мер защиты условно можно разделить на следующие группы:

- выбор вариантов обработки рисков ИБ
- выбор любых мер защиты, нейтрализующих или существенно затрудняющих реализацию актуальных угроз
- выбор мер защиты из фиксированного набора мер защиты для советующего класса (уровня) защищённости системы
- использование готовых ТОП-ов (перечней) мер защиты



Слева направо снижается сложность реализации предлагаемого варианта, но при это возрастает и абстрактность получаемых результатов. Таким образом, потребуется найти баланс между доступными вашей команде ресурсами, в т.ч. временны́ми, и релевантностью получаемых результатов.

Давайте последовательно рассмотрим эти варианты, начиная с выбора вариантов обработки рисков ИБ.

В **первом варианте** существует четыре возможных сценария:

- избежать риска, т.е. отказаться от действий или использования систем, которые этот риск создают
- передать риск, т.е. передача действий и систем на аутсорсинг, страхование и т.п.
- снизить (митигировать) риск, т.е. принять любые меры защиты, которые снизят вероятность возникновения риска и/или ущерб в случае его возникновения
- принять риск, т.е. не принимать никаких мер защиты и продолжать использовать системы

Второй вариант – это выбор любых мер защиты, нейтрализующих или существенно затрудняющих реализацию актуальных угроз. Для этого можно использовать любые реестры (перечни) мер.

Например, меры на базе методического документа ФСТЭК России [6], которые можно сгруппировать в следующие группы (самих же мер там более 100):

- идентификация и аутентификация пользователей/устройств

- управление доступом (дискреционный, мандатный, ролевой или иной метод)
- ограничение программной среды (контроль за установкой/запуском ПО)
- защита машинных носителей (учёт, контроль использования и уничтожения)
- регистрация событий безопасности (ведение и анализ журналов аудита)
- антивирусная защита
- обнаружение вторжений
- контроль (анализ) защищенности
- обеспечение целостности системы и информации
- обеспечение доступности системы и информации
- защита среды виртуализации
- защита технических средств (оборудования)
- защита сети
- выявление и реагирование на инциденты ИБ
- управление конфигурацией системы
- управление обновлениями ПО
- информирование и обучение персонала

Или перечень мер защиты из стандарта ISO/IEC 27001, в котором 14 категорий и более 100 контролей:

- политика ИБ
- организация деятельности по ИБ
- безопасность, связанная с персоналом
- управление активами
- управление доступом
- криптографическая защиты
- физическая защита
- операционная безопасность (безопасность при эксплуатации систем)
- безопасность коммуникаций
- безопасность при приобретении, разработке и поддержке систем
- безопасность при взаимодействии с поставщиками
- управление инцидентами ИБ
- безопасность в рамках обеспечения непрерывности бизнеса
- соответствие требованиям

Третий вариант – это выбор мер защиты из фиксированного набора мер защиты для советующего класса (уровня и т.п.) защищённости системы согласно нормативно-правовым и методическим документам, например:

- мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных
- меры защиты информации в государственных информационных системах
- мер по обеспечению безопасности значимых объектов критической информационной инфраструктуры
- меры защиты информации, применяемые финансовыми организациями для реализации требований к обеспечению защиты информации, установленных нормативными актами Банка России

И наконец, последний, **четвёртый вариант** – это использование уже готовых перечней мер. Наиболее авторитетной вариант – это ТОП-18/20 так называемых «критических контролей». Его мы рассмотрим подробнее в следующем блоке.

Теперь давайте подробнее рассмотрим выбор мер защиты согласно методическому документу ФСТЭК России [6].

Предусмотрена следующая последовательность выбора мер защиты:

- определение базового набора мер защиты для установленного класса защищенности системы
- адаптация базового набора мер защиты применительно к структурно-функциональным характеристикам системы, информационным технологиям, особенностям функционирования системы
- уточнение адаптированного базового набора мер защиты информации с учётом не выбранных ранее мер защиты для блокирования (нейтрализации) всех угроз безопасности информации, включенных в модель угроз
- дополнение уточненного адаптированного базового набора мер защиты мерами, обеспечивающими выполнение требований о защите информации, установленными иными нормативными правовыми актами в области защиты информации, в т.ч. в области защиты персональных данных

Вне зависимости от используемого варианта на выходе вы получите перечень мер. Но из-за постоянно существующих ресурсных ограничений все меры одномоментно реализовать не получиться. Потребуется выставить им приоритеты.

> 💡 Выбирая и приоритизируя меры защиты помните о принципе «разумной достаточности» (разумное применение мер противодействия), т.е. затраты на защиту не должны превышать стоимость защищаемых систем и информации.

К вариантам приоритизация мер защиты можно отнести:

- принцип Парето (правило 80/20): отдавайте приоритет мерам, которые «покрывают» сразу несколько актуальных угроз
- концепция «низко висящих фруктов»: отдавайте приоритет мерам, которые вы быстро/менее затратно можете реализовать
- сначала превентивные меры, потом детективные

Популярные ИБ best practices и cybersecurity frameworks

Стандарты ISO/IEC 27k серии

Это серия из нескольких десятков стандартов, разрабатываемых и пополняемых Международной организацией по стандартизации (International Organization for Standardization) и Международной электротехнической комиссией (International Electrotechnical Commission), начиная с 2000 года.

Выступает де-факто эталонным стандартами в области управления (менеджмента) ИБ.

В настоящее время представляет из себя отдельную индустрию, в которой предусмотрены:

- подготовка и сертификация организаций
- обучение и сертификация специалистов
- различные инструменты и маппинги с другими стандартами

В Российской Федерации часть стандартов (редакций стандартов) получали переиздание в формате государственных стандартов, но, к сожалению, качество переводов и темпы обновлений не соответствуют оригиналам.

🔥 При изучении и применении на практике, не говоря уже о сертификации, используйте оригинальные издания, приобретаемые на веб-ресурсах: https://www.iso.org/ или https://www.standards.ru/ («язык оригинала: английский»).

Подход к работе с данной серией стандартов следующий:

- знакомство с актуальной версий ISO/IEC 27001 «Information security, cybersecurity and privacy protection — Information security management systems — Requirements»
- поиск и работа со стандартом по интересующей Вас тематике (например, сетевая безопасность (network security) - ISO/IEC 27033; безопасность хранение данных (data storage security) - ISO/IEC 27040; приватность (privacy) - ISO/IEC 27701 и т.д.)

NIST Cybersecurity Framework

Это один из стандартов (ныне framework) Национального института стандартов и технологий США (National Institute of Standards and Technology), появившийся в 2014 году.

Изначально, его областью примирения была критическая информационная инфраструктура США, но за счёт своей популярности им может пользоваться любая организация. Сейчас стандарт активно поддерживается многими организациями-производителями средств защиты информации.

Помимо самого стандарта, предоставляется готовый XLS-маппинг с другими стандартами, масса сопутствующих материалов.

Framework предусматривает пять ключевых блоков:

- *идентификация (identify):* определение рисков для всех активов, включая персонал, системы и информацию
- *превентивная защита (protect):* внедрение систем, обеспечивающих защиту наиболее важных активов
- *обнаружение (detect)*: выявление инцидентов ИБ
- *реагирование (respond):* реагирование на инциденты ИБ
- *восстановление (recover):* восстановление возможностей или сервисов, пострадавших в результате инцидентов ИБ

Top Critical Security Controls

Сейчас «критические контроли» курирует Центр безопасности Интернета (Center for Internet Security), ранее ими занимался SANS™ Institute.

Это уже приоритизированный и упрощённый набор лучших мер защиты (18-20 групп), но дополнительно приоритизированный в составе трёх логических групп конкретных контролей:

IG1 – основополагающие / «гигиенические» контроли (для малого и среднего бизнеса)

IG2 – широко применимые контроли для организаций с выделенным ИБ-подразделением

IG3 – специализированные / экспертные контроли

Список регулярно пересматривается.

CIS Controls
Version 8

01	Inventory and Control of Enterprise Assets
02	Inventory and Control of Software Assets
03	Data Protection
04	Secure Configuration of Enterprise Assets and
05	Account Management
06	Access Control Management
07	Continuous Vulnerability Management
08	Audit Log Management
09	Email and Web Browser Protections
10	Malware Defenses
11	Data Recovery
12	Network Infrastructure Management
13	Network Monitoring and Defense
14	Security Awareness and Skills Training
15	Service Provider Management
16	Application Software Security
17	Incident Response Management
18	Penetration Testing

Помимо самого списка, предоставляется готовый маппинг с другими стандартами, масса сопутствующих материалов. Материал активно поддерживается многими организациями-производителями средств защиты информации.

Проекты OWASP

Различные проекты, разрабатываемые сообществом Open Web Application Security Project, но ориентированные на веб-безопасность.

Среди наиболее популярных проектов можно выделить:

- Top 10 Web Application Security Risks
- API Security Top 10
- Mobile Top 10

Присутствует много сопутствующих материалов и сервисов, в т.ч. поддержка «Top 10 Web Application Security Risks» в базах знаний различных средств контроля (анализа) защищенности – сканерах безопасности.

Выводы

- Моделирование угроз – основополагающий этап построения системы защиты информации, но он не является безальтернативным вариантом выбора и обоснования мер защиты
- Существуют различные варианты определения актуальных угроз, имеющие свои достоинства и недостатки
- Понимание типовой последовательности кибератак позволяет адекватнее определять актуальные угрозы, помня, что человек – это самое слабое звено в любой системе безопасности
- Модель угроз требует регулярного пересмотра и поддержания в актуальном состоянии (вариант «сделал и забыл» не подходит)

- В части сведений об угрозах и уязвимостях нужно держать «руку на пульсе»
- Меры защиты нужно выбирать разумно, а также грамотно их приоритизировать
- Существуют различные best practices и cybersecurity frameworks, но любой из них потребует адаптации («доработки напильником»)

Дополнительные материалы

1. Книга «Threat Modeling: A Practical Guide for Development Teams», Изар Тарандач и Мэтью Дж. Коулз, 2020.
2. Новостной telegram-канал про уязвимости: t.me/CyberSecurityTechnologies.
3. Статья «Руководство по моделированию угроз для разработчиков», Джим Гамбли.
4. Статья «Общий обзор реестров и классификаций уязвимостей (CVE, OSVDB, NVD, Secunia)», Андрей Сапожников.
5. Статья «Системы классификации и оценки уязвимостей и угроз информационных систем: какие они бывают и зачем нужны», Ольга Роде.
6. Статья «Матрица ATT&CK. Как устроен язык описания угроз и как его используют», Борис Осепов и Александр Мессерле.
7. Статья «Обзор международных стандартов в области ИБ», Мария Романычева.

Использованная литература

1. Методический документ «Методика оценки угроз безопасности информации», ФСТЭК России, 2021.
2. Методический документ «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», ФСТЭК России, 2008.
3. ГОСТ Р 52448-2005 «Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения».

4. ГОСТ Р 56546-2015 «Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем».

5. Статья «Модели кибератак. Систематизируем защиту и нападение», Александр Кузнецов.

6. Статья «Моделирование нарушителя. Как узнать своего врага в лицо», Александр Кузнецов.

7. Методический документ «Меры защиты информации в государственных информационных системах», ФСТЭК России, 2014.