Введение в информационную безопасность

Введение

Защита информации – это обеспечение

1) целостности,
2) конфиденциальности,
3) доступности информационных ресурсов (информация и средства её обработки).

Дополнительными свойствами информации в состоянии защищенности являются:

4) неотказуемость,
5) подлинность,
6) подотчетность.

Введение

Угроза безопасности информации – это потенциальная причина возникновения нежелательного инцидента информационной безопасности, который может нанести ущерб активам и нарушить состояние защищенности информации (одного из 6 свойств выше). Инциденту может предшествовать несанкционированное изменение состояния актива, называющееся событием информационной безопасности.

Моделирование угроз – это идентификация всех угроз, которые могут нанести ущерб активам, и векторов атак, которые могут быть использованы источниками угроз для нанесения ущерба.

Ущерб:

- ***прямой*** – непосредственные очевидные и легко прогнозируемые потери компании;
- ***непрямой*** – потери качественные (снижение эффективности деятельности, потеря клиентов) или косвенные (недополученная прибыль, потеря деловой репутации).

Угроза безопасности информации возникает при наличии следующих взаимосвязанных компонентов:

1) источник угрозы,
2) уязвимость актива,
3) способ реализации угрозы,
4) объект воздействия,
5) вредоносное воздействие и его последствия.

1 Источники угрозы

Внешние нарушители не имеют легитимного доступа к объекту защиты, т.е. не являются сотрудниками компании, легитимными пользователями внутренних информационных систем, аутсорсерами, подрядчиками, поставщиками, заказчиками и прочими лицами, связанными юридическими отношениями с рассматриваемой организацией.

Меры противодействия: весь спектр способов обеспечения информационной безопасности; проведение оценки подверженности компании риску атаки со стороны внешних злоумышленников.

Источники угрозы

Внутренние нарушители – сотрудники и руководители компании, а также юридические лица, которые имеют договорные отношения с компанией; отличаются хорошими знаниями о работе атакуемого актива, имеют или могут получить к нему доступ, зачастую санкционированный и с расширенными полномочиями.

Условная градация инсайдеров:

– халатные,
– саботирующие,
– увольняющиеся,
– целенаправленные.

Меры противодействия: технические (DLP, IAM, в т.ч. для борьбы с попавшими в ЛВС внешними атакующими), физические (СКУД, CCTV), организационные. Оценка подверженности риску. Управление аутсорсерами, в т.ч. провайдерами услуг, которые могут использоваться как плацдарм для дальнейшей атаки («атаки на цепочки поставок»).

Источники угрозы

Третьи лица, силы природы – еще одна категория нарушителей.

Меры противодействия: соблюдение законодательства, процедуры обеспечения непрерывности деятельности и восстановления работоспособности, учебные тревоги, страхование.

Модель нарушителя по ФСБ РФ

«Методические рекомендации по разработке НПА для угроз безопасности ПДн», 2015 г.

Возможности нарушителей:

1) Возможность проводить атаки за пределами КЗ.
2) Возможность проводить атаки в пределах КЗ без физического доступа к СВТ.
3) Возможность проводить атаки в пределах КЗ с физическим доступом к СВТ.
4) Возможность привлекать специалистов для анализа ПЭМИН.
5) Возможность привлекать специалистов для использования НДВ в прикладном ПО.
6) Возможность привлекать специалистов для использования НДВ в ПО/АО.

На основе МН осуществляется построение ***модели угроз (МУ)***, ***выбор классов СЗИ, СКЗИ,*** проводится оценка наличия ***способов, мотивов, возможностей*** злоумышленников.

Пример списка нарушителей

Внешние нарушители:

- Посетитель веб-сайта (случайный / зарегистрированный клиент);
- Хакеры-самоучки низкой квалификации;
- Киберпреступники «среднего звена»;
- Нанятые конкурентами злоумышленники;
- Высококвалифицированные хакеры, международные хакерские группы;
- Организованные группы киберсолдат и киберармии.

Внутренние нарушители:

- Инсайдеры разного уровня доступа (пользователи, администраторы, архитекторы) и разной степени лояльности;
- Нанятые конкурентами/хакерами инсайдеры.

Третьи лица:

- Государственные контролирующие органы.

Силы природы:

- Стихийные бедствия (природные и техногенные катастрофы: потопы, пожары, землетрясения); социальные катастрофы (эпидемии, теракты, вооруженные конфликты).

2 Уязвимости

ГОСТ Р 56546-2015 «Защита информации. УЯЗВИМОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ. Классификация уязвимостей информационных систем»:

Уязвимость – это недостаток программно-технического средства или информационной системы в целом, который может быть использован для реализации угроз безопасности информации.

ISO/IEC 27000:2018 «Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология»:

Уязвимость – это слабое место актива или средства контроля и управления, которое может быть использовано злоумышленниками.

Типы уязвимостей

Возможные ***типы уязвимостей*** (по ГОСТ Р 56546-2015):

- ***уязвимость кода*** – уязвимость, появившаяся в процессе разработки программного обеспечения;
- ***уязвимость конфигурации*** – уязвимость, появившаяся в процессе настройки программного обеспечения и технических средств;
- ***уязвимость архитектуры*** – уязвимость, появившаяся в процессе проектирования информационной системы;
- ***организационная уязвимость*** – уязвимость, связанная с недостатками организационных мер, такими как несоблюдение сотрудниками правил эксплуатации системы или требований нормативных документов;
- ***многофакторная уязвимость*** – уязвимость, появившаяся в результате комбинации нескольких уязвимостей перечисленных типов.

Места возникновения уязвимостей

Потенциальные ***места возникновения уязвимостей*** (по ГОСТ Р 56546-2015):

– ***уязвимости в общесистемном ПО*** – в операционных системах, СУБД, файловых системах, драйверах;
– ***уязвимости в прикладном ПО*** – во всех тех программах, которые может установить и запускать пользователь;
– ***уязвимости в специальном ПО*** – в программах, разработанных для решения специфических задач данной системой;
– ***уязвимости в технических средствах*** – в прошивках, BIOS, микроконтроллерах;
– ***уязвимости в портативных технических средствах*** – в мобильных устройствах и приложениях для них, а также в аппаратном обеспечении данных устройств;
– ***уязвимости в сетевом оборудовании*** – в маршрутизаторах, коммутаторах, модемах и т.д.;
– ***уязвимости в средствах защиты информации***.

Степень опасности уязвимости

Уязвимость характеризуется степенью своей ***опасности***, которая стандартом ГОСТ Р 56546-2015 определяется как сравнительная величина, характеризующая подверженность информационной системы уязвимости и ее влияние на нарушение свойств безопасности информации (конфиденциальность, целостность, доступность).

Шкала оценок уязвимостей CVSS (v2, v3), реестры уязвимостей (БДУ ФСТЭК, MITRE CVE, NIST NVD, CERT/CC NVD).

3 Способы реализации угроз

Способы (методы) реализации угроз (по методике ФСТЭК России):

- ***несанкционированный сбор информации*** – сбор и кража информации об объекте воздействия;
- ***исчерпание ресурсов*** – намеренное злоупотребление ресурсами системы для нарушения её функционирования;
- ***инъекция*** – установление контроля над атакуемой системой с помощью манипулирования входными данными;
- ***подмена при взаимодействии*** – умышленное искажение представления источника угрозы как доверенного субъекта;
- ***манипулирование сроками и состоянием*** – искажение параллельно выполняющегося потока задач путем нарушения временной синхронизации или информации о состоянии системы;

Способы реализации угроз

- ***злоупотребление функционалом*** – деструктивное использование штатных функций системы;
- ***вероятностные методы*** – использование вероятностных методов для изучения и преодоления механизмов безопасности системы;
- ***нарушение аутентификации*** – эксплуатация уязвимостей механизмов идентификации и аутентификации;
- ***нарушение авторизации*** – эксплуатация уязвимостей механизмов управления доступом к ресурсам и функциональным возможностям системы;
- ***манипулирование структурами данных*** – манипулирование характеристиками структур данных для нарушения предполагаемого использования и обхода защиты этих структур;
- ***анализ целевого объекта*** – изучение работы атакуемой системы в целях обхода средств её защиты или для подготовки и проведения других атак;

Способы реализации угроз

– ***манипулирование ресурсами*** – злонамеренное использование штатных ресурсов (файлов, приложений, библиотек, инфраструктуры, конфигурации системы);
– ***использование технических отказов, ошибок*** – эксплуатация программных и аппаратных уязвимостей;
– ***получение физического доступа*** – деструктивное воздействие на аппаратные компоненты системы;
– ***использование слабостей в организации*** – эксплуатация недостатков законодательства или организационных мер защиты.

Тактики атакующих

Тактики атакующих (по MITRE ATT&CK, подход Cyber Kill Chain):

- ***сбор информации о цели, подготовка вредоносного ПО, фишинговой кампании***;
- ***первоначальный доступ*** – техники первичного проникновения в защищаемую сеть;
- ***исполнение*** – техники запуска вредоносного кода на локальной или удаленной системе;
- ***закрепление*** – техники получения злоумышленниками постоянного несанкционированного доступа к системе;
- ***повышение привилегий*** – техники, применяемые атакующими для повышения своих привилегий до системных/административных с целью получения более широких полномочий на скомпрометированной системе;
- ***обход средств защиты*** – техники, с помощью которых злоумышленникам удается избежать обнаружения и противодействия со стороны механизмов защиты;

Тактики атакующих

- ***доступ к учетным данным*** – техники получения валидных учетных данных к атакуемым системам с правами легитимных пользователей и администраторов;
- ***исследование*** – техники получения информации о свойствах атакованной системы/сети;
- ***дальнейшее продвижение*** – техники расширения несанкционированного доступа в атакованной сети с использованием уже захваченных систем;
- ***сбор данных*** – техники получения ценной информации в атакованных системах/сетях;
- ***управление и контроль*** – техники, с помощью которых злоумышленники извне управляют взломанными системами/сетями;
- ***вывод данных*** – перенос собранной ценной информации из взломанных систем/сетей в системы/сети злоумышленников;
- ***воздействие*** – техники негативного воздействия на доступность или целостность атакованных систем, служб или сетей.

Пример тактики

Каждая тактика раскрывается в виде набора конкретных техник атакующих с определенным условным идентификатором.

TACTICS

- Enterprise
  - Reconnaissance
  - Resource Development
  - Initial Access
  - Execution
  - Persistence
  - Privilege Escalation
  - Defense Evasion
  - Credential Access
  - Discovery
  - Lateral Movement
  - Collection
  - Command and Control
  - Exfiltration
  - Impact
- Mobile

Home > Tactics > Enterprise > Initial Access

Initial Access

The adversary is trying to get into your network.

Initial Access consists of techniques that use various entry vectors to gain their initial foothold within a network. Techniques used to gain a foothold include targeted spearphishing and exploiting weaknesses on public-facing web servers. Footholds gained through initial access may allow for continued access, like valid accounts and use of external remote services, or may be limited-use due to changing passwords.

ID: TA0001
Created: 17 October 2018
Last Modified: 19 July 2019

Version Permalink

Techniques

Techniques: 9

ID	Name	Description
T1189	Drive-by Compromise	Adversaries may gain access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is typically targeted for exploitation, but adversaries may also use compromised websites for non-exploitation behavior such as acquiring Application Access Token.
T1190	Exploit Public-Facing Application	Adversaries may attempt to take advantage of a weakness in an Internet-facing computer or program using software, data, or commands in order to cause unintended or unanticipated behavior. The weakness in the system can be a bug, a glitch, or a design vulnerability. These applications are often websites, but can include databases (like SQL), standard services (like SMB or SSH), network device administration and management protocols (like SNMP and Smart Install), and any other applications with Internet accessible open sockets, such as web servers and related services. Depending on the flaw being exploited this may include Exploitation for Defense Evasion.
T1133	External Remote Services	Adversaries may leverage external-facing remote services to initially access and/or persist within a network. Remote services such as VPNs, Citrix, and other access mechanisms allow users to connect to internal enterprise network resources from external locations. There are often remote service gateways that manage connections and credential authentication for these services. Services such as Windows Remote Management and VNC can also be used externally.
T1200	Hardware Additions	Adversaries may introduce computer accessories, computers, or networking hardware into a system or network that can be used as a vector to gain

4 Объекты воздействия

Объектами воздействия являются:

– ***люди;***
– ***Информация;***
– ***процессы разработки;***
– ***производства и поставки;***
– ***каналы передачи данных;***
– ***программные и аппаратные средства и компоненты систем.***

Люди – самое слабое звено (социальная инженерия, фишинг) => важность программ повышения осведомленности сотрудников в вопросах защиты информации.

5 Вредоносное воздействие и его последствия

Вредоносное воздействие – нарушение целостности, конфиденциальности, доступности информационных ресурсов, атаки на неотказуемость, подлинность, подотчетность информации.

Защитные меры подразделяются на:

– организационные;
– технические;
– физические;

применяются к:

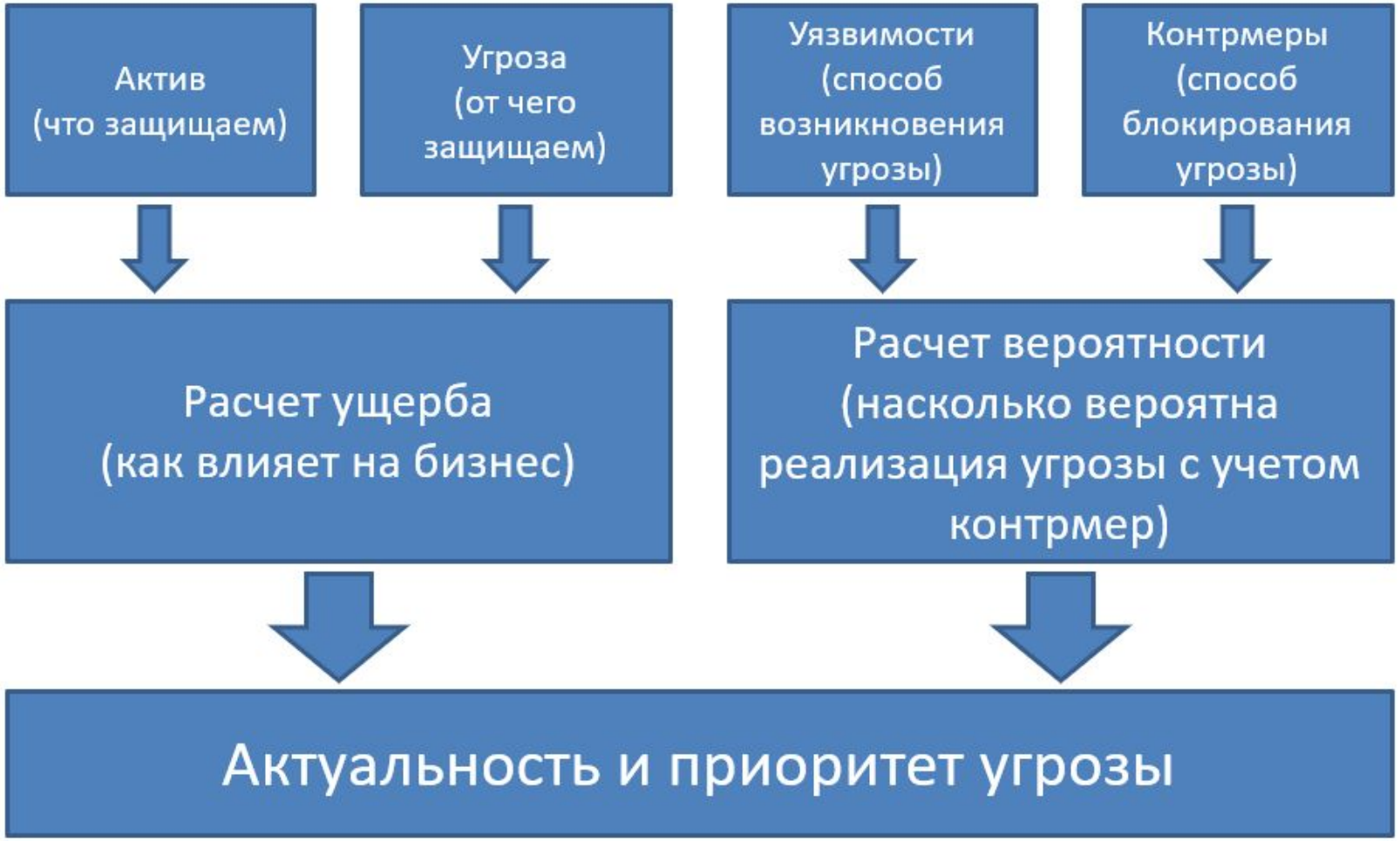
– сотрудникам;
– процессам;
– технологиям.

Цели применения мер

По ***целям применяемых*** мер существует разделение на меры:

– ***предупредительные;***
– ***директивные;***
– ***превентивные;***
– ***сдерживающие;***
– ***корректирующие;***
– ***восстановительные;***
– ***расследовательные;***
– ***компенсирующие.***

Блок-схема процесса моделирования угроз ИБ



Моделирование угроз

Моделирование угроз по Проекту документа ФСТЭК России «Методика моделирования угроз безопасности информации» (2020 г.).

Процесс моделирования угроз ИБ состоит из следующих этапов:

1) ***определение возможных негативных последствий*** от реализации угроз по результатам оценки рисков нарушения бизнес-процессов и/или нарушения защищенности информации, что может привести к таким негативным последствиям, как экономический или репутационный ущерб;

2) ***определение условий для реализации угроз безопасности информации***, т.е. выявление возможных путей доступа к ИТ-системам, которые могут быть использованы злоумышленниками;

3) ***определение источников угроз и оценка возможностей нарушителей*** (внешних и внутренних);

4) ***определение сценариев реализации угроз*** с помощью перечня тактик и техник атакующих;

5) ***оценка уровня опасности угроз безопасности информации*** путем анализа типа доступа, необходимого для реализации атаки, сложности сценария атаки и уровня важности атакуемых активов.

Риск информационной безопасности

Риск информационной безопасности – это потенциальная возможность использования уязвимостей активов конкретной угрозой для причинения ущерба организации.

*ВеличинаРиска=ВероятностьСобытия*РазмерУщерба*, где

*ВероятностьСобытия=ВероятностьУгрозы*ВеличинаУязвимости.*

Способы обработки риска ИБ:

– игнорировать,
– принять,
– избежать,
– передать,
– минимизировать.

Минимизация рисков информационной безопасности

Стоимость контрмер < Стоимость актива > Стоимость атаки (где «<» и «>» – это операторы количественного сравнения).

Цели ***анализа*** рисков ИБ:

– Идентифицировать активы и оценить их ценность.
– Идентифицировать угрозы активам и уязвимости в системе защиты.
– Просчитать вероятность реализации угроз и их влияние на бизнес.
– Соблюсти баланс между стоимостью возможных негативных последствий и стоимостью мер защиты, дать рекомендации руководству компании по обработке выявленных рисков.

Процессы, проекты, функции

Проект – однократное выполнение некоторой новой задачи для достижения определенной цели. Характеристики проекта: стоимость, качество (масштаб, граница), время на реализацию. Цели проекта должны быть конкретными, измеримыми, достижимыми, релевантными, ограниченными по времени.

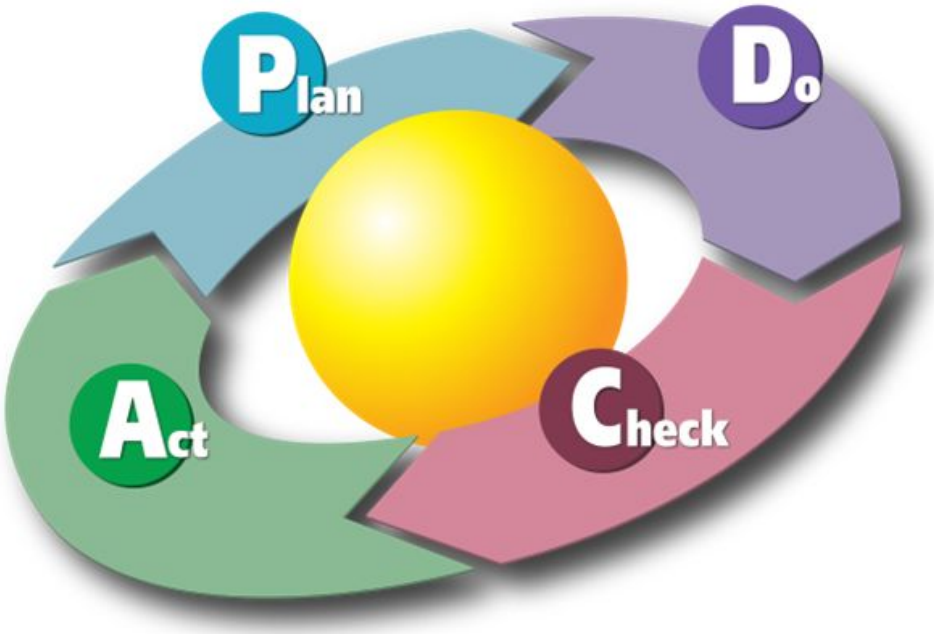
Функция – выполнение некоторой задачи по алгоритму вне зависимости от потребностей конечного получателя.

Процесс – непрерывное выполнение задач с применением гибких, настраиваемых технологий, в целях удовлетворения потребностей конечного получателя.

Процессы ИБ – использование мер и средств защиты (организационных, технических, физических) для минимизации рисков ИБ в целях удовлетворения потребностей бизнес-заказчиков.

Цикл Деминга для управления процессами

Цикл Деминга для управления процессами:
Plan – Do – Check – Act (P.D.C.A.-цикл)
Планирование – Выполнение – Оценка – Корректировка



Модель зрелости процессов (ИБ)

Модель CMMI (Capability Maturity Model Integration – Модель зрелости интеграции) можно использовать для оценки зрелости процессов ИБ. Конечная цель: выстроенные, адекватные процессы ИБ, решающие поставленную задачу.

Уровни ***зрелости*** процессов:

1) уровень (initial) – первичный уровень, хаотичность, реактивность.

2) уровень (repeatable) – процессы не задокументированы, но повторяются, реактивность присутствует в меньшем объеме.

3) уровень (defined) – процессы задокументированы, все действия проактивны.

4) уровень (managed) – процессы контролируются и могут быть оценены количественно.

5) уровень (optimizing) – все процессы непрерывно улучшаются, оптимизируются.

Спасибо за внимание!