Анализ защищенности объекта защиты информации

Основы информационной безопасности

Количественный анализ рисков

Рассмотрим методику на примере веб-сервера организации, который используется для продажи определенного товара.
Количественный разовый ущерб от выхода сервера из строя можно оценить как произведение среднего чека покупки на среднее число обращений за определенный временной интервал, равное времени простоя сервера. Допустим, стоимость разового ущерба от прямого выхода сервера из строя составит 100 тысяч рублей.
Теперь следует оценить экспертным путем, как часто может возникать такая ситуация (с учетом интенсивности эксплуатации, качества электропитания и т д.). Например, с учетом мнения экспертов и статистической информации, мы понимаем, что сервер может выходить из строя до 2 раз в год.
Умножаем две эти величины, получаем, что **среднегодовой** ущерб от реализации угрозы прямого выхода сервера из строя составляет 200 тысяч рублей в год.

Количественный анализ рисков

Эти расчеты можно использовать при обосновании выбора защитных мер. Например, внедрение системы бесперебойного питания и системы резервного копирования общей стоимостью 100 тысяч рублей в год позволит минимизировать риск выхода сервера из строя и будет вполне эффективным решением.

Угрозы безопасности ИС

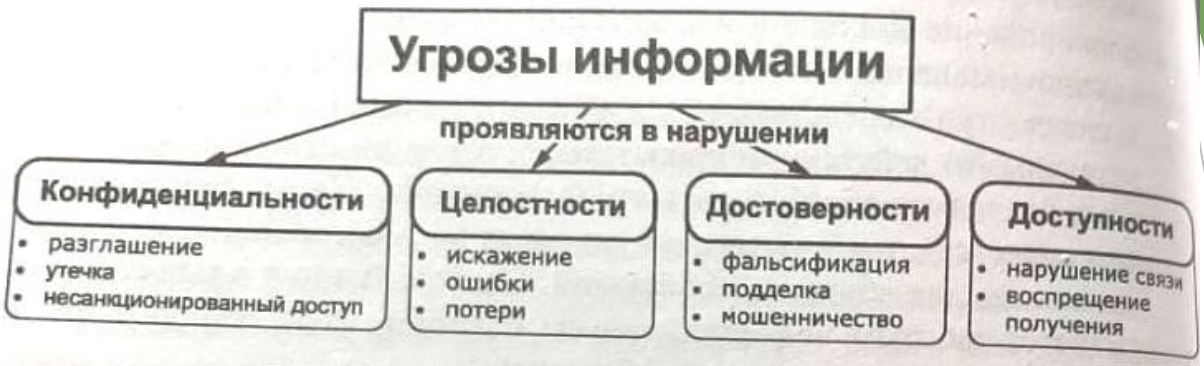

Рис. 1.16. Классификация воздействий угроз на безопасность информации

Рис. 1.17. *Классификация угроз неизменности (целостности) информации*

Угрозы безопасности ИС

Угрозы безопасности ИС

Свойства информации, подверженные влиянию угроз

Способы нанесения ущерба	Объекты воздействий			
	оборудование	программы	данные	персонал
Раскрытие (утечка) информации	Хищение носителей информации, подключение к линии связи, несанкционированное использование ресурсов	Несанкционированное копирование, перехват	Хищение, копирование, перехват	Передача сведений о защите, разглашение, халатность
Потеря целостности информации	Подключение, модификация, специальные вложения, изменение режимов работы, несанкционированное использование ресурсов	Внедрение «троянских коней» и «жучков»	Искажение, модификация	Вербовка персонала, «маскарад»
Нарушение работоспособности автоматизированной системы	Изменение режимов функционирования, вывод из строя, хищение, разрушение	Искажение, удаление, подмена	Искажение, удаление, навязывание ложных данных	Уход, физическое устранение
Незаконное тиражирование (воспроизведение) информации	Изготовление аналогов без лицензий	Использование незаконных копий	Публикация без ведома авторов	

Оценка риска угроз

2. Характер происхождения угроз

- 2.1. Умышленные факторы
  - 2.1.1. Хищение носителей информации
  - 2.1.2. Подключение к каналам связи
  - 2.1.3. Перехват электромагнитных излучений (ЭМИ)
  - 2.1.4. Несанкционированный доступ
  - 2.1.5. Разглашение информации
  - 2.1.6. Копирование данных
- 2.2. Естественные факторы
  - 2.2.1. Несчастные случаи (пожары, аварии, взрывы)
  - 2.2.2. Стихийные бедствия (ураганы, наводнения, землетрясения)
  - 2.2.3. Ошибки в процессе обработки информации (ошибки пользователя, оператора, сбои аппаратуры)

Оценка риска угроз

Источники угроз (понимается непосредственный исполнитель угрозы в плане ее негативного воздействия на информацию):

- люди;
- технические устройства;
- модели, алгоритмы, программы;
- технологические схемы обработки;
- внешняя среда. Предпосылки появления угроз:
- объективные (количественная или качественная недостаточность элементов системы) - причины, не связанные непосредственно с деятельностью людей и вызывающие случайные по характеру происхождения угрозы;
- субъективные - причины, непосредственно связанные с деятельностью человека и вызывающие как преднамеренные (деятельность разведок иностранных государств, промышленный шпионаж, деятельность уголовных элементов и недобросовестных сотрудников), так и непреднамеренные (плохое психофизиологическое состояние, недостаточная подготовка, низкий уровень знаний) угрозы информации.

Оценка риска угроз

Классы каналов несанкционированного получения информации
Рассмотрим относительно полное множество каналов несанкционированного получения информации, сформированного на основе такого показателя, как степень взаимодействия злоумышленника с элементами объекта обработки информации и самой информацией.
К первому классу относятся каналы от источника информации при НСД к нему.
Хищение носителей информации.
Копирование информации с носителей (материально-вещественных, магнитных и т. д.).
Подслушивание разговоров (в том числе аудиозапись).
Установка закладных устройств в помещение и съем информации с их помощью.
Выведывание информации обслуживающего персонала на объекте.
Фотографирование или видеосъемка носителей информации внутри помещения.

Классы каналов несанкционированного получения информации

Ко второму классу относятся каналы со средств обработки информации при НСД к ним.

Снятие информации с устройств электронной памяти.
Установка закладных устройств в СОИ.
Ввод программных продуктов, позволяющих злоумышленнику получать информацию.
Копирование информации с технических устройств отображения (фотографирование с мониторов и др.).

Классы каналов несанкционированного получения информации

К третьему классу относятся каналы от источника информации без
Получение информации по акустическим каналам (в системах вентиляции, теплоснабжения, а также с помощью направленных микрофонов).
Получение информации по виброакустическим каналам (с использованием акустических датчиков, лазерных устройств).
Использование технических средств оптической разведки (биноклей, подзорных труб и т. д.).
Использование технических средств оптико-электронной разведки (внешних телекамер, приборов ночного видения и т. д.).
Осмотр отходов и мусора.
Выведывание информации у обслуживающего персонала за пределами объекта.
Изучение выходящей за пределы объекта открытой информации (публикаций, рекламных проспектов и т. д.).

Классы каналов несанкционированного получения информации

К четвертому классу относятся каналы со средств обработки информации без НСД к ним.
Электромагнитные излучения СОИ (паразитные электромагнитные излучения (ПЭМИ), паразитная генерация усилительных каскадов, паразитная модуляция высокочастотных генераторов низкочастотным сигналом, содержащим конфиденциальную информацию).
Электромагнитные излучения линий связи.
Подключения к линиям связи.
Снятие наводок электрических сигналов с линий связи.
Снятие наводок с системы питания.
Снятие наводок с системы заземления.
Снятие наводок с системы теплоснабжения.
Использование высокочастотного навязывания.
Снятие с линий, выходящих за пределы объекта, сигналов, образованных на технических средствах за счет акустоэлектрических преобразований.
Снятие излучений оптоволоконных линий связи.
Подключение к базам данных и ПЭВМ по компьютерным сетям.

Причины нарушения целостности информации

10.2. Причины нарушения целостности информации

1. Субъективные

1.1. Преднамеренные

1.1.1. Диверсия (организация пожаров, взрывов, повреждений электропитания и др.)

1.1.2. Непосредственные действия над носителем (хищение, подмена носителей, уничтожение информации)

1.1.3. Информационное воздействие (электромагнитное облучение, ввод в компьютерные системы разрушающих программных средств, воздействие на психику личности психотропным оружием)

1.2. Непреднамеренные

1.2.1. Отказы обслуживающего персонала (гибель, длительный выход из строя)

1.2.2. Сбои людей (временный выход из строя)

1.2.3. Ошибки людей

Причины нарушения целостности информации

2. Объективные, непреднамеренные

2.1. Отказы (полный выход из строя) аппаратуры, программ, систем питания и жизнеобеспечения

2.2. Сбои (кратковременный выход из строя) аппаратуры, программ, систем питания и жизнеобеспечения

2.3. Стихийные бедствия (наводнения, землетрясения, ураганы)

2.4. Несчастные случаи (пожары, взрывы, аварии)

2.5. Электромагнитная несовместимость

Оценка риска угроз

- **Цель:** Формирование умений и навыков определения угроз и защищённости объектов информации
- Для выбранного определенного объекта защиты информации (номер варианта соответствует номеру студента по списку) необходимо описать объект защиты, провести анализ защищенности объекта защиты информации по следующим разделам:

  1 виды угроз;

  2 характер происхождения угроз;

  3 классы каналов несанкционированного получения информации;

  4 источники появления угроз;

  5 причины нарушения целостности информации;

Оценка риска угроз

Наименование объекта защиты информации:

1) Одиночно стоящий компьютер в бухгалтерии.

2) Сервер в бухгалтерии.

3) Почтовый сервер.

4) Веб-сервер.

5) Компьютерная сеть материальной группы.

6) Одноранговая локальная сеть без выхода в Интернет.

7) Одноранговая локальная сеть с выходом в Интернет.

8) Сеть с выделенным сервером без выхода в Интернет.

9) Сеть с выделенным сервером с выхода в Интернет.

10) Телефонная база данных (содержащая и информацию ограниченного пользования) в твердой копии и на электронных носителях.

Оценка риска угроз

Наименование объекта защиты информации:

11) Телефонная сеть.

12) Средства телекоммуникации (радиотелефоны, мобильные телефоны).

13) Банковские операции (внесение денег на счет и снятие).

14) Операции с банковскими пластиковыми карточками.

15) Компьютер, хранящий конфиденциальную информацию о сотрудниках предприятия.

16) Компьютер, хранящий конфиденциальную информацию о разработках предприятия.

17) Материалы для служебного пользования на твердых носителях и на электронных носителях в производстве.

18) Материалы для служебного пользования на твердых носителях и на электронных носителях на закрытом предприятии.

Анализ защищенности объекта защиты информации

Наименование объекта защиты информации:

19) Материалы для служебного пользования на твердых носителях в архиве.

20) Материалы для служебного пользования на твердых носителях и на электронных носителях в налоговой инспекции.

21) Комната для переговоров по сделкам на охраняемой территории.

22) Комната для переговоров по сделкам на неохраняемой территории.

23) Сведения для средств массовой информации, цензура на различных носителях информации (твердая копия, фотографии, электронные носители и др.).

Анализ защищенности объекта защиты информации

Шкала ценности активов

Идентификатор актива	Актив организации		Конфиденциальность	Целостность	Доступность	Ценность актива
A.	Основные активы Информация	Информация, необходимую для реализации назначения или бизнеса организации	2	4	4	**4**
B.		Информация личного характера, которая определена особым образом, соответствующим национальным законам о неприкосновенности частной жизни	3	1	1	**3**
C.		Стратегическая информация, необходимая для достижения целей организации	2	2	1	**2**
D.		Информацию, обработка которой требуют продолжительного времени и/или связаны с большими затратами на ее приобретение	3	2	2	**3**
E.	Аппаратно-программный комплекс		–	3	4	**4**
F.	Носители информации		–	1	2	**2**
G.	Сеть		–	3	4	**4**
H.	Сотрудники		–	1	1	**1**
I.	Место функционирования организации		–	1	1	**1**

Первоначально необходимо определить ценность активов (далее – ЦН) организации, в данном случае будет рассмотрена четырехбалльная система оценки ценности активов:

1 – реализация риска, направленного на конфиденциальность, целостность и/или доступность актива не будет иметь последствий, как для организации в целом, так и бизнес-процессов, в частности.

2 – реализация риска, направленного на конфиденциальность, целостность и/или доступность актива приведет к незначительным потерям для организации, в условиях, когда восстановление прежнего состояния системы возможно без остановки бизнес-процессов.

Оценка риска угроз

3 – реализация риска, направленного на конфиденциальность, целостность и/или доступность актива приведет к значительным финансовым потерям и/или окажет существенное негативное влияние на престиж организации, в условиях, когда восстановление прежнего состояния системы возможно, но требует больших временных и/или финансовых ресурсов.

4 – реализация риска, направленного на конфиденциальность, целостность и/или доступность актива может привести полной остановке бизнес-процессов, большим финансовым потерям и/или окажет значительное негативное влияние на престиж организации.

Оценка риска угроз

Таблица 2

Степень уязвимости актива

Угрозы ИБ	Ценные активы организации								
	A.	B.	C.	D.	E.	F.	G.	H.	I.
014	–	–	–	–	2	–	–	–	–
018	1	1	1	1	3	–	–	–	–
022	–	–	–	–	2	–	2	–	–
023	–	–	–	–	3	–	–	–	–
030	2	2	2	2	1	–	–	–	–
034	–	–	–	–	–	–	1	–	–
036	1	1	1	1	1	–	1	–	–
091	3	3	3	3	–	–	–	–	–
113	–	–	–	–	2	–	–	–	–

В табл. 2 представлен результат оценки уязвимости актива для перечня угроз, где 1 – низкая уязвимость по отношению конфиденциальности, целостности и/или доступности ценного актива организации, 2 – средняя степень уязвимости, а 3 – высокая степень уязвимости.

Анализ защищенности объекта защиты информации

Таблица 3

Вероятность реализации угроз

ID угрозы	014	018	022	023	030	034	036	091	113	121	122	139	140	143	155	156	157	158	160	170	172	182	186	189
Вероятность	2	1	2	3	1	2	2	4	2	2	2	3	2	2	2	4	3	3	3	2	2	3	3	2

Оценка риска угроз

Последним этапом перед расчетом рисков ИБ является оценка вероятности реализации угроз ИБ (далее – В), представленных в табл. 2. Оценка вероятности представлена в табл. 3, где 1 – угроза существует, но не встречалась в рассматриваемой сфере, 2 – угроза возникает в рассматриваемой сфере 2–3 раза в год, 3 – угроза была реализована в рассматриваемой системе, 4 – угроза возникает 2–3 раза в год в рассматриваемой системе.

Общий уровень риска ИБ для каждого из ценных активов организации рассчитывается по формуле 1, в табл. 4 представлен результат для активов A, E, G.

$$Р = ЦН \times СУ \times В \qquad (1)$$

Приемлемым риском считается риск, чье числовое значение находится в промежутке от 1 до 10, такой риск считается

Оценка риска угроз

Таблица 4

Оценка рисков ИБ

Ценный актив организации	Угрозы	ЦН	СУ	В	Р	Числовое значение оценки риска
Информация, необходимую для реализации назначения или бизнеса организации	018	4	1	1	4	Низкий
	030	4	2	1	8	Низкий
	036	4	1	2	8	Низкий
	091	4	3	4	48	Высокий
	121	4	2	2	16	Средний
	139	4	1	3	12	Средний
	143	4	3	2	24	Высокий
	155	4	1	2	8	Низкий
	156	4	3	4	48	Высокий
	158	4	1	3	12	Низкий
	160	4	1	3	12	Низкий
	170	4	2	2	16	Низкий
	186	4	2	3	24	Высокий

незначительным, и обработка такого риска не требуется.

Средний риск, чье числовое значение находится в диапазоне от 11 до 21 рекомендован к обработке с целью его минимизации. [15–16]

Высокий риск, чье числовое значение находится в диапазоне от 22 до 64, данный риск считается существенным, и его обработка обязательна.

Оценка риска угроз

Рекомендованные контрмеры

Ценный актив организации	Угрозы	Риск	Приемлемый риск	Планируемые меры	Остаточный риск
Информация, необходимую для реализации назначения или бизнеса организации	091	48	От 1 до 19	Система резервного копирования, система защиты от НСД	12
	143	24		Система антивирусной защиты, межсетевое экранирование	12
	156	48		Учет носителей информации	12
	186	24		Система антивирусной защиты, межсетевое экранирование; Организационные меры	8
Аппаратно-программный комплекс	023	36		Межсетевое экранирование, система доверенной загрузки, система антивирусной защиты; Организационные меры	12
	139	36		Системы видеонаблюдения, адекватные средства физической защиты; Организационные меры.	12
	140	24		Система межсетевого экранирования	12
	155	24		Система межсетевого экранирования	12
	160	24		Системы видеонаблюдения, адекватные средства физической защиты; Организационные меры.	8
Сеть	140	24		Система межсетевого экранирования	12
	155	24		Система межсетевого экранирования	12
	186	24		Система антивирусной защиты, межсетевое экранирование; Организационные меры	8

4. Возможные контрмеры

Допустим, что руководитель предприятия принимает решение, что риски с числовым значением выше 20 подлежат обработке с целью их минимизации. Возможные контрмеры представлены в табл. 5. [17–20]

После обработки рисков ИБ, остаточный риск стал приемлемым для каждой из актуальных угроз информационной безопасности.

Оценка риска угроз

Актуальной считается угроза, которая может быть реализована в ИСПДн и представляет опасность для ПДн.

Согласно Постановлению Правительства РФ №1119 для ИСПДн различают угрозы трех типов:

· Угрозы 1 типа - связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.

· Угрозы 2 типа - связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

· Угрозы 3 типа - не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

Контроль чётности

Составить программу, реализующую код проверки на чётность и прямоугольный код

https://bdu.fstec.ru/threat

https://fstec21.blogspot.com/2017/07/type-actual-security-threats.html