Практическая работа №5

ОБЕСПЕЧЕНИЕ КОНФИДЕНЦИАЛЬНОСТИ, ДОСТУПНОСТИ И ЦЕЛОСТНОСТИ ИНФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИОННОЙ СИСТЕМЕ

Цель работы. Изучить методику построения модели нарушителя информационной безопасности. Произвести классификацию определенного нарушителя и построить его модель.

Краткие сведения из теории

Понятия угрозы безопасности объекта и уязвимости объекта были введены ранее. Для полного представления взаимодействия угрозы и объекта защиты введем понятия источника угрозы и атаки.

Угроза безопасности объекта – возможное воздействие на объект, которое прямо или косвенно может нанести ущерб его безопасности.

Источник угрозы – это потенциальные антропогенные, техногенные или стихийные носители угрозы безопасности.

Уязвимость объекта – это присущие объекту причины, приводящие к нарушению безопасности информации на объекте.

Атака – это возможные последствия реализации угрозы при взаимодействии источника угрозы через имеющиеся уязвимости. Атака – это всегда пара «источник – уязвимость», реализующая угрозу и приводящая к ущербу.

Предположим, студент ходит на учебу каждый день и при этом пересекает проезжую часть в неположенном месте. И однажды он попадает под машину, что причиняет ему ущерб, при котором он теряет трудоспособность и не может посещать занятия. Проанализируем данную ситуацию. Последствия в данном случае – это убытки, которые студент понес в результате несчастного случая. Угрозой у нас выступает автомобиль, который сбил студента. Уязвимостью явилось то, что студент пересекал проезжую часть в неустановленном месте. А источником угрозы в данной ситуации явилась та некая сила, которая не дала возможности водителю избежать наезда на студента.

С информацией не намного сложнее. Угроз безопасности информации не так уж и много. Угроза, как следует из определения, – это опасность причинения ущерба, то есть в этом определении проявляется жесткая связь технических проблем с юридической категорией, каковой является «ущерб».

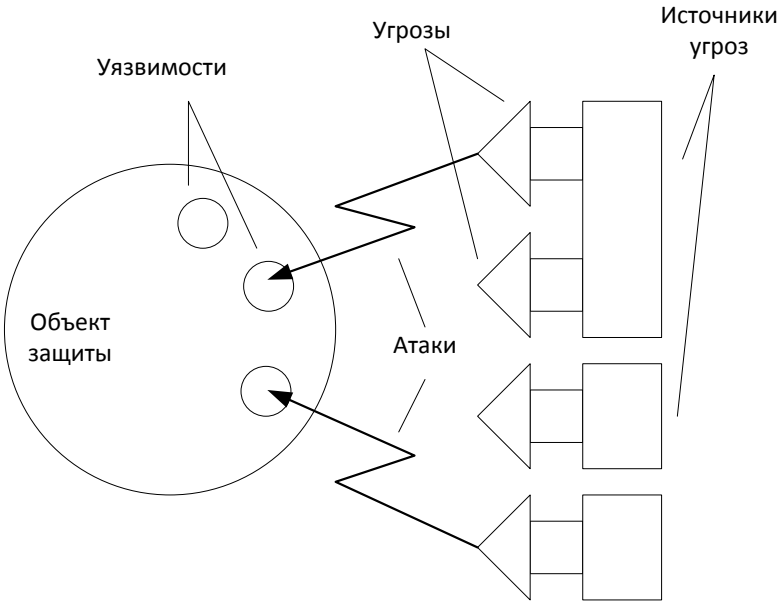

Рисунок 1 – Взаимосвязь понятий угроза, источник угрозы, уязвимость и атака

Проявления возможного ущерба могут быть различны:

– моральный и материальный ущерб деловой репутации организации;

– моральный, физический или материальный ущерб, связанный с разглашением персональных данных отдельных лиц;

– материальный (финансовый) ущерб от разглашения защищаемой (конфиденциальной) информации;

– материальный (финансовый) ущерб от необходимости восстановления нарушенных защищаемых информационных ресурсов;

– материальный ущерб (потери) от невозможности выполнения взятых на себя обязательств перед третьей стороной;

– моральный и материальный ущерб от дезорганизации деятельности организации;

– материальный и моральный ущерб от нарушения международных отношений.

Классификация угроз информационной безопасности

Угрозами безопасности информации являются нарушения при обеспечении:

1. Конфиденциальности;
2. Доступности;

3. Целостности.

Конфиденциальность информации – это свойство информации быть известной только аутентифицированным законным ее владельцам или пользователям.

Нарушения при обеспечении конфиденциальности:

– хищение (копирование) информации и средств ее обработки;

– утрата (неумышленная потеря, утечка) информации и средств ее обработки.

Доступность информации – это свойство информации быть доступной для аутентифицированных законных ее владельцев или пользователей.

Нарушения при обеспечении доступности:

– блокирование информации;

– уничтожение информации и средств ее обработки.

Целостность информации – это свойство информации быть неизменной в семантическом смысле при воздействии на нее случайных или преднамеренных искажений или разрушающих воздействий.

Нарушения при обеспечении целостности:

– модификация (искажение) информации;

– отрицание подлинности информации;

– навязывание ложной информации.

Классификация источников угроз

Носителями угроз безопасности информации являются источники угроз. В качестве источников угроз могут выступать как субъекты (личность), так и объективные проявления. Причем, источники угроз могут находиться как внутри защищаемой организации – внутренние источники, так и вне ее – внешние источники.

Все источники угроз безопасности информации можно разделить на три основные группы:

1 Обусловленные действиями субъекта (антропогенные источники угроз).

2 Обусловленные техническими средствами (техногенные источники угрозы).

3 Обусловленные стихийными источниками.

Антропогенными источниками угроз безопасности информации выступают субъекты, действия которых могут быть квалифицированы как умышленные или случайные преступления. Только в этом случае можно говорит о причинении ущерба. Эта группа наиболее обширна и представляет наибольший интерес с точки зрения организации защиты, так как действия субъекта всегда можно оценить, спрогнозировать и принять адекватные меры. Методы противодействия в этом случае управляемы и напрямую зависят от воли организаторов защиты информации.

В качестве антропогенного источника угроз можно рассматривать субъекта, имеющего доступ (санкционированный или несанкционированный) к работе со штатными средствами защищаемого объекта. Субъекты (источники), действия которых могут привести к нарушению безопасности информации, могут быть как внешние, так и внутренние. Внешние источники могут быть случайными или преднамеренными и иметь разный уровень квалификации.

Внутренние субъекты (источники), как правило, представляют собой высококвалифицированных специалистов в области разработки и эксплуатации программного обеспечения и технических средств, знакомы со спецификой решаемых задач, структурой и основными функциями и принципами работы программно-аппаратных средств защиты информации, имеют возможность использования штатного оборудования и технических средств сети.

Необходимо учитывать также, что особую группу внутренних антропогенных источников составляют лица с нарушенной психикой и специально внедренные и завербованные агенты, которые могут быть из числа основного, вспомогательного и технического персонала, а также представителей службы защиты информации. Данная группа рассматривается в составе перечисленных выше источников угроз, но методы парирования угрозам для этой группы могут иметь свои отличия.

Вторая группа содержит источники угроз, определяемые технократической деятельностью человека и развитием цивилизации. Однако последствия, вызванные такой деятельностью, вышли из-под контроля человека и существуют сами но себе. Данный класс источников угроз безопасности информации особенно актуален в современных условиях, так как в сложившихся условиях эксперты ожидают резкого роста числа техногенных катастроф, вызванных физическим и моральным устареванием используемого оборудования, а также отсутствием материальных средств на его обновление. Технические средства, являющиеся источниками потенциальных угроз безопасности информации, также могут быть внешними и внутренними.

Третья группа источников угроз объединяет обстоятельства, составляющие непреодолимую силу, то есть такие обстоятельства, которые носят объективный и абсолютный характер, распространяющийся на всех. К непреодолимой силе в законодательстве и договорной практике относят стихийные бедствия или иные обстоятельства, которые невозможно предусмотреть или предотвратить или возможно предусмотреть, но невозможно предотвратить при современном уровне человеческого знания и возможностей. Такие источники угроз совершенно не поддаются прогнозированию, и поэтому меры защиты от них должны применяться всегда.

Стихийные источники потенциальных угроз информационной без-

опасности, как правило, являются внешними по отношению к защищаемому объекту и под ними понимаются, прежде всего, природные катаклизмы.

Классификация и перечень источников угроз приведены в таблице 1.

Таблица 1 – **Классификация и перечень источников угроз информационной безопасности**

Антропогенные источники	Внешние	Криминальные структуры
		Потенциальные преступники и хакеры
		Недобросовестные партнеры
		Технический персонал поставщиков телекоммуникационных услуг
		Представители надзорных организаций и аварийных служб
		Представители силовых структур
	Внутренние	Основной персонал (пользователи, программисты, разработчики)
		Представители службы защиты информации (администраторы)
		Вспомогательный персонал (уборщики, охрана)
		Технический персонал (жизнеобеспечение, эксплуатация)
Техногенные источники	Внешние	Средства связи
		Сети инженерных коммуникации (водоснабжения, канализации)
		Транспорт
	Внутренние	Некачественные технические средства обработки информации
		Некачественные программные средства обработки информации
		Вспомогательные средства (охраны, сигнализации, телефонии)
		Другие технические средства, применяемые в учреждении
Стихийные источники	Внешние	Пожары
		Землетрясения
		Наводнения
		Ураганы
		Магнитные бури
		Радиоактивное излучение
		Различные непредвиденные обстоятельства
		Необъяснимые явления
		Другие форс-мажорные обстоятельства

Угрозы, как возможные опасности совершения какого-либо действия, направленного против объекта защиты, проявляются не сами по себе, а через уязвимости, приводящие к нарушению безопасности информации

на конкретном объекте информатизации.

Уязвимости присущи объекту информатизации, неотделимы от него и обусловливаются недостатками процесса функционирования, свойствами архитектуры автоматизированных систем, протоколами обмена и интерфейсами, применяемыми программным обеспечением и аппаратной платформой, условиями эксплуатации и расположения.

Источники угроз могут использовать уязвимости для нарушения безопасности информации, получения незаконной выгоды (нанесения ущерба собственнику, владельцу, пользователю информации). Кроме того, возможны не злонамеренные действия источников угроз по активизации тех или иных уязвимостей, наносящих вред.

Каждой угрозе могут быть сопоставлены различные уязвимости. Устранение или существенное ослабление уязвимостей влияет на возможность реализации угроз безопасности информации.

Уязвимости безопасности информации могут быть:

- объективными;
- субъективными;
- случайными.

Объективные уязвимости зависят от особенностей построения и технических характеристик оборудования, применяемого на защищаемом объекте. Полное устранение этих уязвимостей невозможно, но они могут существенно ослабляться техническими и инженерно-техническими методами парирования угроз безопасности информации.

Субъективные уязвимости зависят от действий сотрудников и, в основном устраняются организационными и программно-аппаратными методами.

Случайные уязвимости зависят от особенностей окружающей защищаемый объект среды и непредвиденных обстоятельств. Эти факторы, как правило, мало предсказуемы и их устранение возможно только при проведении комплекса организационных и инженерно-технических мероприятий по противодействию, угрозам информационной безопасности.

Классификация и перечень уязвимостей информационной безопасности приведены в таблице 2.

Таблица 2.2 – **Классификация и перечень уязвимостей информационной безопасности**

Объективные уязвимости	Сопутствующие техническим средствам излучения	Электромагнитные	Побочные излучения элементов технических средств
			Кабельных линий технических средств
			Излучения на частотах работы генераторов
			На частотах самовозбуждения усилителей
		Электрические	Наводки электромагнитных излучений на линии и проводники

			Просачивание сигналов в цепи электропитания, в цепи заземления
			Неравномерность потребления тока электропитания
		Звуковые	Акустические
			Виброакустические
	Активизируемые	Аппаратные закладки устанавливаемые	В телефонные линии
			В сети электропитания
			В помещениях
			В технических средствах
		Программные закладки	Вредоносные программы
			Технологические выходы из программ
			Нелегальные копии ПО
	Определяемые особенностями элементов	Элементы, обладающие электроакустическими преобразованиями	Телефонные аппараты
			Громкоговорители и микрофоны
			Катушки индуктивности
			Дроссели
			Трансформаторы и пр.
		Элементы, подверженные воздействию электромагнитного поля	Магнитные носители
			Микросхемы
			Нелинейные элементы, подверженные ВЧ навязыванию
	Определяемые особенностями защищаемого объекта	Местоположением объекта	Отсутствие контролируемой зоны
			Наличие прямой видимости объектов
			Удаленных и мобильных элементов объекта
			Вибрирующих отражающих поверхностей
		Организацией каналов обмена информацией	Использование радиоканалов
			Глобальных информационных сетей
			Арендуемых каналов
Субъективные уязвимости	Ошибки (халатность)	При подготовке и использовании программного обеспечения	При разработке алгоритмов и программного обеспечения
			При инсталляции и загрузке программного обеспечения
			При эксплуатации программного обеспечения
			При вводе данных (информации)
			При настройке сервисов универсальных систем
			Самообучающейся (самонастраивающейся) сложной системы систем
		При эксплуатации технических средств	При включении/выключении технических средств
			При использовании технических средств охраны

		Некомпетентные действия	При конфигурировании и управлении сложной системы
			При настройке программного обеспечения
			При организации управления потоками обмена информации
			При настройке технических средств
			При настройке штатных средств защиты программного обеспечения
		Неумышленные действия	Повреждение (удаление) программного обеспечения
			Повреждение (удаление) данных
			Повреждение (уничтожение) носителей информации
			Повреждение каналов связи
	Нарушения	Режима охраны и защиты	Доступа на объект
			Доступа к техническим средствам
			Соблюдения конфиденциальности
		Режима эксплуатации технических средств и ПО	Энергообеспечения
			Жизнеобеспечения
			Установки нештатного оборудования
			Инсталляции нештатного ПО (игрового, обучающего, технологического)
		Использования информации	Обработки и обмена информацией
			Хранения и уничтожения носителей информации
			Уничтожения производственных отходов и брака
	Психогенные	Психологические	Антагонистические отношения (зависть, озлобленность, обида)
			Неудовлетворенность своим положением
			Неудовлетворенность действиями руководства (взыскание, увольнение)
			Психологическая несовместимость
		Психические	Психические отклонения
			Стрессовые ситуации
		Физиологические	Физическое состояние (усталость, болезненное состояние)
			Психосоматическое состояние
ные уяз- вимо	бои и тказы	Отказы и неисправности технических средств	Обрабатывающих информацию
			Обеспечивающих работоспособность средств обработки информации

			Обеспечивающих охрану и контроль доступа
		Старение и размагничивание носителей информации	Дискет и съемных носителей
			Жестких дисков
			Элементов микросхем
			Кабелей и соединительных линий
		Сбои программного обеспечения	Операционных систем и СУБД
			Прикладных программ
			Сервисных программ
			Антивирусных программ
		Сбои электроснабжения	Оборудования, обрабатывающего информацию
			Обеспечивающего и вспомогательного оборудования

Оценку угроз и уязвимостей следует производить совокупно, оценивая критерии опасности угрозы и уязвимости исходя из того, что первая будет реализована через вторую. При этом следует использовать подкорректированные критерии, соответствующие указанной совокупной оценке «угроза – уязвимость»:

– критерий C_1 (от англ. *Criterion*) – возможность возникновения источника угрозы в достаточном окружении от объекта информатизации для реализации угрозы через уязвимость;

– критерий C_2 – степень готовности источника угрозы воспользоваться уязвимостью объекта информатизации и реализовать угрозу;

– критерий C_3 – распространенность уязвимости по объекту информатизации или частота ее появления;

– критерий C_4 – доступность уязвимости для реализации угрозы ее источником;

– критерий C_5 – фатальность от реализации угрозы источником угрозы через уязвимость объекта информатизации.

Все критерии оцениваются экспертами по десятибалльной шкале (дискретно от 1 до 10). Принцип выставления баллов для первых четырех критериев прост: чем в большей степени появляется критерий, тем большего балла он заслуживает. Критерии C_1 и C_2 в паре «угроза – уязвимость» в большей степени имеют отношение к угрозе, а критерии C_3 и C_4 – к уязвимости. Критерий C_5 в одинаковой степени зависит как от угрозы, так и от уязвимости, и для него целесообразно использовать более конкретизированную систему оценивания.

При оценке фатальности от реализации угрозы для объектов информатизации железнодорожного транспорта, специфика которых была указана выше, важно не только принимать во внимание нарушение информационной безопасности, но также учитывать и функциональную безопасность. Ниже представлены баллы и соответствующие им уровни нарушения безопасности объектов информатизации исходя из соображений первостепенной важности

обеспечения функциональной безопасности для объектов железнодорожного транспорта:

1 – нарушение доступности информации объекта информатизации, не приведшее к нарушению его функциональной безопасности;

2 – нарушение конфиденциальности или целостности информации объекта информатизации, не приведшее к нарушению его функциональной безопасности;

3 – нарушение конфиденциальности и целостности информации объекта информатизации, не приведшее к нарушению его функциональной безопасности;

4 – нарушение конфиденциальности, целостности и доступности информации объекта информатизации, не приведшее к нарушению его функциональной безопасности;

5 – частичное нарушение функциональной безопасности объекта информатизации;

6 – нарушение доступности информации объекта информатизации, сопровождающееся частичным нарушением его функциональной безопасности;

7 – нарушение конфиденциальности или целостности информации объекта информатизации, сопровождающееся частичным нарушением его функциональной безопасности;

8 – нарушение конфиденциальности и целостности информации объекта информатизации, сопровождающееся частичным нарушением его функциональной безопасности;

9 – нарушение конфиденциальности, целостности и доступности информации объекта информатизации, сопровождающееся частичным нарушением его функциональной безопасности;

10 – нарушение функциональной безопасности объекта информатизации – полный его выход из строя.

При таком подходе оценивается опасность реализации угрозы через уязвимость объекта информатизации. Коэффициент опасности реализации угрозы через уязвимость ($K_{\text{оп}}$) оценивается N экспертами по следующей формуле:

$$K_{\text{опугуз}N} = \frac{\sum_{i=1}^{N} C_{1i} \cdot \sum_{i=1}^{N} C_{2i} \cdot \sum_{i=1}^{N} C_{3i} \cdot \sum_{i=1}^{N} C_{4i} \cdot \sum_{i=1}^{N} C_{5i}}{(10N)^5} \qquad (1)$$

Порядок выполнения работы

1 По заданию преподавателя выбрать объект защиты.

2 Придумать несколько пар «угроза – уязвимость» для нарушения конфиденциальности, доступности и целостности информации объекта защиты и заполните таблицу 3.

Таблица 3 – **Угрозы и уязвимости информационной безопасности**

Угроза	Источник угрозы	Уязвимость	Последствия атаки
			Нарушение конфиденциальности информации объекта защиты
			Нарушение доступности информации объекта защиты
			Нарушение целостности информации объекта защиты

4 Выставить оценки по всем критериям, указанным в кратких сведениях из теории, рассчитать коэффициенты опасности пар «угроза – уязвимость» и провести их ранжирование. Ранги следует выставлять таким образом, чтобы пара «угроза – уязвимость» с самым большим коэффициентом опасности получила первый ранг, с меньшим – второй и т. д. Результаты расчетов необходимо свести в таблицу 4.

Таблица 4 – **Экспертная оценка опасности потенциальных угроз**

Пара «угроза – уязвимость»	Эксперт	Критерии оценки опасности					$K_{оп}$	Ранг
		C_1	C_2	C_3	C_4	C_5		
1	1							
	2							
	3							
	…							
	средняя оценка							
2	1							
	2							
	3							
	…							
	средняя оценка							
и т. д.								

5 Сделать выводы о наиболее опасных угрозах и уязвимостях для объекта защиты и предложить решения для обеспечения конфиденциальности, доступности и целостности информации.

Содержание отчета

1 Цель работы.
2 Перечень пар «угроза – уязвимость» (таблица 3).
3 Результаты экспертной оценки (таблица 4).

4 Вывод по работе.

Контрольные вопросы

1 Что такое угроза информационной безопасности?
2 Что такое источник угрозы?
3 Классификация источников угрозы информационной безопасности.
4 Что такое уязвимость объекта защиты?
5 Классификация уязвимостей.
6 Что такое конфиденциальность информации?
7 Что такое доступность информации?
8 Что такое целостность информации?