МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждения высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«_8_» _04_____ 2023 г.

Защищенные информационные системы

Методические указания по выполнению лабораторных работ по дисциплине «Защищенные информационные системы» для студентов направления подготовки 10.04.01 «Информационная безопасность»

Курск 2023

УДК 004.773.5

Составители: Кулешова Е.А.

Рецензент

Кандидат технических наук, доцент кафедры
вычислительной техники А.В. Киселев

Защищенные информационные системы: методические указания по выполнению лабораторных работ / Юго-Зап. гос. ун-т; сост.: Е.А. Кулешова. – Курск, 2023. – 17 с.: Библиогр.: с. 17.

Содержат сведения по вопросам изучения технологий, методов и средств создания защищенных информационных систем для успешной профессиональной деятельности, а также развития в процессе обучения системного мышления, необходимого для решения задач управления в области информационной безопасности.

Методические указания по выполнению лабораторных работ по дисциплине «Защищенные информационные системы» предназначены для студентов направления подготовки 10.04.01 «Информационная безопасность».

Текст печатается в авторской редакции
Подписано в печать . Формат 60х84 1/16.
Усл. печ.л. . Уч. –изд.л. .Тираж 50 экз. Заказ .
Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

Работа №1. Создание модели вероятного нарушителя

Цель. Создание полной характеристики потенциального нарушителя безопасности и перечня актуальных угроз безопасности для заданного объекта.

Построение модели вероятного нарушителя безопасности объекта. Под моделью нарушителя понимается совокупность количественных и качественных характеристик нарушителя, с учетом которых определяются требования к комплексу инженерно-технических средств охраны и/или его составным частям.

1. Составить список внешних и внутренних нарушителей безопасности заданного объекта. Проанализировать следующие характеристики, присущие нарушителям, заполнить таблицу 1.

Таблица 1 - Характеристики нарушителя

Признак характеристики нарушителя	Характеристика
1	2
Цели и задачи	проникновение на охраняемый объект без причинения объекту видимого ущерба
	причинение ущерба объекту
	преднамеренное проникновение при отсутствии враждебных намерений
	случайное проникновение
	Дополнить
Степень принадлежности вероятного нарушителя к объекту	сотрудник охраны
	сотрудник учреждения
	посетитель
	постороннее лицо
	Дополнить

Продолжение таблицы 1

1	2
Степень осведомленности вероятного нарушителя об объекте	детальное знание объекта
	осведомленность о назначении объекта, его внешних признаках и чертах
	неосведомленный вероятный нарушитель
Степень осведомленности нарушителя о системе охраны объекта	полная информация о системе охраны объекта
	информация о системе охраны вообще и о системе охраны конкретного объекта охраны
	информация о системе охраны вообще, но не о системе охраны конкретного объекта
	неосведомленный вероятный нарушитель
Степень профессиональной подготовленности вероятного нарушителя	специальная подготовка по преодолению систем охраны
	не имеет специальной подготовки по преодолению систем охраны
Степень физической подготовленности вероятного нарушителя	специальная физическая подготовка
	низкая физическая подготовка
Владение вероятным нарушителем способами маскировки	владеет
	не владеет
Степень технической оснащенности вероятного нарушителя	высокая
	средняя
	низкая
Способ проникновения вероятного нарушителя на объект	взлом замка
	проход по поддельным документам
	Дополнить

2. Определить категорию нарушителя.

Модель (образ) нарушителя представляет собой его комплексную характеристику, отражающую его возможное психологическое состояние, уровень физической и технической подготовленности, осведомленности, которая позволяет оценить степень его способности в практической реализации проникновения.

Характеристики нарушителя учитываются при определении требований к комплексу инженерно-технических средств охраны и/или его составным частям.

Составляющие модели нарушителя:

- категории нарушителя и его возможные тактические методы

(внешние, внутренние, внешние в сговоре с внутренними);

- возможные действия нарушителя (применение силы, хищение, дезинформация и т.д.);
- причины и мотивы действий нарушителя;
- возможности нарушителя (навык, опыт, количество, оснащенность-техника, оружие, транспорт).

Для описания моделей нарушителей в качестве критериев классификации рассматриваются следующие критерии.

1 Цели и задачи вероятного нарушителя:

- проникновение на охраняемый объект без причинения объекту видимого ущерба;
- причинение ущерба объекту;
- преднамеренное проникновение при отсутствии враждебных намерений;
- случайное проникновение.

2 Степень принадлежности вероятного нарушителя к объекту:

- вероятный нарушитель - сотрудник охраны;
- вероятный нарушитель - сотрудник учреждения;
- вероятный нарушитель - посетитель;
- вероятный нарушитель - постороннее лицо.

3 Степень осведомленности вероятного нарушителя об объекте:

- детальное знание объекта;
- осведомленность о назначении объекта, его внешних признаках;
- неосведомленный вероятный нарушитель.

4 Степень осведомленности нарушителя о системе охраны объекта:

- полная информация о системе охраны объекта;
- информация о системе охраны вообще и о системе охраны конкретного объекта охраны;
- информация о системе охраны вообще, но не о системе охраны

конкретного объекта;

- неосведомленный вероятный нарушитель.

5 Степень профессиональной подготовленности вероятного нарушителя:

- специальная подготовка по преодолению систем охраны;
- вероятный нарушитель не имеет специальной подготовки по преодолению систем охраны.

6 Степень физической подготовленности вероятного нарушителя:

- специальная физическая подготовка;
- низкая физическая подготовка.

7 Владение вероятным нарушителем различными способами маскировки.

8 Степень технической оснащенности вероятного нарушителя.

9 Способ проникновения вероятного нарушителя на объект.

При анализе безопасности информационной системы можно выделить обычно четыре основные категории нарушителей:

1. нарушитель первой категории - специально подготовленный по широкой программе, имеющий достаточный опыт нарушитель-профессионал с враждебными намерениями, обладающий специальными знаниями и средствами для преодоления различных систем защиты объектов;
2. нарушитель второй категории - непрофессиональный нарушитель с враждебными намерениями, действующий под руководством другого субъекта, имеющий определенную подготовку для проникновения на конкретный объект;
3. нарушитель третьей категории - нарушитель без враждебных намерений, совершающий нарушение безопасности объекта из любопытства или из каких-то иных личных намерений;
4. нарушитель четвертой категории - нарушитель без враждебных намерений, случайно нарушающий безопасность объекта.

3. Построить неформализованную модель нарушителя безопасности в соответствии с таблицей 2.

Таблица 2 - Типовая модель нарушителя

Тип нарушителя	Категория	Подготовленность нарушителя								
		Психофизическая			Техническая			Осведомленность		
		В	С	Н	В	С	Н	В	С	Н
Внутренние	Сотрудники, имеющие санкционированный доступ к материальным ценностям		+			+		+		
	Сотрудники, имеющие доступ к финансовым ценностям		+			+		+		
	Сотрудники, имеющие доступ к служебной информации	+			+			+		
	Сотрудники, имеющие доступ к элементам системы защиты		+			+			+	
	Обслуживающий персонал (охрана, инженерно-технические службы)			+		+			+	
Внешние	Уполномоченный персонал разработчиков, который имеет право на техническое обслуживание	+			+			+		
	Уволенный сотрудник		+			+			+	
	Недобросовестные партнеры		+			+			+	
	Конкуренты		+				+		+	
	Посетители			+			+			+

В – высокая, С – средняя, Н – низкая

Контрольные вопросы

1. Что подразумевается под моделью вероятного нарушителя?
2. Какие основные шаги следует выполнить при создании модели вероятного нарушителя?
3. Какие факторы нужно учитывать при определении профиля

вероятного нарушителя?

4. Какие методы и инструменты используются для сбора информации о вероятных нарушителях?

5. Что такое анализ угроз и как он связан с созданием модели вероятного нарушителя?

6. Какие типы данных используются при создании модели вероятного нарушителя?

7. Какие методы статистического анализа могут быть применены для моделирования вероятного нарушителя?

8. Каким образом можно оценить эффективность модели вероятного нарушителя?

9. Какие преимущества может предоставить модель вероятного нарушителя в рамках кибербезопасности?

10. Какие ограничения или вызовы могут возникнуть при создании модели вероятного нарушителя?

Работа №2. Составление модели угроз безопасности информационной системы

Анализ угроз безопасности включает:

- описание угроз;
- оценку вероятности возникновения угроз;
- оценку реализуемости угроз;
- оценку опасности угроз;
- определение актуальности угроз.

1. Составить список всех возможных угроз физической безопасности для заданного объекта. При этом использовать перечень угроз, данный в таблице 1.

Таблица 1 - Основные угрозы физической безопасности

Угроза	Тип источника угроз
1	2
Несанкционированное проникновение в КЗ	Антропогенный
Совершение диверсии в КЗ	Антропогенный
Совершение террористических актов	Антропогенный
Несанкционированные действия, приводящие к нарушению производственных технологических процессов	Антропогенный
Несанкционированный доступ к компьютерам	Антропогенный
Кража технических средств с хранящейся в них информацией	Антропогенный
Кража носителей информации	Антропогенный
Кража материальных и финансовых ценностей	Антропогенный
Просмотр информации с экранов дисплеев и других средств ее отображения, бумажных и иных носителей информации, в том числе с помощью оптических средств	Антропогенный
Прослушивание телефонных и радиопереговоров	Антропогенный
Внедрение «закладок»	Антропогенный
Воздействие на технические средства в целях нарушения их работоспособности	Техногенный
Воздействие на программные средства информационных систем в целях нарушения конфиденциальности, целостности и доступности информации	Техногенный
Воздействие на средства защиты информации	Техногенный

Продолжение таблицы 1

1	2
Побочные электромагнитные излучения информативного сигнала от технических средств, обрабатывающих конфиденциальную информацию, и линий передачи этой информации	Техногенный
Наводки информативного сигнала, обрабатываемого техническими средствами, на цепи электропитания и линии связи, выходящие за пределы КЗ	Техногенный
Радиоизлучения, модулированные информативным сигналом, возникающие при работе различных генераторов, входящих в состав технических средств, при наличии паразитной генерации в узлах технических средств	Техногенный
Радиоизлучения или электрические сигналы от внедренных в технические средства и защищаемые помещения специальных электронных устройств перехвата речевой информации "закладок", модулированные информативным сигналом	Техногенный
Радиоизлучения или электрические сигналы от электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки информации	Техногенный
Угроза пожара	Стихийный
Угроза наводнения	Стихийный
Отказы и сбои в работе инженерно-технических средств охраны	Техногенный
Отказы и сбои в работе системы электроснабжения	Техногенный
Незапланированная потеря каналов связи, невозможность управления системой ОПС и видеонаблюдения на объектах с пульта централизованного наблюдения	Техногенный
выход из строя системы видеонаблюдения	Техногенный
выход из строя СКУД	Техногенный
Непреднамеренные (ошибочные, случайные, без корыстных целей) нарушения установленных требований при работе с материальными ценностями, финансовыми ресурсами, информацией, приводящие к непроизводительным затратам ресурсов, утратам и хищениям	Антропогенный
Преднамеренные (в корыстных целях, по принуждению, со злым умыслом, т.п.) действия сотрудников, допущенных к материальным, финансовым и информационным ресурсам, приводящие к непроизводительным затратам ресурсов, утратам и хищениям	Антропогенный

2. Вычислить все необходимые показатели угроз.

Для построения модели угроз безопасности можно применить руководящие документы ФСТЭК, разработанные для защиты персональных данных. Под частотой (вероятностью) реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности для данной организации в складывающихся условиях обстановки. Частота реализации угроз безопасности определяется экспертным методом в соответствии с и на основании результатов обследования объекта.

Оценка вероятности реализации угрозы (Y2) определяется по четырем вербальным градациям:

- маловероятно - отсутствуют объективные предпосылки для осуществления угрозы (0);
- низкая вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (2);
- средняя вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности недостаточны (5);
- высокая вероятность - объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности не приняты (10).

С учетом изложенного коэффициент реализуемости угрозы Y будет определяться соотношением

$$Y = (Y_i + Y_2) / 20 .$$

По значению коэффициента реализуемости угрозы Y формируется вербальная интерпретация реализуемости угрозы следующим образом:

- если $0 < Y < 0{,}3$, то возможность реализации угрозы признается низкой;
- если $0{,}3 < Y < 0{,}6$, то возможность реализации угрозы средняя;
- если $0{,}6 < Y < 0{,}8$, то возможность реализации угрозы высокая;
- если $Y > 0{,}8$, то возможность реализации угрозы очень высокая.

Определение опасности угроз проводится экспертным методом с учетом

результатов обследования объекта. Y1=5 для среднего уровня исходной защищенности.

Показателем опасности, имеет три значения:

- низкая опасность - если реализация угрозы может привести к незначительным негативным последствиям;

- средняя опасность - если реализация угрозы может привести к негативным последствиям;

- высокая опасность - если реализация угрозы может привести к значительным негативным последствиям.

Определение актуальных угроз безопасности.

Актуальная угроза - угроза, которая может быть реализована и представляет опасность. Правила определения актуальности УБСКХ приведены в таблице 2.

Таблица 2 - Правила определения актуальности угроз

Возможность реализации угрозы	Показатель опасности угрозы		
	Низкая	Средняя	Высокая
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

3. Построить модель угроз по примеру таблицы 3.

Таблица 3 - Модель угроз безопасности защищаемого объекта

Угроза	Вероятность реализаци и угрозы	Возможность реализации угрозы	Показатель опасности угрозы	Актуальность угрозы
Несанкционированный доступ к компьютерам	Маловеро-ятно (0)	0,25 (низкая)	Низкая опасность	Неактуальная
Кража технических средств с хранящейся в них информацией	Маловеро-ятно (0)	0,25 (низкая)	Низкая опасность	Неактуальная
Кража носителей информации	Маловеро-ятно (0)	0,25 (низкая)	Низкая опасность	Неактуальн ая
Кража материальных и финансовых ценностей	Средняя вероятность (5)	0,5 (средняя)	Высокая	Актуальная
Просмотр информации с экранов дисплеев и других средств ее отображения, бумажных и иных носителей	Средняя вероятность (5)	0, 6 (средняя)	Высокая	Актуальная
Прослушивание телефонных и радиопереговоров	Средняя вероят-ность(5)	0,5 (средняя)	Высокая	Актуальная
Внедрение «закладок»	Маловеро-ятно (0)	0,25 (низкая)	Низкая опасность	Неактуальная

Выписать из таблицы только актуальные угрозы безопасности.

Контрольные вопросы

1 Что подразумевается под моделью угроз безопасности информационной системы?

2 Какие основные шаги следует выполнить при составлении модели угроз безопасности информационной системы?

3 Какие типы угроз могут быть учтены при составлении модели?

4 Каким образом проводится идентификация и анализ потенциальных угроз безопасности информационной системы?

5 Какие методы и инструменты используются при составлении модели угроз безопасности информационной системы?

6 Каким образом определяются вероятность и воздействие угроз в модели безопасности информационной системы?

7 Какие факторы нужно учитывать при оценке рисков и последствий угроз безопасности информационной системы?

8 Каким образом составленная модель угроз может быть использована для планирования мер по обеспечению безопасности информационной системы?

9 Какая роль имеет обновление и поддержка модели угроз в процессе обеспечения безопасности информационной системы?

10 Какие вызовы могут возникнуть при составлении и использовании модели угроз безопасности информационной системы?

Работа №3. Обзор руководящих документов Федеральной службы технического и экспортного контроля (ФСТЭК России)

Цель. Изучение руководящих документов Федеральной службы технического и экспортного контроля (ФСТЭК России).

Изучите руководящие документы Федеральной службы технического и экспортного контроля (ФСТЭК России) и подготовьте краткий обзор, в котором вы опишете основные принципы и нормативные требования, предусмотренные этими документами. Ваш обзор должен включать следующие пункты:

1. Общая информация о ФСТЭК России: цели, задачи, компетенция.

2. Описание руководящих документов ФСТЭК России: указать наиболее важные документы, их назначение и сферу применения.

3. Основные принципы и положения, установленные руководящими документами: например, требования к защите информации, стандарты безопасности, процедуры сертификации и аккредитации.

4. Примеры практического применения руководящих документов: описать случаи, когда эти документы были использованы для обеспечения безопасности информационных систем или защиты конфиденциальной информации.

Обзор должен быть структурированным, содержательным и информативным. Используйте доступные ресурсы https://fstec.ru/ для изучения документов ФСТЭК России и анализа их содержания. Представьте ваш обзор в форме письменного доклада, применяя четкое изложение и академический стиль написания.

Контрольные вопросы

1. Какая организация разрабатывает руководящие документы в области технического и экспортного контроля в России?

2. Какие основные задачи выполняет Федеральная служба технического и экспортного контроля (ФСТЭК России)?

3. Что такое лицензирование при экспорте технических средств и информационных материалов?

4. Какие руководящие документы ФСТЭК России относятся к требованиям информационной безопасности?

5. Упомяните некоторые из руководящих документов ФСТЭК России, относящихся к классификации информации.

6. Что представляет собой документ "Правила защиты информации" (ПЗИ)?

7. Каким образом ФСТЭК России регулирует использование шифровальных (криптографических) средств?

8. Какие требования к защите информации устанавливаются в документе "Основные положения по обеспечению безопасности информации" (ОПБИ)?

9. Что такое сертификация средств защиты информации и какую роль в этом процессе играет ФСТЭК России?

10. Какие основные изменения были внесены в руководящие документы ФСТЭК России за последний год (последние известные изменения на момент 2021 года)?

Перечень литературы

1. Технологии обеспечения безопасности информационных систем : учебное пособие / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов [и др.]. – Москва ; Берлин : Директ-Медиа, 2021. – 210 с. – URL: https://biblioclub.ru/index.php?page=book&id=598988 (дата обращения: 22.05.2023). – Режим доступа: по подписке. – Текст : электронный.

2. Марухленко, А. Л. Разработка защищённых интерфейсов Web-приложений : учебное пособие / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов. – Москва ; Берлин : Директ-Медиа, 2021. – 175 с. – URL: https://biblioclub.ru/index.php?page=book&id=599050 (дата обращения: 22.05.2023). – Режим доступа: по подписке. – Текст : электронный.

3. Кобылянский, В. Г. Операционные системы, среды и оболочки : учебное пособие / В. Г. Кобылянский. – Новосибирск : Новосибирский государственный технический университет, 2018. – 80 с. – URL: https://biblioclub.ru/index.php?page=book&id=576354 (дата обращения: 22.05.2023). – Режим доступа: по подписке. – Текст : электронный.

4.Основы администрирования информационных систем : учебное пособие / Д. О. Бобынцев, А. Л. Марухленко, Л. О. Марухленко [и др.]. – Москва ; Берлин : Директ-Медиа, 2021. – 202 с. – URL: https://biblioclub.ru/index.php?page=book&id=598955 (дата обращения: 22.05.2023). – Режим доступа: по подписке. – Текст : электронный.

5.Ищейнов, В. Я. Информационная безопасность и защита информации : теория и практика : учебное пособие / В. Я. Ищейнов. – Москва ; Берлин : Директ-Медиа, 2020. – 271 с. – URL: https://biblioclub.ru/index.php?page=book&id=571485 (дата обращения: 22.05.2023). – Режим доступа: по подписке. – Текст : электронный.