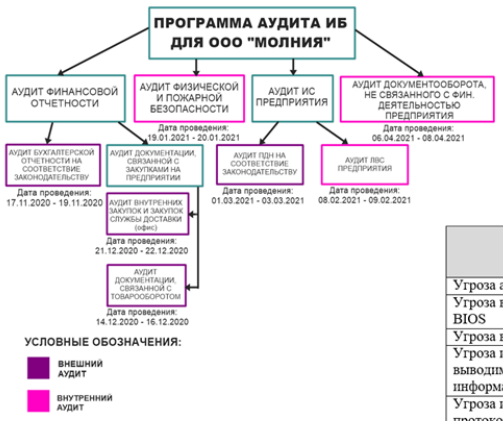
УНИВЕРСИТЕТ ИТМО

И.И. Лившиц

НОРМАТИВНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

	Поток A	Поток B	Поток C	Поток D	Поток E	Поток F
Конфиденциальность	4	2	4	4	3	5
Целостность	1	1	2	2	1	1
Доступность	2	4	2	3	2	4



Наименование характеристики	Значение
Категория обрабатываемых ПДн	Иные
Обрабатываемые ПДн	Сотрудники РГ
Объем обрабатываемых ПДн	Менее 100 000
Угрозы, актуальные для информационной системы	Угрозы 3 типа
Актуальные нарушители ИБ	В качестве **нарушителей** рассматриваются нарушители: – недобросовестные партнеры (1); – бывшие сотрудники (2); – пользователи информационной инфраструктуры (3). – разработчики ПО (4); – обслуживающий персонал (5); – администраторы ИСПДн РГ (6); – взломщики программного обеспечения и информационных систем (7)

№	Обобщенные возможности источников атак	Да/нет
1	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны	Да
2	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны, но без физического доступа к аппаратным средствам (далее – АС), на которых реализованы СКЗИ и среда их функционирования	нет
3	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны с физическим доступом к АС, на которых реализованы СКЗИ и среда их функционирования	нет
4	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области анализа сигналов линейной передачи и сигналов побочного электромагнитного излучения и наводок СКЗИ)	нет
5	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей прикладного программного обеспечения)	нет
6	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей аппаратного и программного компонентов среды функционирования СКЗИ)	нет

Риск	Последствия (1-5)	Вероятность (1-5)	Управляемость (1-5)	Индекс риска (П*В*У)
Угроза аппаратного сброса пароля BIOS	2	2	3	12
Угроза внедрения вредоносного кода в BIOS	1	1	2	2
Угроза внедрения кода или данных	3	2	2	12
Угроза искажения вводимой и выводимой на периферийные устройства информации	2	2	2	8
Угроза использования слабостей протоколов сетевого/локального обмена данными	3	3	2	18
Угроза некорректного использования функционала программного и аппаратного обеспечения	4	4	3	48
Угроза неправомерного ознакомления с защищаемой информацией	5	3	3	45
Угроза несанкционированного доступа к виртуальным каналам передачи	2	2	3	12
Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети	3	3	2	18

Санкт-Петербург
2021

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

УНИВЕРСИТЕТ ИТМО

И.И. Лившиц

НОРМАТИВНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

УЧЕБНО-МЕТОДИЧЕСКОЕ ПОСОБИЕ

РЕКОМЕНДОВАНО К ИСПОЛЬЗОВАНИЮ В УНИВЕРСИТЕТЕ ИТМО
по направлению подготовки 10.04.01 Информационная безопасность
в качестве Учебно-методическое пособие для реализации основных профессиональных образовательных программ высшего образования магистратуры

УНИВЕРСИТЕТ ИТМО

Санкт-Петербург
2021

Лившиц И.И., Нормативно-методическое обеспечение информационной безопасности – СПб: Университет ИТМО, 2021. – 68 с.

Рецензент(ы):
Комаров Игорь Иванович, кандидат физико-математических наук, доцент, заведующий лабораторией лаборатории валидации программного обеспечения, Университета ИТМО.

УНИВЕРСИТЕТ ИТМО

Университет ИТМО – ведущий вуз России в области информационных и фотонных технологий, один из немногих российских вузов, получивших в 2009 году статус национального исследовательского университета. С 2013 года Университет ИТМО – участник программы повышения конкурентоспособности российских университетов среди ведущих мировых научно-образовательных центров, известной как проект «5 в 100». Цель Университета ИТМО – становление исследовательского университета мирового уровня, предпринимательского по типу, ориентированного на интернационализацию всех направлений деятельности.

Аннотация

Учебно-методическое пособие «Нормативно-методическое обеспечение информационной безопасности» предназначено для помощи обучающимся по направлению подготовки 10.04.01 «Информационная безопасность» (магистратура). Пособие содержит полный набор лабораторных работ с соответствующей краткой теоретической частью, примерами заполнения, а также с описанием различных ошибок, которые могут встретиться обучающимся при самостоятельном выполнении.

Каждая лабораторная работа оформлена как единый учебный блок, содержит собственную постановку задачи, описание хода вывода, отдельные промежуточные результаты и общий вывод по итогам работы. Для удобства восприятия информации применяются табличные формы и рисунки, поясняющие ход выполнения каждой лабораторной работы.

В приложении приведены дополнительные материалы (нормативные документы Федеральной службы по техническому и экспертному контролю (ФСТЭК России) и Федеральной службы безопасности (ФСБ России), национальные ГОСТ Р и международные стандарты ISO, ISO/IEC). Эти дополнительные материалы могут быть изучены как в рамках курса «Нормативно-методическое обеспечение информационной безопасности», так и в качестве дополнительных материалов при самообучении.

Рекомендуется выполнение лабораторных работ в последовательности их изложения в данном учебно-методическом пособии, поскольку этот порядок соответствует логике изложения материалов соответствующего теоретического курса и помогает обеспечить системный и гибкий подход при изучении материалов курса и самостоятельной работы.

Содержание

Ведение

Учебно-методическое пособие «Нормативно-методическое обеспечение информационной безопасности» предназначено для помощи обучающимся по направлению подготовки 10.04.01 «Информационная безопасность» (магистратура). Актуальность данного пособия определяется постоянным ростом числа инцидентов информационной безопасности (ИБ) и усилением их критических воздействий как в Российской Федерации, так и в мире. В настоящее время в высшей школе уделяется недостаточно внимания практическим аспектам подготовки магистрантов по направлению 10.04.01, что может иметь определенные негативные последствия в дальнейшем. Новизна данного пособия определяется применением актуальных нормативно-методических документов ФСТЭК России и ФСБ России, а также применимых национальных (ГОСТ Р) и международных (ISO, ISO/IEC) стандартов.

Содержание данного пособия полностью соответствует установленным учебным задачам и рабочей программе по дисциплине М.1.4.3 «Нормативно-методическое обеспечение информационной безопасности». Применение в учебном процессе данного пособия обеспечит достижение планируемых результатов обучения, в частности: знания существующей нормативно-методической базы в области ИБ и умения формировать требования к объектам информационных технологий с учетом требований нормативно-методических документов (НМД) в области ИБ (ПК-3); знания принципов выбора требований НМД в области управления ИБ и владения навыками организации комплекса различных составляющих эффективной системы ИБ (ПК-12), знания состава, структуры и назначения НМД ФСТЭК России и умения оценивать полноту реализации в продуктах информационных технологий требований НМД в области ИБ (ПСК-2).

Пособие содержит набор лабораторных работ с соответствующей собственной теоретической частью, примерами заполнения, а также с описанием различных ошибок, которые могут встретиться обучающимся при самостоятельном выполнении. Каждая лабораторная работа оформлена как единый учебный блок, содержит собственную постановку задачи, описание хода вывода, отдельные промежуточные результаты и общий вывод по итогам работы. Для удобства восприятия информации применяются табличные формы и рисунки, поясняющие ход выполнения каждой лабораторной работы.

В пособии приведены основные источники, в том числе список рекомендуемой литературы и дополнительные НМД. Список рекомендуемой литературы соответствует теоретическому курсу «Нормативно-методическое обеспечение информационной безопасности» и включает актуальные статьи на русском и английских языках, опубликованные в журналах ВАК и/или Scopus /

Web Of Science. В приложении приведены дополнительные материалы (НМД ФСТЭК России и ФСБ России, национальные ГОСТ Р и международные стандарты ISO, ISO/IEC). Эти дополнительные материалы могут быть изучены как в рамках курса «Нормативно методическое обеспечение информационной безопасности», так и в качестве дополнительных материалов при самообучении.

Пособие предусматривает возможность проверки и самопроверки результатов выполнения лабораторных работ, как полностью всего набора по курсу, так и отдельных работ. Кроме того, пособие позволяет выполнять внешний контроль знаний, как в рамках периодической оценки знаний обучающихся, так и в качестве контроля со стороны внешних экспертов. Важным отличительным свойством данного пособия является «трассируемость» всех лабораторных работ к соответствующим актуальным НМД, соответственно, может быть установлена взаимосвязь при изучении отдельных разделов и/или при внесении новых изменений в действующую редакцию каждого упомянутого ссылочного НМД. Кроме того, применяемая логика выполнения лабораторных работ позволяет перейти к другим разделам блока «Технологическая канва формирования нормативно-методического обеспечения информационной безопасности», например: требования, применительно к управлению инцидентами ИБ, управлению рисками ИБ, управлению активами, обеспечению соответствия (*Compliance*) и пр.

Рекомендуется выполнение лабораторных работ в последовательности их изложения в данном учебно-методическом пособии, поскольку этот порядок соответствует логике изложения материалов соответствующего теоретического курса и помогает обеспечить системный и гибкий подход при изучении материалов курса и некоторых смежных вопросов по направлению подготовки 10.04.01 «Информационная безопасность».

Термины и определения

ГОСТ	–	Государственный стандарт
ГОСТ Р		Государственный стандарт России
ИБ	–	Информационная безопасность
ИСПДн		Информационная система персональных данных
КЗ	–	Контролируемая зона
НМД	–	Нормативно-методический документ
НДВ	–	Недекларируемые возможности
ПДн	–	Персональные данные
ПО	–	Программное обеспечение
ПЭМИН		Побочные электромагнитные излучения и наводки
СКЗИ	–	Средство криптографической защиты информации
СМИБ	–	Система менеджмента информационной безопасности
УБИ	–	Угрозы безопасности информации
ФСБ России	–	Федеральной службы безопасности
ФСТЭК России		Федеральная служба по техническому и экспертному контролю
ISO (ИСО)	–	International Organization for Standardization (Международная организация по стандартизации)
IEC (МЭК)	–	International Electrotechnical Committee (Международная электротехническая комиссия)

Основная часть

1 Лабораторная работа № 1. «Определение уровня защищенности персональных данных и класса СКЗИ для обеспечения безопасности персональных данных»

1.1 Цель работы

Освоение навыков применения НМД по защите персональных данных (ПДн) для определения уровня защищенности ПДн, обрабатываемых в информационной системе персональных данных (ИСПДн), и класса средств криптографической защиты информации (СКЗИ).

1.2 Задачи

В Лабораторной работе №1 установлены следующие задачи:

Задача 1: Ознакомление с:

- Приказом ФСБ России от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности») [1];
- Постановлением Правительства Российской Федерации «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» № 1119 от 01 ноября 2012) [2].

Задача 2: Определение уровня защищенности ПДн и класса СКЗИ для информационной системы с исходными данными [3;4].

1.3 Ход работы

1. Обследование объекта защиты
2. Сбор и анализ исходных данных

Пример сбора исходных данных:

- 3 филиала по 10 АРМ.
- У каждого филиала есть 1 руководитель с 1 АРМ.
- Сервер обработки ПДн находится в 1 филиале (ул. Московская д.1).
- Руководитель предприятия находится в 1 филиале (ул. Ленинградская д.1).
- Управление ИБ проводится в 1 филиале (ул. Московская д.1).
- В 3-х филиалах выход в сеть Интернет.

Пример анализа исходных данных:

- Защите подлежат ПДн, обрабатываемые в ИСПДн «Альфа».
- В ИСПДн «Альфа» осуществляется обработка иных категорий ПДн, доступ к которым имеется у ограниченного круга лиц, подключаемых в соответствии с порядком, установленным внутренними НМД.
- В ИСПДн «Альфа» обрабатываются ПДн сотрудников всех 3-х филиалов (менее 100 000 субъектов ПДн).

Основные характеристики ИСПДн «Альфа» представлены в Таблице 1.

Таблица 1. Основные характеристики ИСПДн «Альфа»

Наименование характеристики	**Значение**
Категория обрабатываемых ПДн	Иные
Обрабатываемые ПДн	Сотрудники
Объем обрабатываемых ПДн	Менее 100 000
Угрозы, актуальные для информационной системы	Угрозы 3 типа
Актуальные нарушители ИБ	В качестве нарушителей рассматриваются нарушители: – недобросовестные партнеры (1); – бывшие сотрудники (2); – пользователи информационной инфраструктуры (3). – разработчики ПО (4); – обслуживающий персонал (5); – администраторы ИСПДн «Альфа» (6); – взломщики ПО и информационных систем (7)

3. Определение перечня угроз

Определение перечня угроз ИБ производится в соответствии с «Базовой моделью угроз безопасности ПДн», изданной ФСТЭК России. Перечень возможных угроз безопасности информации, обрабатываемой в ИСПДн «Альфа», и соотнесение угрозы ИБ с возможными нарушителями приведены в Таблице 2.

Таблица 2. Перечень угроз ИБ и возможность реализации угрозы ИБ нарушителем

№ УБИ в БДУ	Угроза безопасности информации	Нарушитель ИБ
-	Угроза утечки информации по визуально-оптическому каналу	1,3,6
-	Угроза утечки информации по каналу ПЭМИН	6,7
004	Угроза аппаратного сброса пароля BIOS	3,6
005	Угроза внедрения вредоносного кода в BIOS	6
006	Угроза внедрения кода или данных	1,4,6
018	Угроза загрузки нештатной операционной системы	3,6
024	Угроза изменения режимов работы аппаратных элементов компьютера	4,6
027	Угроза искажения вводимой и выводимой на периферийные устройства информации	4,6
034	Угроза использования слабостей протоколов сетевого/локального обмена данными	4,6,7
063	Угроза некорректного использования функционала программного и аппаратного обеспечения	3,4,6
067	Угроза неправомерного ознакомления с защищаемой информацией	1,5,6
074	Угроза несанкционированного доступа к аутентификационной информации	1,2,3,4,5,6,7
075	Угроза несанкционированного доступа к виртуальным каналам передачи	3,6
076	Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети	1,4,6
077	Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение	4,6
098	Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб	3,6,7
099	Угроза обнаружения хостов	3,6,7
104	Угроза определения топологии вычислительной сети	3,6,7
113	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники	3,6
115	Угроза перехвата вводимой и выводимой на	3,6

№ УБИ в БДУ	Угроза безопасности информации	Нарушитель ИБ
	периферийные устройства информации	
116	Угроза перехвата данных, передаваемых по вычислительной сети	3,6,7
123	Угроза подбора пароля BIOS	3,6
139	Угроза преодоления физической защиты	1,2,3,4,5,6,7
152	Угроза удаления аутентификационной информации	4,6
157	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	1,5,6
158	Угроза форматирования носителей информации	3,4,6
193	Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика	1,4,6
193	Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика	4,6,7

4. Определение актуальных нарушителей

В соответствии с разработанной моделью нарушителя для ИСПДн «Альфа» актуальными нарушителями являются:

- пользователи информационной инфраструктуры (3).
- разработчики ПО (4);
- администраторы (6);
- взломщики программного обеспечения и информационных систем (7).

5. Определение актуальных угроз

В обследуемой ИСПДн «Альфа» обрабатываются иные ПНд лиц, являющихся сотрудниками, в количестве до 5 000 человек.

Согласно перечню угроз, описанному в постановлении Правительства от 1 ноября 2012 г. N 1119, пункт 6, актуальными являются угрозы 3-го типа: актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей (НДВ) в системном и прикладном программном обеспечении, используемом в информационной системе.

Угрозы, связанные с наличием НДВ в системном и прикладном ПО, признаются неактуальными в связи с:

- использованием лицензионного, постоянно обновляемого системного и прикладного ПО известных мировых и российских производителей;

- заключением договоров на разработку и/или модернизацию используемого прикладного ПО, содержащих четкие требования к его функциональности, предусматривающих ответственность разработчика за несоблюдение условий договора;
- заключением соглашений о конфиденциальности с разработчиками, предусматривающих ответственность за несанкционированное разглашение конфиденциальной информации;
- превышением стоимости защиты от данных типов угроз стоимости защищаемой информации.

6. Определение уровня защищенности

В свою очередь подпункт б пункта 12 постановления Правительства от 1 ноября 2012 г. N 1119 гласит, что обеспечение 4-го уровня защищенности ПДн при их обработке в информационной системе устанавливается при наличии для информационной системы актуальных угроз 3-го типа и если информационная система обрабатывает иные категории ПДн сотрудников оператора или иные категории ПДн менее 100 000 субъектов ПДн, не являющихся сотрудниками оператора. Соответственно, можно прийти к выводу, что рассматриваемая ИСПДн «Альфа» относятся к 4 уровню защищенности.

7. Определение обобщенных возможностей злоумышленника

На основании исходных данных об информационных системах, объектах защиты и источниках выявлены обобщенные возможности злоумышленника, представленные в Таблице 4 (основано на приказе ФСБ России №378).

Таблица 4. Обобщенные возможности источников атак

№	Обобщенные возможности источников атак	Да/нет
1	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны	Да
2	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны, но без физического доступа к аппаратным средствам (далее – АС), на которых реализованы СКЗИ и среда их функционирования	нет
3	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны с физическим доступом к АС, на которых реализованы СКЗИ и среда их функционирования	нет
4	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области анализа сигналов	нет

№	Обобщенные возможности источников атак	Да/нет
	линейной передачи и сигналов побочного электромагнитного излучения и наводок СКЗИ)	
5	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей прикладного программного обеспечения)	нет
6	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей аппаратного и программного компонентов среды функционирования СКЗИ)	нет

8. Определение способов получения исходных данных

Исходя из полученных положительных ответов в Таблице 4 и полученных на этапе обследования ИСПДн «Альфа» сведений, злоумышленником могут быть использованы способы получения исходных данных при создании способов, подготовке и проведении атак, представленные в Таблице 5.

В соответствии с Методическими рекомендациями ФСБ № 149/7/2/6-432 России от 31 марта 2015 года, в случае, если выбрана только обобщенная возможность № 1, необходимо привести обоснование признания угроз 1.1-2.4 неактуальными (см. Таблицу № 5).

Таблица 5. Способы получения исходных данных

№	Уточненные возможности, используемые при создании способов, подготовке и проведении атак для требуемого класса СКЗИ	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
1	**СКЗИ класса КС1**		
1.1	а) создание способов, подготовка и проведение атак без привлечения специалистов в области разработки и анализа СКЗИ;	Не актуально	проводятся работы по подбору персонала; доступ в контролируемую зону, где располагается СКЗИ, обеспечивается в соответствии с контрольно-пропускным режимом;

№	Уточненные возможности, используемые при создании способов, подготовке и проведении атак для требуемого класса СКЗИ	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
			представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены СКЗИ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации; сотрудники, являющиеся пользователями ИСПДн «Альфа», но не являющиеся пользователями СКЗИ, проинформированы о правилах работы в ИСПДн и ответственности за несоблюдение правил обеспечения безопасности информации;
1.2	б) создание способов, подготовка и проведение атак на различных этапах жизненного цикла СКЗИ;	Не актуально	доступ в контролируемую зону, где располагается СКЗИ, обеспечивается в соответствии с контрольно-пропускным режимом; представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены

№	Уточненные возможности, используемые при создании способов, подготовке и проведении атак для требуемого класса СКЗИ	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
			СКЗИ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации; сотрудники, являющиеся пользователями ИСПДн, но не являющиеся пользователями СКЗИ, проинформированы о правилах работы в ИСПДн и ответственности за несоблюдение правил обеспечения безопасности информации;
1.3	в) проведение атаки находясь вне пространства, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств (далее контролируемая зона);	Не актуально	-
1.4	г) проведение на этапах разработки (модернизации), производства, хранения, транспортировки СКЗИ и этапе ввода в эксплуатацию СКЗИ (пусконаладочные работы) следующих атак:	Не актуально	-

№	Уточненные возможности, используемые при создании способов, подготовке и проведении атак для требуемого класса СКЗИ	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	– внесение несанкционированных изменений в СКЗИ		
1.5	д) проведение атак на этапе эксплуатации СКЗИ на: – персональные данные; ключевую, аутентифицирующую и парольную информацию СКЗИ; – программные компоненты СКЗИ; – аппаратные компоненты СКЗИ;	Не актуально	-
1.6	е) получение из находящихся в свободном доступе источников (включая информационно-телекоммуникационные сети, доступ к которым не ограничен определенным кругом лиц, в том числе информационно-телекоммуникационную сеть «Интернет») информации об информационной системе, в которой используется СКЗИ. При этом может быть получена следующая информация: – общие сведения об информационной	Не актуально	-

№	Уточненные возможности, используемые при создании способов, подготовке и проведении атак для требуемого класса СКЗИ	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	системе, в которой используется СКЗИ (назначение, состав, оператор, объекты, в которых размещены ресурсы информационной системы); ….		
1.7	ж) применение: – находящихся в свободном доступе или используемых за пределами контролируемой зоны АС и ПО, включая аппаратные и программные компоненты СКЗИ и СФ;	Не актуально	-
1.8	з) использование на этапе эксплуатации в качестве среды переноса от субъекта к объекту (от объекта к субъекту) атаки действий, осуществляемых при подготовке и (или) проведении атаки: – каналов связи, не защищенных от НСД к информации организационными и техническими мерами;	Не актуально	-
1.9	и) проведение на этапе	Не актуально	-

№	Уточненные возможности, используемые при создании способов, подготовке и проведении атак для требуемого класса СКЗИ	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	эксплуатации атаки из информационно-телекоммуникационных сетей (далее — ИТС), доступ к которым не ограничен определенным кругом лиц, если информационные системы, в которых используются СКЗИ, имеют выход в эти сети;		
1.10	к) использование на этапе эксплуатации находящихся за пределами контролируемой зоны АС и ПО из состава средств информационной системы, применяемых на местах эксплуатации СКЗИ (далее – штатные средства)	Не актуально	-
2	**СКЗИ класса КС2**		
2.1	а) проведение атаки при нахождении в пределах контролируемой зоны;	Не актуально	доступ в контролируемую зону, где располагается СКЗИ, обеспечивается в соответствии с контрольно-пропускным режимом; представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены СКЗИ, и сотрудники, не являющиеся пользователями

№	Уточненные возможности, используемые при создании способов, подготовке и проведении атак для требуемого класса СКЗИ	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
			СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации; сотрудники, являющиеся пользователями ИСПДн «Альфа», но не являющиеся пользователями СКЗИ, проинформированы о правилах работы в ИСПДн и ответственности за несоблюдение правил обеспечения безопасности информации;
2.2	б) проведение атак на этапе эксплуатации СКЗИ на следующие объекты: документацию на СКЗИ и компоненты СФ; Помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем (далее - СВТ), на которых реализованы СКЗИ и СФ	Не актуально	документация на СКЗИ хранится у ответственного за СКЗИ в металлическом сейфе; помещение, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФ, оснащены входными дверьми с замками, обеспечения постоянного закрытия дверей помещений на замок и их хранения
2.3	в) получение в рамках предоставленных полномочий, а также в	Не актуально	доступ в контролируемую зону, где располагается СКЗИ, обеспечивается в

№	Уточненные возможности, используемые при создании способов, подготовке и проведении атак для требуемого класса СКЗИ	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	результате наблюдений следующей информации: сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы; сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы; сведений о мерах по разграничению доступа в Помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ;		соответствии с контрольно-пропускным режимом; представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены СКЗИ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации; сотрудники, являющиеся пользователями ИСПДн «Альфа», но не являющиеся пользователями СКЗИ, проинформированы о правилах работы в ИСПДн и ответственности за несоблюдение правил обеспечения безопасности информации;
2.4	г) использование штатных средств, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных	Не актуально	на АРМ и серверах, на которых установлены СКЗИ: используются сертифицированные средства защиты информации от несанкционированного доступа; используются

№	Уточненные возможности, используемые при создании способов, подготовке и проведении атак для требуемого класса СКЗИ	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
	действий.		сертифицированные средства антивирусной защиты.

9. Определение применимого класса СКЗИ

Согласно Приказу ФСБ России №378, для обеспечения 4 уровня защищенности персональных данных при их обработке в информационной системе должны применяться СКЗИ класса КС1 и выше.

Исходя из результатов анализа способов получения исходных данных при создании способов, подготовке и проведении атак злоумышленников, для обеспечения безопасности персональных данных при реализации целенаправленных действий с использованием аппаратных и (или) программных средств с целью нарушения безопасности защищаемых СКЗИ персональных данных или создания условий для этого должны применяться СКЗИ класса КС1 и выше.

1.4 Ошибки по лабораторной работе

При выполнении лабораторной работы обучающиеся необоснованно полагают актуальными угрозы 2-го типа и даже 1-го типа, что приводит, соответственно, к необходимости парировать УБИ, связанные с НДВ, в системном и(или) прикладном программном обеспечении и применению СКЗИ класса КВ и выше.

Следует также информировать обучающихся, что необоснованное полагание актуальными угроз 2-го типа и даже 1-го типа приводит к значительному усложнению системы защиты для ИСПДн и, соответственно, стоимости применяемых программных и (или) аппаратных средств защиты.

1.5 Вывод по лабораторной работе

В ходе лабораторной работы были изучены НМД, согласно которым определяется уровень защищенности ПДн и класс СКЗИ, применяемых для обеспечения безопасности ПДн. Были определены уровень защищенности ПДн и класс СКЗИ для ИСПДн в соответствии с исходными данными.

2 Лабораторная работа № 2. «Риски информационной безопасности»

2.1 Цель работы

Освоение навыков применения НМД по определению и оценке рисков ИБ для типовой распределенной информационной системы заданного предприятия.

2.2 Задачи

В Лабораторной работе № 2 установлены следующие задачи:

Задача 1: Ознакомление с:

- ГОСТ Р ИСО/МЭК 27000-2012 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология [5];
- ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности [6];
- ГОСТ Р ИСО/МЭК 27003-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности [7];
- ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности [8].
- ГОСТ Р ИСО/МЭК 18045—2013 Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий [9];

Задача 2: Определение и оценка рисков информационной безопасности для типовой распределенной информационной системы заданного предприятия [10; 11]

2.3 Ход работы

1. Обследование объекта защиты

Пример сбора исходных данных:

- 3 филиала по 10 АРМ.
- У каждого филиала есть 1 руководитель с 1 АРМ.
- Сервер обработки ПДн находится в 1 филиале (ул. Московская д.1).
- Руководитель предприятия находится в 1 филиале (ул. Ленинградская д.1).
- Управление ИБ проводится в 1 филиале (ул. Московская д.1).
- В 3-х филиалах выход в сеть Интернет.

Пример анализа исходных данных:

- Защите подлежат ПДн, обрабатываемые в ИСПДн «Альфа»;
- В ИСПДн «Альфа» осуществляется обработка иных категорий ПДн, доступ к которым имеется у ограниченного круга лиц, подключаемых в соответствии с порядком, установленным внутренними НМД;
- В ИСПДн «Альфа» обрабатываются ПДн сотрудников всех 3-х филиалов (менее 100.000 субъектов ПДн);
- Перечень возможных УБИ, обрабатываемой в ИСПДн «Альфа» и соотнесение угрозы ИБ с возможными нарушителями, приведены в Таблице 1.

В качестве нарушителей рассматриваются:

- недобросовестные партнеры (1);
- бывшие сотрудники (2);
- пользователи информационной инфраструктуры (3);
- разработчики ПО (4);
- обслуживающий персонал (5);
- администраторы ИСПДн «Альфа» (6);
- взломщики программного обеспечения и информационных систем (7).

2. Определение перечня угроз

Таблица 1. Перечень угроз ИБ и возможность реализации угрозы ИБ нарушителем

№ УБИ в БДУ	**Угроза безопасности информации**	**Нарушитель ИБ**
-	Угроза утечки информации по визуально-оптическому каналу	1,3,6
-	Угроза утечки информации по каналу ПЭМИН	6,7
004	Угроза аппаратного сброса пароля BIOS	3,6
005	Угроза внедрения вредоносного кода в BIOS	6
006	Угроза внедрения кода или данных	1,4,6
018	Угроза загрузки нештатной операционной системы	3,6
024	Угроза изменения режимов работы аппаратных элементов компьютера	4,6
027	Угроза искажения вводимой и выводимой на периферийные устройства информации	4,6
034	Угроза использования слабостей протоколов сетевого/локального обмена данными	4,6,7

№ УБИ в БДУ	Угроза безопасности информации	Нарушитель ИБ
063	Угроза некорректного использования функционала программного и аппаратного обеспечения	3,4,6
067	Угроза неправомерного ознакомления с защищаемой информацией	1,5,6
074	Угроза несанкционированного доступа к аутентификационной информации	1,2,3,4,5,6,7
075	Угроза несанкционированного доступа к виртуальным каналам передачи	3,6
076	Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети	1,4,6
077	Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение	4,6
098	Угроза обнаружения открытых портов и идентификации привязанных к ним сетевых служб	3,6,7
099	Угроза обнаружения хостов	3,6,7
104	Угроза определения топологии вычислительной сети	3,6,7
113	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники	3,6
115	Угроза перехвата вводимой и выводимой на периферийные устройства информации	3,6
116	Угроза перехвата данных, передаваемых по вычислительной сети	3,6,7
123	Угроза подбора пароля BIOS	3,6
139	Угроза преодоления физической защиты	1,2,3,4,5,6,7
152	Угроза удаления аутентификационной информации	4,6
157	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	1,5,6
158	Угроза форматирования носителей информации	3,4,6
193	Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика	1,4,6
193	Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика	4,6,7

3. Определение уровня исходной защищенности

В соответствии с документом «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. ФСТЭК России 14.02.2008) определяется уровень исходной защищенности ИСПДн «Альфа» (Таблица2).

Таблица 2. Определение уровня исходной защищенности ИСПДн «Альфа»

Технические и эксплуатационные характеристики ИСПДн	**Уровень исходной защищенности**		
	Высокий	**Средний**	**Низкий**
1. По территориальному размещению			
Распределенная ИС, которая охватывает несколько областей, краев, округов или государство в целом	-	-	+
2. По наличию соединения с сетями общего пользования			
ИС, имеющая одноточечный выход в сеть общего пользования	-	+	-
3. По встроенным (легальным) операциям с данными			
Чтение, поиск;	+	-	-
Запись, удаление, сортировка;	-	+	-
Модификация, передача	-	-	+
4. По разграничению доступа к информации			
ИС, к которой имеет доступ определенный перечень работников	-	+	-
5. По наличию соединений с другими базами данных иных ИС			
ИС, в которой используется одна БД, принадлежащая	+	-	-
6. По уровню обобщения информации:			
ИС, в которой предоставляемые пользователю данные не являются обобщенными	-	-	+
7. По объему информации, которая предоставляется сторонним пользователям ИС без предварительной обработки:			
ИС, не предоставляющие никакой информации	+	-	-

ИСПДн «Альфа» имеет «низкий» уровень исходной защищенности, так как менее 70 % (66,67 %) характеристик ИСПДн «Альфа» соответствуют уровням не ниже «средний», а остальные (33,33%) соответствуют уровню защищенности «низкий». Соответственно, степень исходной защищенности ИСПДн «Альфа» Y1 = 10.

4. Определение актуальных угроз безопасности для ИСПДн

Для каждой оставшейся угрозы определяем вероятность возникновения угрозы (Y2), вычисляем коэффициент ее реализуемости (Y), ее опасность и, согласно методике разработки модели угроз определяем ее актуальность в Таблице 3. В Таблице 3 «Актуальность угрозы» определяется как «А» - актуальная или «НА» - неактуальная.

Таблица 3. Определение актуальных УБИ для ИСПДн

№ УБИ в БДУ	Наименование УБИ ИСПДн «Альфа»	Y1 (Уровень исходной защищенности информации) = 10				Оценка вероятности реализации УБИ/ Организационно-технические требования по защите информации ИСПДн «Альфа»
		Вероятность реализации УБИ (Y2)	Возможность реализации УБИ (Y)	Опасность УБИ	Актуальность УБИ	
Угрозы, которые могут быть реализованы внутренними нарушителями безопасности информации						
Угрозы, реализуемые с использованием технических каналов утечки информации						
139	Угроза преодоления физической защиты	0	0,5	Низкая	НА	Реализация угрозы считается маловероятной - отсутствуют объективные предпосылки для осуществления угрозы, так как реализованы следующие меры: – проводятся работы по подбору персонала; – доступ в КЗ ИСПДн «Альфа» обеспечивается в соответствии с контрольно-пропускным режимом; – работники Оператора ПДн

№ УБИ в БДУ	Наименование УБИ ИСПДн «Альфа»	Y1 (Уровень исходной защищенности информации) = 10				Оценка вероятности реализации УБИ/ Организационно-технические требования по защите информации ИСПДн «Альфа»
		Вероятность реализации УБИ (Y2)	Возможность реализации УБИ (Y)	Опасность УБИ	Актуальность УБИ	
						уведомлены о порядке обработки информации ограниченного доступа в ИСПДн «Альфа»; – на защищаемых объектах функционируют СКУД; – посетители и другие лица, не являющиеся работниками
-	Угроза утечки информации по визуально-оптическому каналу	0	0,5	Низкая	НА	Реализация угрозы считается маловероятной - отсутствуют объективные предпосылки для осуществления угрозы, так как реализованы следующие меры: – проводятся работы по подбору персонала; – доступ в КЗ ИСПДн «Альфа» обеспечивается в соответствии с контрольно-пропускным режимом; – пользователи ИСПДн «Альфа» уведомлены о порядке обработки информации ограниченного доступа в ИСПДн «Альфа»; – на защищаемых объектах функционируют СКУД; – посетители и другие лица, не являющиеся работниками
-	Угрозы утечки информации	0	0,5	Низкая	НА	Реализация угрозы считается низкой - отсутствуют объективные предпосылки для осуществления

№ УБИ в БДУ	Наименование УБИ ИСПДн «Альфа»	Y1 (Уровень исходной защищенности информации) = 10				Оценка вероятности реализации УБИ/ Организационно-технические требования по защите информации ИСПДн «Альфа»
		Вероятность реализации УБИ (Y2)	Возможность реализации УБИ (Y)	Опасность УБИ	Актуальность УБИ	
	по каналу ПЭМИН					угрозы по причине следующих условий: – распространение в помещениях Центра обработки данных широкополосного сигнала с равномерным энергетическим спектром во всем рабочем диапазоне частот («белый шум»), мощность такого сигнала существенно превышает уровень мощности ПЭМИН; – стоимость реализации угрозы утечки информации по каналу ПЭМИН, выраженная в стоимости специального оборудования и его эксплуатации, представляется значительной и несопоставимо превышающей возможный ущерб от нарушения конфиденциальности информации ограниченного доступа, обрабатываемой в ИСПДн «Альфа».
067	Угроза неправомерного ознакомления с защищаемой информацией	2	0,6	Средняя	А	Вероятность реализации угрозы считается средней - объективные предпосылки для реализации угрозы существуют ввиду недостаточности мер по контролю и управлению доступом к ТС ИСПДн «Альфа» при

№ УБИ в БДУ	Наименование УБИ ИСПДн «Альфа»	Y1 (Уровень исходной защищенности информации) = 10				Оценка вероятности реализации УБИ/ Организационно-технические требования по защите информации ИСПДн «Альфа»
		Вероятность реализации УБИ (Y2)	Возможность реализации УБИ (Y)	Опасность УБИ	Актуальность УБИ	
						их размещении за пределами КЗ. Принятые меры по защите информации недостаточны.
004	Угроза аппаратного сброса пароля BIOS	5	0,75	Высокая	А	Вероятность реализации угрозы считается высокой, так как объективные предпосылки для реализации угрозы существуют и обусловлены уязвимостями системных (материнских) плат – наличием механизмов аппаратного сброса паролей, установленных в BIOS/UEFI. Принятые меры обеспечения безопасности информации недостаточны.
024	Угроза изменения режимов работы аппаратных элементов компьютера	2	0,6	Низкая	НА	Вероятность реализации угрозы считается низкой - объективные предпосылки для реализации угрозы существуют, но следующие принятые меры существенно затрудняют ее реализацию: – проводятся работы по подбору персонала; – доступ в КЗ ИСПДн «Альфа» обеспечивается в соответствии с контрольно-пропускным режимом; – обслуживание и ремонт ТС ИСПДн «Альфа» осуществляют уполномоченные лица,

№ УБИ в БДУ	Наименование УБИ ИСПДн «Альфа»	Y1 (Уровень исходной защищенности информации) = 10				Оценка вероятности реализации УБИ/ Организационно-технические требования по защите информации ИСПДн «Альфа»
		Вероятность реализации УБИ (Y2)	Возможность реализации УБИ (Y)	Опасность УБИ	Актуальность УБИ	
						ответственные за их проведение; – для доступа к BIOS используется аутентификация на основе пароля;
063	Угроза некорректного использования функционала программного и аппаратного обеспечения	2	0,6	Высокая	А	Вероятность реализации угрозы считается высокой - объективные предпосылки для реализации угрозы существуют и обусловлены наличием известных уязвимостей ПО ИСПДн «Альфа» (Windows, MS SQL Server)
077	Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение	5	0,75	Высокая	А	Вероятность реализации угрозы считается средней, что обусловлено наличием известных слабостей ПО гипервизора, обеспечивающего изолированность адресного пространства, используемого для хранения не только защищаемой информации и программного кода обрабатывающих её программ, но и программного кода, реализующего виртуальное аппаратное обеспечение, от НСД со стороны вредоносной программы, функционирующей внутри виртуальной машины, а также недостаточностью мер антивирусной защиты. Принятые меры обеспечения безопасности информации

№ УБИ в БДУ	Наименование УБИ ИСПДн «Альфа»	Y1 (Уровень исходной защищенности информации) = 10				Оценка вероятности реализации УБИ/ Организационно-технические требования по защите информации ИСПДн «Альфа»
		Вероятность реализации УБИ (Y2)	Возможность реализации УБИ (Y)	Опасность УБИ	Актуальность УБИ	
						недостаточны.
113	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники	2	0,6	Средняя	А	Вероятность реализации угрозы считается низкой - объективные предпосылки для реализации угрозы существуют и обусловлены свойством оперативной памяти компьютера обнулять своё состояние при выключении и перезагрузке.
005	Угроза внедрения вредоносного кода в BIOS	2	0,6	Средняя	А	Вероятность реализации угрозы считается низкой - объективные предпосылки для реализации угрозы существуют, но следующие принятые меры существенно затрудняют ее реализацию: – проводятся работы по подбору персонала; – доступ в КЗ ИСПДн «Альфа» обеспечивается в соответствии с контрольно-пропускным режимом; – ремонт и обслуживание ТС ИСПДн «Альфа» осуществляют уполномоченные лица, ответственные за их проведение; – для доступа к BIOS используется аутентификация на основе пароля;
027	Угроза искажения	5	0,75	Средняя	А	Вероятность реализации угрозы считается средней, так как

№ УБИ в БДУ	Наименование УБИ ИСПДн «Альфа»	Y1 (Уровень исходной защищенности информации) = 10				Оценка вероятности реализации УБИ/ Организационно-технические требования по защите информации ИСПДн «Альфа»
		Вероятность реализации УБИ (Y2)	Возможность реализации УБИ (Y)	Опасность УБИ	Актуальность УБИ	
	вводимой и выводимой на периферийные устройства информации					объективные предпосылки для реализации угрозы существуют и обусловлены недостаточностью мер антивирусной защиты. Принятые меры обеспечения безопасности информации недостаточны.
034	Угроза использования слабостей протоколов сетевого/локального обмена данными	5	0,75	Высокая	А	Вероятность реализации угрозы считается средней, что обусловлено слабостями протоколов (заложенных в них алгоритмов) обмена данными, ошибками, допущенными в ходе реализации протоколов. Принятые меры обеспечения безопасности информации недостаточны.
018	Угроза загрузки нештатной операционной системы	2	0,6	Низкая	НА	Вероятность реализации угрозы считается низкой - объективные предпосылки для реализации угрозы существуют, но следующие принятые меры существенно затрудняют ее реализацию: – проводятся работы по подбору персонала; – доступ в КЗ ИСПДн «Альфа» обеспечивается в соответствии с контрольно-пропускным режимом; – обслуживание и ремонт ТС ИСПДн «Альфа» осуществляют уполномоченные лица,

№ УБИ в БДУ	Наименование УБИ ИСПДн «Альфа»	Y1 (Уровень исходной защищенности информации) = 10				Оценка вероятности реализации УБИ/ Организационно-технические требования по защите информации ИСПДн «Альфа»
		Вероятность реализации УБИ (Y2)	Возможность реализации УБИ (Y)	Опасность УБИ	Актуальность УБИ	
						ответственные за их проведение; – для доступа к BIOS используется аутентификация на основе пароля;
075	Угроза несанкционированного доступа к виртуальным каналам передачи	5	0,75	Высокая	А	Вероятность реализации угрозы считается средней, что обусловлено недостаточностью мер разграничения доступа к виртуальным каналам передачи данных и мер межсетевого экранирования. Принятые меры обеспечения безопасности информации недостаточны.
115	Угроза перехвата вводимой и выводимой на периферийные устройства информации	5	0,75	Средняя	А	Вероятность реализации угрозы считается средней, так как объективные предпосылки для реализации угрозы существуют и обусловлены недостаточностью мер антивирусной защиты, а также невозможностью осуществления защиты вводимой и выводимой на периферийные устройства информации с помощью СКЗИ. Принятые меры обеспечения безопасности информации недостаточны.
116	Угроза перехвата данных, передаваемых	5	0,75	Высокая	А	Вероятность реализации угрозы считается средней, что обусловлено недостаточностью мер межсетевого экранирования, а также возможными

№ УБИ в БДУ	Наименование УБИ ИСПДн «Альфа»	Y1 (Уровень исходной защищенности информации) = 10				Оценка вероятности реализации УБИ/ Организационно-технические требования по защите информации ИСПДн «Альфа»
		Вероятность реализации УБИ (Y2)	Возможность реализации УБИ (Y)	Опасность УБИ	Актуальность УБИ	
	по вычислительной сети					ошибками в конфигурации сетевого ПО. Принятые меры обеспечения безопасности информации недостаточны.
098	Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб	5	0,75	Высокая	А	Вероятность реализации угрозы считается средней, что обусловлено недостаточностью мер разграничения доступа и межсетевого экранирования. Принятые меры обеспечения безопасности информации недостаточны.
099	Угроза обнаружения хостов	5	0,75	Высокая	А	Вероятность реализации угрозы считается средней, что обусловлено слабостями механизмов сетевого взаимодействия, предоставляющих клиентам сети открытую техническую информацию о сетевых узлах, а также с ошибками конфигурирования средств межсетевого экранирования и фильтрации сетевого трафика, используемых в ИСПДн «Альфа» и (или) недостаточностью (отсутствием) этих средств ИСПДн «Альфа». Принятые меры обеспечения безопасности информации недостаточны.

№ УБИ в БДУ	Наименование УБИ ИСПДн «Альфа»	Y1 (Уровень исходной защищенности информации) = 10				Оценка вероятности реализации УБИ/ Организационно-технические требования по защите информации ИСПДн «Альфа»
		Вероятность реализации УБИ (Y2)	Возможность реализации УБИ (Y)	Опасность УБИ	Актуальность УБИ	
104	Угроза определения топологии вычислительной сети	5	0,75	Высокая	А	Вероятность реализации угрозы считается средней, что обусловлено слабостями сетевых протоколов, недостаточностью мер по разграничению доступа к сетевой инфраструктуре ИСПДн «Альфа», а также отсутствием механизмов контроля входных и выходных данных в ПО сетевого оборудования. Принятые меры обеспечения безопасности информации недостаточны.
006	Угроза внедрения кода или данных	5	0,75	Высокая	А	Вероятность реализации угрозы считается средней, что обусловлено недостаточностью мер антивирусной защиты. Принятые меры обеспечения безопасности информации недостаточны.
174	Угроза «фарминга»	5	0,75	Высокая	А	Вероятность реализации угрозы считается средней, так как объективные предпосылки для реализации угрозы существуют и обусловлены известными уязвимостями DNS-сервера и сетевого оборудования. Принятые меры обеспечения безопасности информации недостаточны.
152	Угроза удаления	5	0,75	Высокая	А	Вероятность реализации угрозы считается средней, так как

№ УБИ в БДУ	Наименование УБИ ИСПДн «Альфа»	Y1 (Уровень исходной защищенности информации) = 10				Оценка вероятности реализации УБИ/ Организационно-технические требования по защите информации ИСПДн «Альфа»
		Вероятность реализации УБИ (Y2)	Возможность реализации УБИ (Y)	Опасность УБИ	Актуальность УБИ	
	аутентификационной информации					объективные предпосылки для реализации угрозы существуют и обусловлены известными уязвимостями ПО ИСПДн «Альфа», осуществляющего разграничение доступа (Windows), и недостаточностью мер по разграничению доступа к аутентификационной информации безопасности. Принятые меры обеспечения безопасности информации недостаточны.
076	Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети	5	0,75	Высокая	А	Вероятность реализации угрозы считается средней, что обусловлено наличием множества разнообразных интерфейсов взаимодействия между гипервизором и виртуальной машиной и (или) физической сетью, известными уязвимостями ПО гипервизора, а также ограниченностью функциональных возможностей аппаратных средств, используемых для обеспечения его работоспособности.
123	Угроза подбора пароля BIOS	2	0,6	Высокая	А	Вероятность реализации угрозы считается низкой, так как объективные предпосылки для реализации угрозы существуют и обусловлены слабостями механизма

№ УБИ в БДУ	Наименование УБИ ИСПДн «Альфа»	Y1 (Уровень исходной защищенности информации) = 10				Оценка вероятности реализации УБИ/ Организационно-технические требования по защите информации ИСПДн «Альфа»
		Вероятность реализации УБИ (Y2)	Возможность реализации УБИ (Y)	Опасность УБИ	Актуальность УБИ	
						аутентификации в BIOS, но принятые меры обеспечения безопасности и факты затрудняют ее реализацию: – используется аутентификация в BIOS на основе пароля; – для реализации угрозы помимо соответствующих привилегий в ОС ТС ИСПДн «Альфа» нарушителю необходимо обладать специальным программным средством перебора паролей BIOS.
193	Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика	5	0,75	Высокая	А	Вероятность реализации угрозы считается средней, что обусловлено недостаточностью мер антивирусной защиты информации ИСПДн «Альфа» и межсетевого экранирования. Принятые меры обеспечения безопасности информации недостаточны.
158	Угроза форматирования носителей информации	0	0,5	Низкая	НА	Реализация угрозы считается маловероятной - отсутствуют объективные предпосылки для осуществления угрозы, так как реализованы следующие меры: – проводятся работы по подбору

№ УБИ в БДУ	Наименование УБИ ИСПДн «Альфа»	Y1 (Уровень исходной защищенности информации) = 10				Оценка вероятности реализации УБИ/ Организационно-технические требования по защите информации ИСПДн «Альфа»
		Вероятность реализации УБИ (Y2)	Возможность реализации УБИ (Y)	Опасность УБИ	Актуальность УБИ	
						персонала; – доступ в КЗ ИСПДн «Альфа» обеспечивается в соответствии с контрольно-пропускным режимом; – работники Оператора ПДн уведомлены о порядке обработки информации ограниченного доступа в ИСПДн «Альфа»; – на защищаемом объекте функционируют СКУД; – посетители и другие лица, не являющиеся работниками – осуществляется резервное копирование БД ИСПДн «Альфа».
139	Угроза преодоления физической защиты	0	0,5	Низкая	НА	Реализация угрозы считается маловероятной - отсутствуют объективные предпосылки для осуществления угрозы, так как реализованы следующие меры: – проводятся работы по подбору персонала; – доступ в КЗ ИСПДн «Альфа» обеспечивается в соответствии с контрольно-пропускным режимом; – работники Оператора ПДн уведомлены о порядке обработки информации ограниченного

№ УБИ в БДУ	Наименование УБИ ИСПДн «Альфа»	Y1 (Уровень исходной защищенности информации) = 10				Оценка вероятности реализации УБИ/ Организационно-технические требования по защите информации ИСПДн «Альфа»
		Вероятность реализации УБИ (Y2)	Возможность реализации УБИ (Y)	Опасность УБИ	Актуальность УБИ	
						доступа в ИСПДн «Альфа»; – на защищаемых объектах функционируют СКУД; – посетители и другие лица, не являющиеся работниками
157	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/ передачи информации	0	0,5	Низкая	НА	Реализация угрозы считается маловероятной - отсутствуют объективные предпосылки для осуществления угрозы, так как реализованы следующие меры: – проводятся работы по подбору персонала; – доступ в КЗ ИСПДн «Альфа» обеспечивается в соответствии с контрольно-пропускным режимом; – работники Оператора ПДн уведомлены о порядке обработки информации ограниченного доступа в ИСПДн «Альфа»; – на защищаемых объектах функционируют СКУД; – посетители и другие лица, не являющиеся работниками

5. Определение перечня актуальных угроз безопасности для ИСПДн
Для ИСПДн «Альфа» актуальны следующие УБИ (см. Таблицу 4):

Таблица 4: Актуальные угрозы ИСПДн «Альфа»

№ УБИ БДУ	Угроза безопасности информации
004	Угроза аппаратного сброса пароля BIOS
005	Угроза внедрения вредоносного кода в BIOS
006	Угроза внедрения кода или данных
027	Угроза искажения вводимой и выводимой на периферийные устройства информации
034	Угроза использования слабостей протоколов сетевого/локального обмена данными
063	Угроза некорректного использования функционала программного и аппаратного обеспечения
067	Угроза неправомерного ознакомления с защищаемой информацией
075	Угроза несанкционированного доступа к виртуальным каналам передачи
076	Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети
077	Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение
098	Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб
099	Угроза обнаружения хостов
104	Угроза определения топологии вычислительной сети
113	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники
115	Угроза перехвата вводимой и выводимой на периферийные устройства информации
116	Угроза перехвата данных, передаваемых по вычислительной сети
123	Угроза подбора пароля BIOS
139	Угроза преодоления физической защиты
152	Угроза удаления аутентификационной информации
157	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации
158	Угроза форматирования носителей информации
174	Угроза «фарминга»
193	Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика

6. Анализ и оценка рисков

На основании сформированного выше перечня актуальных УБИ для ИСПДн далее выполним анализ и оценку рисков.

Оценка рисков выполняется для каждой актуальной УБИ по количественной шкале для 3-х аргументов: значения вероятности (В), значения управляемости (У) и величина последствий (П). Каждый аргумент оценивается по шкале от 1 до 5, итоговое значение индекса риска определяется перемножением (П*В*У). Результат анализа и оценки рисков приведены в Таблице 5.

Таблица 5: Оценка рисков

Риск	Последствия (1-5)	Вероятность (1-5)	Управляемость (1-5)	Индекс риска (П*В*У)
Угроза аппаратного сброса пароля BIOS	2	2	3	12
Угроза внедрения вредоносного кода в BIOS	1	1	2	2
Угроза внедрения кода или данных	3	2	2	12
Угроза искажения вводимой и выводимой на периферийные устройства информации	2	2	2	8
Угроза использования слабостей протоколов сетевого/локального обмена данными	3	3	2	18
Угроза некорректного использования функционала программного и аппаратного обеспечения	4	4	3	48
Угроза неправомерного ознакомления с защищаемой информацией	5	3	3	45
Угроза несанкционированного доступа к виртуальным каналам передачи	2	2	3	12
Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети	3	3	2	18
Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение	3	1	3	9
Угроза обнаружения открытых портов и	2	4	3	24

идентификации привязанных к нему сетевых служб				
Угроза обнаружения хостов	2	4	3	24
Угроза определения топологии вычислительной сети	2	4	3	24
Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники	3	3	3	27
Угроза перехвата вводимой и выводимой на периферийные устройства информации	2	3	2	12
Угроза перехвата данных, передаваемых по вычислительной сети	3	2	3	18
Угроза подбора пароля BIOS	2	1	2	4
Угроза преодоления физической защиты	2	1	2	4
Угроза удаления аутентификационной информации	2	2	2	8
Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации	2	2	2	8
Угроза форматирования носителей информации	2	1	3	6
Угроза «фарминга»	3	2	2	12
Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика	4	3	3	36

2.4 Ошибки по лабораторной работе

При выполнении лабораторной работы обучающиеся необоснованно могут определить значения факторов риска (последствий, вероятностей и управляемости), что приводит, соответственно, к неверному определению итогового значения риска.

Следует также информировать обучающихся, что необходимо обеспечивать объективность при экспертном определении указанных выше факторов риска (последствий, вероятностей и управляемости), например, воспроизводимость и повторяемость оценок рисков.

Игнорирование данных требований может привести к значительному усложнению системы защиты для ИСПДн и, соответственно, стоимости применяемых программных и (или) аппаратных средств защиты.

2.5 Вывод по лабораторной работе

В ходе лабораторной работы были изучены НМД, согласно которым могут определяться и оцениваться риски ИБ на предприятии.

3 Лабораторная работа № 3. «Определение ценных активов предприятия и их категорирование»

3.1 Цель работы

Освоение навыков применения НМД по защите информации для идентификации активов в пределах области функционирования системы менеджмента ИБ (СМИБ) и последствий воздействия на них.

3.2 Задачи

В Лабораторной работе №3 установлены следующие задачи:

Задача 1: Ознакомление с:

- ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности требования [12];
- ГОСТ Р ИСО 22301-2014 Системы менеджмента непрерывности бизнеса. Общие требования [13].

Задача 2: Определение ценных активов предприятия по перечню критериев.

3.3 Ход работы

1. Обследование объекта защиты
2. Формирование организационно-структурной схемы (см. рис.1)

Рисунок 1 – Организационно-структурная схема

3. Определение наиболее важных информационных потоков

На основании организационно-структурной схемы определяем наиболее важные информационные потоки:

- «Директор – Информация о стратегическом управлении (актив)» – Поток A;
- «Директор по производству – Сведения о производимой продукции (актив)» – Поток B;
- «Технический директор – «Сведения о разработках на предприятии (актив)» – Поток C;
- «Директор по качеству и технологии – «Сведения о качестве продукции и используемых технологиях производства (актив)» – Поток D;
- «Директор по персоналу» – ПДн работников (актив)» – Поток E;
- «Директор по безопасности» – «Сведения о системах защиты (актив)» – Поток F.

4. Определение последствий нарушения свойств ИБ для информационных потоков

Последствия нарушений связаны с основными свойствами ИБ (согласно ГОСТ Р ИСО/МЭК 27001):

- конфиденциальностью – свойством информации быть недоступной и закрытой для неавторизованного индивидуума, логического объекта или процесса;
- целостностью – свойством сохранения правильности и полноты активов;
- доступностью – свойством объекта находиться в состоянии готовности и возможности использования по запросу авторизованного логического объекта

Таблица 1 – Таблица последствий нарушения свойств ИБ

	Поток A	**Поток B**	**Поток C**	**Поток D**	**Поток E**	**Поток F**
Конфиденциальность	+		+	+	+	+
Целостность	+	+		+		
Доступность	+	+				

5. Определение критичности свойств ИБ для информационных потоков

Для обеспечения уверенности в том, что информация защищена на надлежащем уровне, необходима ее классификация исходя из правовых требований, ее конфиденциальности, а также ценности и критичности для организации. На основе внутренней экспертной оценки последствий нарушений, применительно к конкретному информационному потоку, можно сделать качественные выводы, выраженные в соответствии со шкалой, где 0 - «нет воздействия», 5 - «наиболее высокая степень критичности воздействия».

Таблица 2 – Таблица критичности свойств ИБ

	Поток A	**Поток B**	**Поток C**	**Поток D**	**Поток E**	**Поток F**
Конфиденциальность	4	1	5	5	3	4
Целостность	2	3	1	3	1	1
Доступность	2	3	1	1	1	1

6. Определение вероятности нарушения свойств ИБ для информационных потоков

Для оценки рисков значимой информации, циркулирующей в конкретном потоке, необходима оценка вероятности нарушения свойств ИБ. На основе внутренней экспертной оценки вероятностей, применительно к конкретному информационному потоку, можно сделать качественные выводы, выраженные в соответствии со шкалой, где 0 - «крайне низкая вероятность», 5 - «наиболее высокая вероятность».

Таблица 3 – Таблица вероятности нарушения свойств ИБ

	Поток A	Поток B	Поток C	Поток D	Поток E	Поток F
Конфиденциальность	4	1	4	4	3	5
Целостность	1	1	1	2	1	1
Доступность	2	4	1	1	1	1

7. Определение стоимости активов

На основании полученных выше данных о критичности и вероятности свойств ИБ в отношении значимой информации, относящихся к конкретному информационному потоку, определим стоимость активов.

Для определения стоимости актива используем формулу:

$$Ц_a = (C_р+C_п)*k_1*k_2+Л$$

где:

$C_р$ – затраты на создание, разработку актива, руб.;

$C_п$ – затраты на обеспечение правовой охраны актива, руб.;

k_1 – коэффициент технико-экономической значимости (0 – 1);

k_2 – коэффициент промышленной готовности (0 – 1);

Л – лицензионные выплаты, руб.

Таблица 4 – Оценка стоимости активов

Атрибут	**Поток A**	**Поток B**	**Поток C**	**Поток D**	**Поток E**	**Поток F**
$C_р$, тыс. руб.	45	100	150	60	130	90
$C_п$, тыс. руб.	0	30	50	0	60	45

k_1	0,8	0,7	0,8	1	0,6	1
k_2	1	1	0,7	0,5	1	1
Л, тыс. руб.	0	30	75	25	0	100
$Ц_а$, тыс. руб.	**36**	**121**	**187**	**55**	**114**	**235**

3.4 Варианты выполнения лабораторной работы

В качестве варианта выполнения данной лабораторной работы можно рекомендовать начать с построения схемы информационного воздействия, на которой показаны информационные потоки и основные подразделения относительно границ предприятия (см. рис. 2)

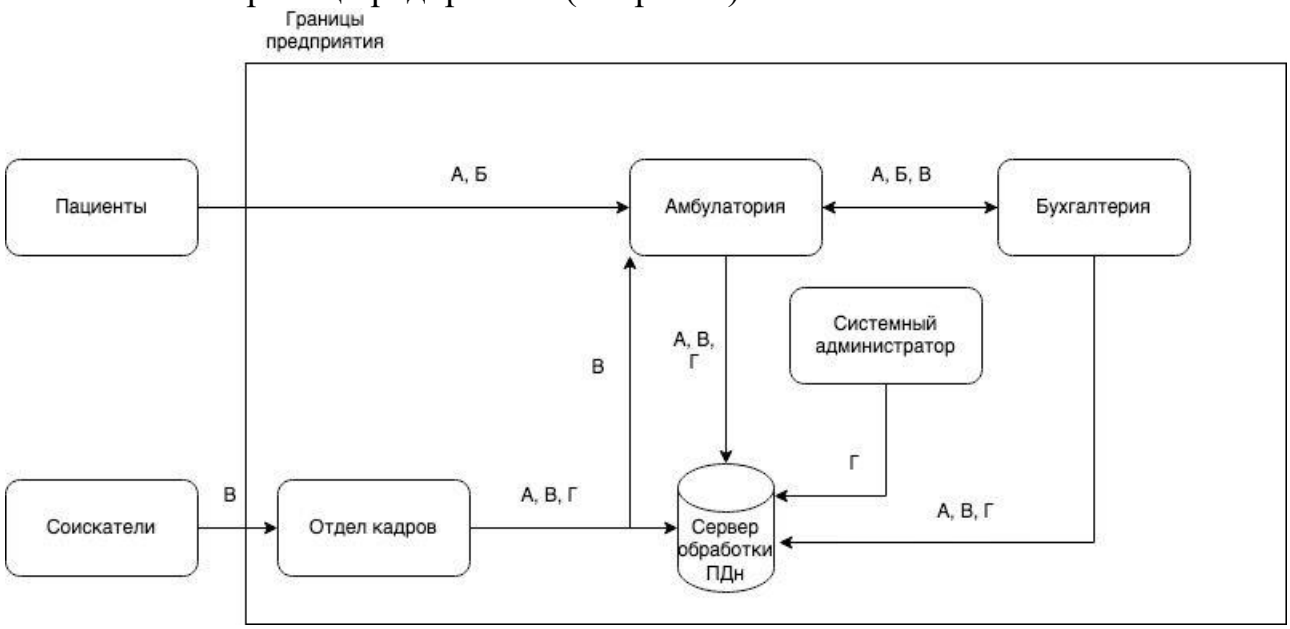


Рисунок 2 – Схема информационного воздействия

Также можно рекомендовать определять вероятность атаки на каждый актив в абсолютных значениях (от 0 до 1), нормируя полную вероятность для каждого конкретного потока к 1. Пример показан ниже в Таблице 5.

Таблица 5 – Таблица вероятности атак на каждый из активов

	Поток А	**Поток Б**	**Поток В**	**Поток Г**
Конфиденциальность	0,5	0,6	0,5	0,4
Целостность	0,25	0,1	0,3	0,4
Доступность	0,25	0,3	0,2	0,2

3.5 Ошибки по лабораторной работе

При выполнении лабораторной работы обучающиеся необоснованно могут упустить или неверно определить лицензионные платежи за ПО (например –

операционные системы, прикладное ПО и пр.), что приводит, соответственно, к неверному определению итоговой стоимости активов.

Следует информировать обучающихся, что необходимо обеспечивать объективность и полноту описания информационных потоков на реальном объекте, поскольку пропуск или дублирование критичных информационных потоков может негативно повлиять на итоговый анализ стоимости активов.

Следует также информировать обучающихся, что необходимо обеспечивать реальную оценку активов, минимально по «триаде» конфиденциальности, целостности и доступности, но при этом учесть и возможность расширения свойств ИБ – неотказуемость, подотчетность, прослеживаемость на реальном объекте.

Игнорирование данных требований может привести к значительному усложнению системы защиты для ИСПДн и, соответственно, стоимости применяемых программных и (или) аппаратных средств защиты.

3.6 Вывод по лабораторной работе

В ходе лабораторной работы были изучены НМД, согласно которым обеспечивается соответствующая защита информационных активов организации. Были определены наиболее важные информационные потоки, критичность свойств связанных с ними активов, вероятность реализации атак на них, а также осуществлен расчет стоимости активов.

4 Лабораторная работа № 4. «Аудит информационной безопасности»

4.1 Цель работы

Освоение навыков применения НМД по аудиту СМИБ.

4.2 Задачи

В Лабораторной работе №4 установлены следующие задачи:

Задача 1: Ознакомление с:

- ISO 19011:2018 Guidelines for auditing management systems [15].
- ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности требования [12].
- ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод и набор правил менеджмента информационной безопасности [6].
- ГОСТ Р ИСО/МЭК 27007-2014 Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности [14].

Задача 2: Подготовка программы аудита системы менеджмента информационной безопасности [16;17]

4.3 Ход работы

1. Подготовительные мероприятия

- Установление контакта аудиторской группы с руководством проверяемой организации;
- На первичной встрече определяются каналы передачи информации, предоставляется необходимая документация для проведения аудита, определения необходимых мероприятий, согласования планов-графиков;
- Проведение анализа документации при подготовке к проведению аудита на месте;
- Документация для проведения аудита включает в себя документы по ИБ, и в случае наличия, отчеты по предыдущим аудитам;
- Подготовка программы аудита;
- Подготовка отчета по аудиту.

2. Определение цели аудита

Цель аудита - Систематический, независимый и документируемый процесс получения свидетельств аудита и объективного их оценивания с целью установления степени выполнения согласованных критериев аудита.

Цели отдельных аудиторов – проведение оценки соответствия отдельных критериев.

Пример описания места проведения аудита.

- Офис компании имеет площадь 200 м^2, в офисе располагаются 25 АРМ.
- Производственный цех имеет площадь 2000 м^2, в нем располагаются 60 АРМ.

3. Определение рисков аудита

Для проведения аудита должны быть определены риски, связанные с программой аудита, обязанности по аудиту, необходимые ресурсы. Для проведения аудита привлекаются руководитель аудиторской проверки и 3 аудитора. Аудит проводится по этапам:

- Подготовка к проведению аудита на месте (Выполнение анализа документов при подготовке к аудиту);
- Сбор информации для подготовки мероприятий аудита и подходящих рабочих документов, например относящихся к процессам, должностным обязанностям;
- Обзор документации системы для выявления возможных пробелов;
- Проведение аудита на месте;
- Подготовка отчета об аудите.

4. Типовые действия при аудите

Типовые действия при аудите в соответствии с ГОСТ Р ИСО 19011-2012 представлены на Рис. 1.

Рисунок 1 — Действия при проведении аудита

5. Основные объекты анализа в рамках аудита

Пример основных объектов анализа в рамках аудита:

- Бизнес-стратегия предприятия;
- Модель бизнес-процессов предприятия, включая процессы управления, основной деятельности и процессы обеспечивающей деятельности;
- Организационная структура предприятия;
- Положения о подразделениях предприятия;
- Документация системы менеджмента качества;
- Документация СМИБ;
- Документация в части системы управления ИТ:
    - штатное расписание ИТ-подразделений;
    - положения об ИТ-подразделениях и его структурных единицах;
    - регламенты, должностные инструкции сотрудников ИТ-подразделений;

- проектная, эксплуатационная и пользовательская документация по системам автоматизации управления предприятия (системы поддержки процессов управления ИТ-услугами, управления ИТ-инфраструктурой, мониторинга приложений и ИТ-инфраструктуры и т.п.);
- документация по структуре, составу и технологическим характеристикам эксплуатируемых информационных систем предприятия.

6. Идентификация ресурсов для проведения аудита

В стоимость проведения аудита включается оплата за работу аудиторской группы, расходы на проезд, проживание, потребности организационного характера, финансовые ресурсы по улучшению аудиторской деятельности, технические средства проведения аудита.

План проведения аудита согласовывается заранее с организацией заказчиком.

7. Распределение работ между членами аудиторской группы

Руководитель аудиторской группы отвечает за распределение ответственности между членами группы, осуществляет взаимодействие с руководством проверяемой организации, несет ответственность за проведение аудита. Члены группы осуществляют анализ документации, проведение аудиторской проверки внутри предприятия.

8. Подготовка документации

План выборки, составленный для проведения в компании:

- Выборочная проверка документации.
- Выборочная проверка технических средств защиты и ИТ-инфраструктуры.

9. Проведение аудита на месте

- Проведение предварительного совещания.
- Выполнение анализа документов во время проведения аудита.
- Обмен информацией во время проведения аудита.
- Роль и обязанности сопровождающих лиц и наблюдателей.
- Сбор и верификация информации.
- Формирование выводов аудита.
- Подготовка заключений по результатам аудита.
- Проведение заключительного совещания.

10. Подготовка и рассылка отчета по аудиту

Руководитель группы по аудиту несет ответственность за подготовку и содержание отчета по аудиту. Отчет по аудиту должен содержать полные, точные, четко сформулированные и понятные записи по аудиту и, в соответствии с процедурами аудита, должен включать в себя или содержать ссылку на следующее:

- цели аудита;
- область аудита, в частности, идентификация проверенных организационных и функциональных подразделений или процессов и охватываемый период времени;
- идентификацию заказчика аудита;
- идентификацию членов группы по аудиту и представителей проверяемой организации, принимавших участие в проведении аудита;
- даты и места проведения аудита на месте;
- критерии аудита;
- выводы аудита;
- заключения по результатам аудита;
- заявление о степени соответствия критериям аудита.

Отчет по аудиту должен быть подготовлен и представлен в согласованные сроки, должен иметь дату выпуска, надлежащим образом проанализирован и утвержден в соответствии с процедурами программы аудита. Затем отчет по аудиту должен быть разослан получателям, определенным процедурами аудита.

11. Формирование программы аудита

Программа аудита показана в Табл.1

Таблица 1. Формирование программы аудита

Дата	Этап	Описание	Исполнитель
30.09.2020 - 02.10.2020	Подготовительный этап	– Установление первичного контакта с клиентом; – Предварительный анализ документации; – Подготовка плана проведения аудита; – Разделение обязанностей между аудиторами; – Подготовка рабочей документации.	Начальник отдела аудита
05.10.2020 -	Выезд на место, проведение аудита	– Встреча аудиторской группы с руководителем;	Аудиторы

09.10.2020		– Анализ документации; – Интервьюирование; – Аудит технических средств; – Сбор и верификация информации; – Выводы; – Завершающая встреча с руководителем.	
12.10.2020 - 16.10.2020	Подготовка отчетной документации	– Подготовка отчета по результатам аудита; – Отправка отчетной документации заказчику.	Технический писатель отдела аудита

4.4 Варианты выполнения лабораторной работы

1. Могут быть определены следующие цели программы аудита:
   – Обследование бизнес-процессов, выделенных в рамках проекта «Альфа», которое проводится с целью выявления в них информационных активов, нуждающихся в защите,
   – Создание концептуального понимания принципов легитимного обращения с конфиденциальной информацией в подразделениях.

2. Могут быть определены следующие риски и возможности, связанные с программой аудита и действия по их обработке:
   – Риски, связанные с коммуникацией (плохо работающими процессами/каналами внутреннего/внешнего обмена информацией);
   – Риски, связанные с реализацией (ненадлежащей координацией в рамках программы аудита или недостаточным вниманием к вопросам ИБ и конфиденциальности).

3. Могут быть определены следующие критерии отбора членов группы по аудиту. Сотрудник должен быть:
   – этичным, т.е. справедливым, правдивым, искренним, честным и сдержанным;
   – открытым, то есть иметь желание рассматривать альтернативные идеи или точки зрения;
   – дипломатичным, т.е. тактичным в общении с людьми;
   – наблюдательным, т.е. активно отслеживать окружающую обстановку и действия;
   – проницательным, т.е. знать и быть в состоянии понимать ситуации;
   – гибким, т.е. способным легко адаптироваться к различным ситуациям;

- упорным, т.е. настойчивым и направленным на достижение поставленных целей;
- логичным, т.е. способным своевременно делать выводы на основе логических рассуждений и анализа;
- уверенным в себе, т.е. способным действовать независимо, при этом результативно взаимодействуя с другими;
- принципиальным, т.е. способным действовать ответственно и в рамках этики, даже если эти действия не всегда могут вызывать одобрение и иногда вести к несогласию или конфронтации;
- готовым к совершенствованию, т.е. имеющим желание извлекать уроки из ситуаций;
- уважительным к культурным особенностям, т.е. соблюдающим и уважающим культурные традиции проверяемой организации;
- настроенным на сотрудничество, т.е. результативно взаимодействующим с другими, в том числе членами группы по аудиту и персоналом проверяемой организации.

Могут быть определены следующие требования к способностям аудиторов:

- понимать характер рисков и возможностей, связанных с аудитом, и принципы риск-ориентированного подхода к аудиту;
- результативно планировать и организовывать работу;
- проводить аудит в рамках согласованного графика;
- расставлять приоритеты и фокусироваться на вопросах, имеющих важное значение;
- результативно обмениваться информацией в устной и письменной форме (лично или через переводчиков);
- собирать информацию путем результативного интервьюирования, выслушивания, наблюдения и анализа документированной информации, включая записи и данные;
- понимать пригодность и последствия использования методов выборки для аудита;
- воспринимать и учитывать мнения экспертов;
- проводить аудит процесса от начала до конца, включая взаимосвязи с другими процессами и различными функциями, где это требуется;
- проверять актуальность и точность собранной информации;
- подтверждать достаточность и пригодность свидетельств аудита для обоснования выводов и заключений аудита;
- оценивать те факторы, которые могут повлиять на достоверность выводов и заключений аудита;

– документировать мероприятия по аудиту и выводы аудита, а также формировать отчеты;
– соблюдать конфиденциальность и меры защиты информации.

4.5 Ошибки по лабораторной работе

При выполнении лабораторной работы обучающиеся необоснованно могут упустить или неверно определить даты выполнения аудита, например не принять во внимание выходные, праздничные дни и государственные праздники, что приводит, соответственно, к неверному определению итоговой программы аудита.

Следует информировать обучающихся, что необходимо обеспечивать общую длительность аудита не более 5 рабочих дней на площадке заказчика (*on-site audit*), поскольку увеличение длительности аудита может негативно повлиять на итоговый результат аудита.

Следует информировать обучающихся, что необходимо ограничивать общую численность команды аудиторов, поскольку значительное увеличение числа участников аудита может негативно повлиять на итоговый результат аудита и, кроме того, привести к необоснованному увеличению издержек.

Игнорирование данных требований может привести к значительному усложнению процесса аудита ИБ или невозможности достижения поставленных целей аудита в установленный срок.

4.6 Вывод по лабораторной работе

В ходе лабораторной работы были изучены НМД, согласно которым определяется процесс аудита ИБ, а также составлена программа проведения аудита для Предприятия.

5 Заключение

В данном учебно-методическом пособии представлен набор лабораторных работ для обучения по курсу «Нормативно-методическое обеспечение информационной безопасности» для подготовки магистрантов по направлению 10.04.01 «Информационная безопасность». Все лабораторные работы имеют постановку задачи, собственную теоретическую часть, примеры заполнения, а также описание различных ошибок, которые могут встретиться обучающимся при самостоятельном выполнении. Каждая лабораторная работа оформлена как единый учебный блок, содержит собственную постановку задачи, описание хода вывода, отдельные промежуточные результаты и общий вывод по итогам работы. Для удобства восприятия информации применяются табличные формы и рисунки, поясняющие ход выполнения каждой лабораторной работы. Также в пособии приведены основные источники, в том числе список рекомендуемой литературы и дополнительные НМД. Список рекомендуемой литературы соответствует теоретическому курсу «Нормативно-методическое обеспечение информационной безопасности» и включает актуальные статьи на русском и английских языках. В приложении приведены дополнительные материалы (нормативные документы ФСТЭК России и ФСБ России, национальные ГОСТ Р и международные стандарты ISO, ISO/IEC). Эти дополнительные материалы могут быть изучены как в рамках курса «Нормативно-методическое обеспечение информационной безопасности», так и в качестве дополнительных материалов при самообучении.

Основными тенденциями развития учебной дисциплины можно полагать дальнейшее углубленное изучение всего спектра применяемых современных ИТ, в том числе применяемых для защиты информации критических и высоконагруженных приложений, функционирующих круглосуточно, а также повышенное внимание к современных точным методам оценки рисков нарушения безопасности ИТ и формирование оптимальных мер и средств обеспечения ИБ. Можно полагать, что основные выводы для обучающихся по программе подготовки 10.04.01 «Информационная безопасность» должны лежать в плоскости не чисто технической, а юридической и технологической, поскольку от правильного выбора ИТ и корректного построения системы обеспечения безопасности зависит стабильность и результативность функционирования бизнес-процессов современного предприятия.

В настоящем учебно-методическом пособии по причине ограниченности объема рассмотрены не все возможные проблемы. Можно отметить, что в настоящее время не полностью решены вопросы с корректным категорированием объектов критической инфраструктуры, даже при наличии профильного Федерального закона (ФЗ-187) и Постановления Правительства (ПП-127). Важными характеристиками данной проблемы можно полагать значительный

охват по отраслям промышленности, огромное количество объектов, подлежащих категорированию и учету, сложность выявления существующих закономерностей развития ИТ и соответствующих встроенных мер защиты (подсистем аварийной защиты, ПАЗ) для различных производителей.

Для дальнейшего изучения дисциплины обучающимся рекомендуется постоянно работать с перечнем актуальных НМД. Состав этих документов может отличаться от указанного перечня рекомендуемой литературы, поскольку периодически обновляются и выходят новые национальные стандарты в системе ГОСТ Р, а также новые международные стандарты ISO и ISO/IEC. Отдельно нужно отметить рекомендации по ознакомлению с актуальными версиями НМД на сайтах ФСТЭК России и ФСБ России.

6 Список рекомендуемой литературы

1. Приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;
2. Постановление Правительства Российской Федерации «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» №1119 от 01 ноября 2012.
3. Лившиц И.И. Оценка степени влияния General Data Protection Regulation на безопасность предприятий РФ // Вопросы кибербезопасности - 2020. - № 4(38). - С. 66-74
4. Лившиц И.И. Оценка уровня обеспечения информационной безопасности в кредитной организации // Стандарты и качество - 2020. - № 7. - С. 44-49
5. ГОСТ Р ИСО/МЭК 27000-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология
6. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности;
7. ГОСТ Р ИСО/МЭК 27003-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности;
8. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.
9. ГОСТ Р ИСО/МЭК 18045—2013 Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий;

10. Лившиц И.И. Метод оценивания безопасности облачных ИТ-компонент по критериям существующих стандартов // Труды СПИИРАН [SPIIRAS Proceedings] - 2020. - Т. 19. - № 2(69). - С. 383-411
11. Лившиц И.И., Неклюдов А. Риски токсичных активов в информационных технологиях // Стандарты и качество - 2017. - № 5. - С. 20-25
12. ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности требования;
13. ГОСТ Р ИСО 22301-2014 Системы менеджмента непрерывности бизнеса. Общие требования.
14. ГОСТ Р ИСО/МЭК 27007-2014 Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности.
15. ISO 19011:2018 Guidelines for auditing management systems.
16. Livshitz I.I., Neklyudov A.V., Lontsikh P.A. Evaluation of IT security – genesis and its state-of-art // Journal of Physics: Conference Series - 2018, Vol. 1015, No. 4, pp. 042029
17. Livshitz I.I., Neklyudov A.V., Lontsikh P.A. IT security evaluation - “hybrid” approach and risk of its implementation // Journal of Physics: Conference Series - 2018, Vol. 1015, No. 4, pp. 042030

7 Приложения

7.1 Определение уровня защищенности ПДн в зависимости от типа актуальных угроз

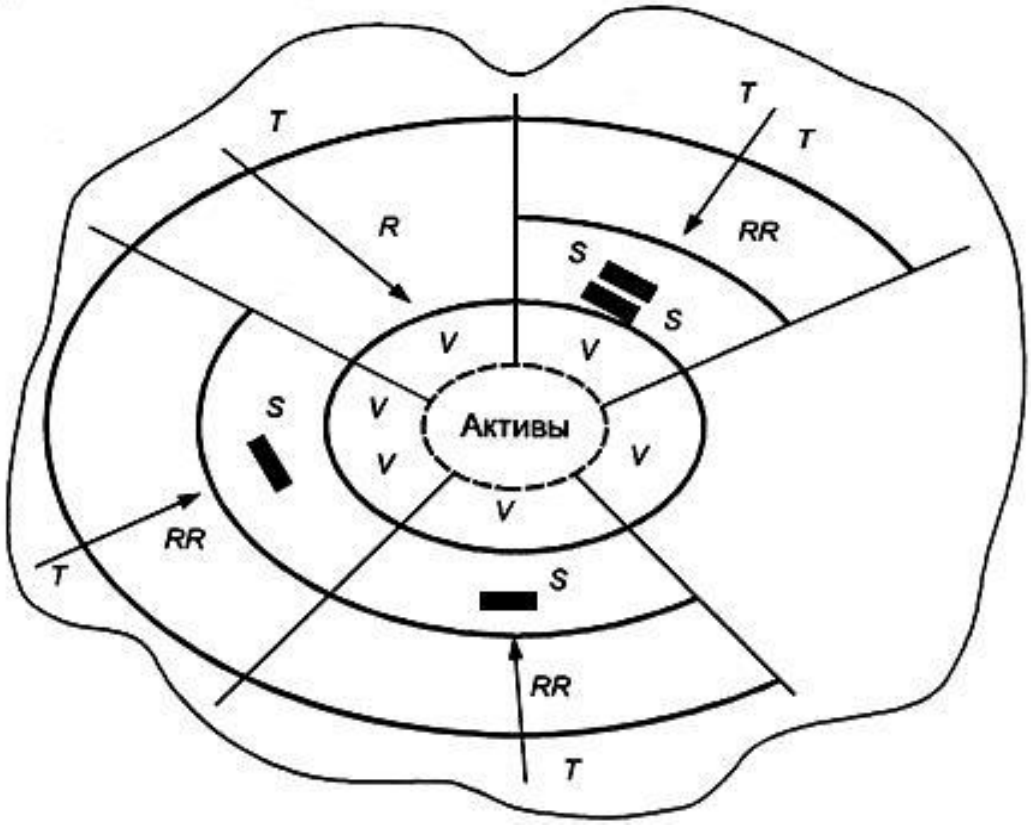
Определение уровней защищенности ПДн в зависимости от типа актуальных угроз в соответствии с Постановлением Правительства Российской Федерации «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» №1119 от 01 ноября 2012, показано на рис. 4:

Тип ИСПДн	Категории субъектов	Количество субъектов	Тип актуальных угроз		
			1 тип	2 тип	3 тип
ИСПДн-С	Не сотрудников	Более 100 000	УЗ 1	УЗ 1	УЗ 2
		Менее чем 100 000	УЗ 1	УЗ 2	УЗ 3
	Сотрудников	Более 100 000	УЗ 1	УЗ 2	УЗ 3
		Менее чем 100 000	УЗ 1	УЗ 2	УЗ 3
ИСПДн-Б	Не сотрудников	Более 100 000	УЗ 1	УЗ 2	УЗ 3
		Менее чем 100 000	УЗ 1	УЗ 2	УЗ 3
	Сотрудников	Более 100 000	УЗ 1	УЗ 2	УЗ 3
		Менее чем 100 000	УЗ 1	УЗ 2	УЗ 3
ИСПДн-И	Не сотрудников	Более 100 000	УЗ 1	УЗ 2	УЗ 3
		Менее чем 100 000	УЗ 1	УЗ 3	УЗ 4
	Сотрудников	Более 100 000	УЗ 1	УЗ 3	УЗ 4
		Менее чем 100 000	УЗ 1	УЗ 3	УЗ 4
ИСПДн-О	Не сотрудников	Более 100 000	УЗ 2	УЗ 2	УЗ 4
		Менее чем 100 000	УЗ 2	УЗ 3	УЗ 4
	Сотрудников	Более 100 000	УЗ 2	УЗ 3	УЗ 4
		Менее чем 100 000	УЗ 2	УЗ 3	УЗ 4

Рисунок 4. Определение уровней защищенности ПДн

7.2 Взаимосвязь компонентов безопасности

Взаимосвязь компонентов безопасности в соответствии с ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных систем, показана на рис. 5:



R – риск; RR – остаточный риск; S – защитная мера; T – угроза; V – уязвимость актива

Рисунок 5. Определение уровней защищенности ПДн

7.3 Пример классификации активов

Пример классификации активов в соответствии с ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных систем, показан далее.

Активы включают в себя (но не ограничиваются):

1. материальные активы (например, вычислительные средства, средства связи, здания);
2. информацию (данные) (например, документы, базы данных);
3. программное обеспечение;
4. способность производить продукт или предоставлять услугу;
5. людей;
6. нематериальные ресурсы (например, престиж фирмы, репутацию).

7.4 Принципы проведения аудита

Принципы проведения аудита в соответствии с ГОСТ Р ИСО 19011-2012 Руководящие указания по аудиту систем менеджмента, включают:

а) Целостность (integrity) - основа профессионализма. Аудиторам и лицам, управляющим программой аудита, следует:

- выполнять свою работу честно, старательно и ответственно;
- соблюдать и относиться с уважением к любым применяемым законодательным требованиям;
- демонстрировать свою техническую компетентность при выполнении работы;
- выполнять свою работу беспристрастно, оставаться честными и непредвзятыми во всех своих действиях;
- быть осмотрительными и не поддаваться каким-либо влияниям, которые могут оказывать на их суждения или выводы другие заинтересованные стороны.

b) Беспристрастность (fair presentation) - обязательство предоставлять правдивые и точные отчеты. В выводах (наблюдениях) аудитов, заключениях по результатам аудита и отчетах следует отражать деятельность по аудиту правдиво и точно. Неразрешенные проблемы и разногласия между группой по аудиту и проверяемой организацией следует отражать в отчетах. Обмен информацией должен быть правдивым, точным, объективным, своевременным, понятным и полным.

c) Профессиональная осмотрительность (due professional care) - прилежание и умение принимать правильные решения при проведении аудита. Профессиональная осмотрительность аудиторов соответствует важности выполняемого задания и доверительности со стороны заказчика аудита и других заинтересованных сторон. Важным фактором при выполнении аудиторами своей работы с профессиональной осмотрительностью является способность принимать обоснованные решения в любых ситуациях в ходе выполнения аудита.

d) Конфиденциальность (confidentiality) - сохранность информации.

Аудиторы должны проявлять осмотрительность при использовании и обеспечении защиты и сохранности информации, полученной ими при проведении аудита. Информация, полученная при проведении аудита, не должна использоваться ненадлежащим образом для получения личной выгоды аудитором или заказчиком аудита или способом, наносящим ущерб законным интересам проверяемой организации. Соблюдение этого принципа включает в себя

надлежащее обращение с конфиденциальной или классифицированной информацией.

e) Независимость (independence) - основа беспристрастности и объективности заключений по результатам аудита. Аудиторы должны быть независимыми от проверяемой деятельности во всех случаях, когда это осуществимо, и всегда выполнять свою работу таким образом, чтобы быть свободными от предубеждений и конфликта интересов. При проведении внутренних аудитов аудиторы должны быть независимыми от руководителей подразделений и направлений деятельности, которые они проверяют. Аудиторы должны сохранять объективное мнение в течение всего процесса аудита для обеспечения того, чтобы выводы и заключения аудита основывались только на свидетельствах аудита.

Для малых организаций может оказаться невозможным обеспечение независимости внутренних аудиторов от проверяемой ими деятельности, однако следует предпринять все возможные усилия для исключения какой бы то ни было заинтересованности и обеспечения объективного рассмотрения проверяемой деятельности.

f) Подход, основанный на свидетельстве (evidence-based approach), - разумная основа для достижения надежных и воспроизводимых заключений аудита в процессе систематического аудита. Свидетельство аудита должно быть проверяемым. Оно основано на выборках имеющейся информации, поскольку аудит осуществляется в ограниченный период времени и с ограниченными ресурсами. Соответствующее использование выборок тесно связано с доверием, с которым относятся к заключениям по результатам аудита.

7.5 Применяемые методы проведения аудита

Применяемые методы проведения аудита в соответствии с ГОСТ Р ИСО 19011-2012 Руководящие указания по аудиту систем менеджмента, включают:

Степень вовлеченности между организацией-аудитором и проверяемой организацией	Местоположение аудитора	
	на местах производственной деятельности организации	на расстоянии
Взаимодействие людей	Проведение интервью. Заполнение проверочных листов и вопросников с участием персонала проверяемой организации. Проведение анализа документации с участием представителей проверяемой организации. Осуществление представительных выборок	Через интерактивные средства коммуникации: - проведение интервью; - заполнение проверочных листов и вопросников; - проведение анализа документации с участием представителей проверяемой организации
Без взаимодействия людей	Проведение анализа документации (например, анализ записей, данных). Наблюдение за выполнением работы. Посещение производственных подразделений. Заполнение проверочных листов. Осуществление представительных выборок	Проведение анализа документации (например, анализ записей, данных). Наблюдение за выполнением работы с помощью технических средств, обеспечивающих надзор за производственной деятельностью, с учетом социальных и юридических требований. Анализ данных

Лившиц Илья Иосифович

Нормативно-методическое обеспечение информационной безопасности

Учебно-методическое пособие

В авторской редакции
Редакционно-издательский отдел Университета ИТМО
Зав. РИО Н.Ф. Гусарова
Подписано к печати
Заказ №
Тираж
Отпечатано на ризографе

Редакционно-издательский отдел
Университета ИТМО
197101, Санкт-Петербург, Кронверкский пр., 49, литер А