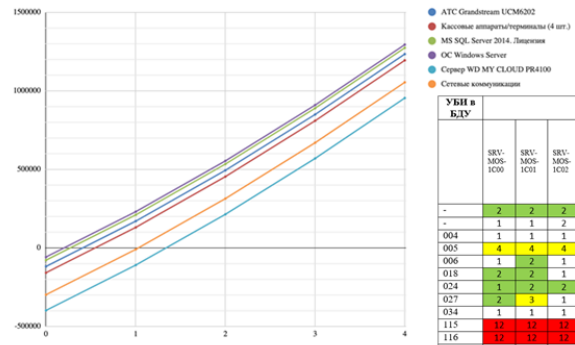
УНИВЕРСИТЕТ ИТМО

И.И. Лившиц

ЭКОНОМИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Компонент \ Критерий	Стоимость (Лицензия)	Наличие резерва	Наличие сервисного договора (По Лицензии компонента)	Обучение персонала (Курсы)
1С: Бюджетирование;	670 000 руб.	-	+	+
1С:УПП	400 000 руб.	-	+	+
Outlook	200 000 руб	+	+	-
Интернет-браузер	Бесплатный	+	-	-
MS Excel;	2000 руб	+	-	+
MS Word	2000 руб	+	-	-
AdobeReader	1800 руб	+	-	-
AutoCAD	100 000 руб	-	+	+
Общая оценка (балльная)	**4**	**3**	**2**	**4**



t	Прибыль (CI)	Затраты (CO)	CF	$(1+R)^{(1-t)}$	CF ^{disc}	NPV
0	0	380 000	-380 000	1,00	-380 000	-380 000
1	50 000	0	50 000	0,91	45 500	-305 137
2	100 000	0	100 000	0,83	83 000	-237 833
3	150 000	0	150 000	0,75	112 500	-112 208
4	200 000	0	200 000	0,68	136 000	-135 734
5	250 000	0	250 000	0,62	155 000	-87 138
6	300 000	0	300 000	0,57	171 000	-49 000
7	350 000	0	350 000	0,51	178 500	-22 020
8	400 000	0	400 000	0,47	188 000	5 535

УБИ в БДУ	Активы															
	SRV-MOS-1C00	SRV-MOS-1C01	SRV-MOS-1C02	SRV-MOS-1C03	SRV-MOS-MAIL01	SRV-MOS-MAIL02	SRV-MOS-SQL01	SRV-MOS-SQL02	SRV-MOS-SQL03	ARM-MOS-UKM01	ARM-MOS-UKM02	ARM-MOS-UKM03	ARM-MOS-UKM04	ARM-MOS-UKM05	ARM-MOS-UKM06	ARM-MOS-UKM07
-	2	2	2	2	2	2	2	2	2	4	4	4	4	4	4	4
-	1	1	2	1	1	1	1	1	1	2	2	4	2	2	2	2
004	1	1	1	1	1	1	3	1	1	4	4	4	4	4	4	4
005	4	4	4	4	4	4	4	4	4	6	9	9	9	9	9	6
006	1	2	1	1	1	2	1	1	1	1	1	1	1	1	3	1
018	2	2	1	1	1	1	1	1	1	4	4	4	4	4	4	4
024	1	2	2	1	6	6	2	1	1	4	4	4	4	4	4	4
027	2	3	1	2	1	1	1	1	1	1	1	2	2	1	1	1
034	1	1	1	1	1	1	1	1	1	2	2	2	2	4	2	2
115	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12
116	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12
123	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1
139	1	1	1	1	3	1	1	1	1	1	1	1	1	3	1	1
152	2	3	2	2	2	2	2	2	2	2	2	2	2	2	2	2
157	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3
193	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6

Санкт-Петербург
2021

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

УНИВЕРСИТЕТ ИТМО

И.И. Лившиц

ЭКОНОМИЧЕСКОЕ 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

Санкт-Петербург
2021

Лившиц И.И., Экономическое обеспечение информационной безопасности – СПб: Университет ИТМО, 2021. – 69 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 «Экономика защиты информации» 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 (национальные ГОСТ Р и международные стандарты ISO, ISO/IEC). Эти дополнительные материалы могут быть изучены как в рамках курса «Экономика защиты информации», так и в качестве дополнительных материалов при самообучении.

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

Содержание

Ведение

Учебно-методическое пособие «Экономика защиты информации» предназначено для помощи обучающимся по направлению подготовки 10.04.01 «Информационная безопасность» (магистратура). Актуальность данного пособия определяется постоянным ростом числа инцидентов информационной безопасности 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 национальных (ГОСТ Р) и международных (ISO, ISO/IEC) стандартов.

Содержание данного пособия полностью соответствует установленным учебным задачам и рабочей программе по дисциплине ЭД1.13 «Экономика защиты информации». Применение в учебном процессе данного пособия обеспечит достижение планируемых результатов обучения, в частности: знать основы разработки программных и программно-аппаратных средств для систем защиты информации автоматизированных систем, основы применения экономических методов при разработке систем и средств защиты информации (СЗИ) и применять методы расчета экономической эффективности при разработке систем и средств защиты информации, а также рассчитывать экономические затраты на разработку программно-аппаратных средств защиты информации (ПК-С1.2.1), знать требования к программным и программно-аппаратным средствам защиты информации, уметь планировать экономические затраты на разработку, тестирование, введение в эксплуатацию и поддержание средства защиты информации (ПК-С1.2.2).

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 «Экономика защиты информации» и включает актуальные статьи на русском и английских языках, опубликованные в журналах ВАК и/или Scopus / Web Of Science. В приложении приведены дополнительные материалы (национальные ГОСТ Р и международные

стандарты ISO, ISO/IEC). Эти дополнительные материалы могут быть изучены как в рамках курса «Экономика защиты информации», 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 при внесении новых изменений в действующую редакцию каждого упомянутого НМД. Кроме того, применяемая логика выполнения лабораторных работ позволяет перейти к другим разделам, например: управлению требованиями ИБ, управлению инцидентами информационной безопасности (ИБ), управлению рисками ИБ, управлению активами, обеспечению соответствия и пр.

Рекомендуется выполнение лабораторных работ в последовательности их изложения в данном учебно-методическом пособии, поскольку это 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

АРМ	–	Автоматизированное рабочее место
ГОСТ	–	Государственный стандарт
ГОСТ Р		Государственный стандарт России
ИБ	–	Информационная безопасность
ИСПДн		Информационная система персональных данных
КЗ	–	Контролируема зона
НДВ	–	Недекларируемые возможности
ПДн	–	Персональные данные
ПО	–	Программное обеспечение
СЗИ	–	Средство защиты информации
СКЗИ	–	Средство криптографической защиты информации
СМИБ	–	Система менеджмента информационной безопасности
ФСТЭК России		Федеральная служба технического и экспортного контроля России
ISO (ИСО)	–	International Organization for Standardization (Международная организация по стандартизации)
IEC (МЭК)	–	International Electrotechnical Committee (Международная электротехническая комиссия)
NPV (ЧДД)	–	Net Present Value (Чистый дисконтируемый доход)

Основная часть

1 Лабораторная работа № 1. «Определение активов предприятия»

1.1 Цель работы

Освоение навыков применения НМД при идентификации активов для определения необходимости и целесообразности создания системы защиты.

1.2 Задачи

В Лабораторной работе №1 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
- ГОСТ Р ИСО 22301-2014 Системы менеджмента непрерывности бизнеса. Общие требования;
- ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология (ИТ). Методы и средства обеспечения безопасности.
- ГОСТ Р 55.0.02-2014/ИСО 55001:2014 Управление активами. Национальная система стандартов. Системы менеджмента

Задача 2: Идентификация активов предприятия для определения необходимости и целесообразности создания системы защиты.

1.3 Ход работы

1. Идентификация бизнес-процессов предприятия
   Основные бизнес-процессы предприятия показаны на рис. 1.

Рисунок 1. – Основные бизнес-процессы предприятия

В группу процессов «Закупки и обеспечение производства» (О1) входят:

- Планирование закупок основного и вспомогательного сырья;
- Закупки основного и вспомогательного сырья;
- Отчетность и контроль по закупкам основного и вспомогательного сырья.

В группу процессов «Производство» (О2) входят:

- Согласование планов производства продукции;
- Планирование кооперации между заводами/цехами;
- Контроль и анализ состояния производства, обеспеченности ресурсами;
- Утверждение плановых норм расхода и выхода продукции;
- Контроль и анализ соблюдения технологических параметров;
- Контроль и анализ продукции, выходах годного и видах брака.

В группу процессов «Продажи» (О3) входят:

- Формирование годового плана продаж;
- Ежемесячное оперативное планирование продаж (на квартал);
- Организация поставки продукции клиенту;
- Привлечение новых клиентов;
- Еженедельный контроль обеспечения заявок на отгрузку продукции;
- Ежедневный контроль обеспечения заявок на отгрузку продукции;
- Формирование аналитической отчетности по продажам.

2. Оценка важности бизнес-процессов

Оценка важности бизнес-процессов предприятия выполняется по нескольким критериям, например:

- Допустимый простой (в днях);
- Влияние на прибыль;
- Проблемы с поставками;
- Влияние на производство;
- Влияние на связь с поставщиками и партнерами;
- Репутационные потери.

Оценка важности по критериям переводится в баллы по следующей схеме:

- Допустимый простой:
  - 1 день – 5 баллов;
  - 2-3 дня – 4 балла;
  - 4-5 дня – 3 балла;
  - 6 дней – 2 балла;
  - 7 и более – 1 балл.

– Влияние на прибыль:
  - 200 тыс. руб. и более – 10 баллов;
  - от 160 тыс. руб. до 200 тыс. руб. – 8 баллов;
  - от 120 тыс. руб. до 160 тыс. руб. – 6 баллов;
  - от 80 тыс. руб. до 120 тыс. руб. – 4 балла;
  - от 40 тыс. руб. до 80 тыс. руб. – 2 балла;
  - 40 тыс. руб. и менее – 1 балл.

– Задержки с поставками:
  - На 1 день – 5 баллов;
  - На 2-3 дня – 4 балла;
  - На 4-5 дня – 3 балла;
  - На 6 дней – 2 балла;
  - На 7 и более – 1 балл.

– Влияние на производство:
  - 250 тыс. руб. и более – 10 баллов;
  - от 200 тыс. руб. до 250 тыс. руб. – 8 баллов;
  - от 150 тыс. руб. до 200 тыс. руб. – 6 баллов;
  - от 100 тыс. руб. до 150 тыс. руб. – 4 балла;
  - от 50 тыс. руб. до 100 тыс. руб. – 2 балла;
  - 50 тыс. руб. и менее – 1 балл.

– Влияние на связь с поставщиками и партнерами
  - Рассчитывается по шкале от 1 до 10, где 1 – поставщики и партнеры остаются, 10 – поставщики и партнеры уходят в течение года

– Репутационные потери
  - Рассчитываются по шкале от 1 до 10, где 1 – негативных статей в СМИ нет, 10 – негативные статьи в СМИ появляются каждую неделю.

Результаты балльной оценки важности бизнес-процессов представлены в Табл.1.

Таблица 1 – Оценка важности бизнес-процессов предприятия

Бизнес-процесс / **Критерий**	**О1**	**О2**	**О3**
Допустимый простой (в часах)	5	5	4
Влияние на прибыль	8	10	8
Задержки с поставками	5	5	3
Влияние на производство	4	10	2
Влияние на связь с поставщиками и партнерами	1	2	3
Репутационные потери	1	1	3
Общая оценка (балльная)	**24**	**32**	**23**

3. Оценка влияния основных компонент ИТ-инфраструктуры

Основные компоненты ИТ-инфраструктуры предприятия:

- 1С:УПП;
- MS Excel;
- AdobeReader;
- Электронная почта (MS Exchange - Outlook);
- MS Word;
- AutoCAD;
- 1С Бюджетирование;
- MS Office;
- Интернет-браузер (Browser Yandex).

Оценка влияния основных компонент ИТ-инфраструктуры переводится в баллы по схеме:

- Стоимость (Лицензии):
  - Свыше 600 тыс. руб. – 7 баллов;
  - от 600 тыс. руб. до 500 тыс. руб. – 6 баллов;
  - от 500 тыс. руб. до 400 тыс. руб. – 5 баллов;
  - от 400 тыс. руб. до 300 тыс. руб. – 4 балла;
  - от 300 тыс. руб. до 200 тыс. руб. – 3 балла;
  - от 200 тыс. руб. до 100 тыс. руб. – 2 балла;
  - от 100 тыс. руб. и менее – 1 балл;
  - Бесплатно – 0 баллов.

- Наличие:
  - «+» (да) – 1 балл;
  - «-» (нет) – 0 баллов;

Результаты балльной оценки важности основных компонент ИТ-инфраструктуры представлены в Табл. 2.

Таблица 2 – Основные компоненты ИТ-инфраструктуры предприятия

Критерий / **Компонент**	Стоимость (Лицензия)	Наличие резерва	Наличие сервисного договора (По Лицензии компонента)	Обучение персонала (Курсы)	Общая оценка (балльная)
1С: Бюджетирование	670 000 руб.	-	+	+	**9**
1С:УПП	400 000 руб.	-	+	+	**6**
Outlook	200 000 руб.	+	+	-	**4**
Интернет-браузер	Бесплатный	+	-	-	**1**
MS Excel	200 000 руб.	+	-	+	**4**
MS Word	200 000 руб.	+	-	-	**3**
AdobeReader	180 000 руб.	+	-	-	**3**
AutoCAD	100 000 руб.	-	+	+	**3**

4. Оценка влияния ИТ-компонент на бизнес-процессы

Данные компоненты могут оказать влияние на различные бизнес-процессы предприятия:

В группу процессов «Закупки и обеспечение производства» (О1) входят:

- Планирование закупок основного и вспомогательного сырья;
- Закупки основного и вспомогательного сырья;
- Отчетность и контроль по закупкам основного и вспомогательного сырья.

Для автоматизации данных процессов используются следующие информационные системы:

- 1С:УПП;
- MS Excel;
- AdobeReader;
- Электронная почта.

В группу процессов «Производство» (О2) входят:

- Согласование планов производства продукции;
- Планирование кооперации между заводами/цехами;

- Контроль и анализ состояния производства, обеспеченности ресурсами;
- Утверждение плановых норм расхода и выходов годного;
- Контроль и анализ соблюдения технологических параметров;
- Контроль и анализ продукции, выходах годного и видах брака.

Для автоматизации данных процессов используются следующие информационные системы:

- 1С:УПП;
- MS Excel;
- MS Word;
- Электронная почта;
- AutoCAD;
- 1С Бюджетирование.

В группу процессов «Продажи» (О3) входят:

- Формирование годового плана продаж;
- Ежемесячное оперативное планирование продаж (на квартал);
- Организация поставки продукции клиенту;
- Привлечение новых клиентов;
- Еженедельный контроль обеспечения заявок на отгрузку продукции
- Ежедневный контроль обеспечения заявок на отгрузку продукции
- Формирование аналитической отчетности по продажам

Для автоматизации данных процессов используются следующие информационные системы:

- 1С: Бюджетирование;
- 1С:УПП;
- MS Office;
- AdobeReader
- Электронная почта;
- Интернет-браузер.

Оценка влияния компонент ИТ-инфраструктуры переводится в баллы по следующей схеме:

- Наличие:
    - «+» (да) – 1 балл;
    - «-» (нет) – 0 баллов;

Результаты балльной оценки важности влияния компонент ИТ-инфраструктуры на бизнес-процессы представлены в Табл. 3.

Таблица 3 – Влияние основных ИТ-компонент на бизнес-процессы предприятия

Бизнес-процесс / **Компонент**	**О1**	**О2**	**О3**
1С: Бюджетирование		+	+
1С:УПП	+	+	+
Outlook	+	+	+
Интернет-браузеры			+
MS Excel	+	+	
MS Word		+	+
AdobeReader	+		+
AutoCAD		+	
Общая оценка (балльная)	**4**	**6**	**6**

Зависимость компонент ИТ-инфраструктуры от активов представлена в Табл. 4.

Таблица 4 – Зависимость компонент ИТ-инфраструктуры от активов предприятия

Компонент / **Актив**	1С: Бюджетирование	1С: УПП	Exchange Outlook	MS Office (MS Excel, MS Word)	AutoCAD	Adobe Reader
Сервер SRV-MOS-1C00	+					
Сервер SRV-MOS-1C01	+					
Сервер SRV-MOS-1C02		+				
Сервер SRV-MOS-1C03		+				
Сервер SRV-MOS-MAIL01			+			
Сервер SRV-MOS-MAIL02			+			
Сервер SRV-MOS-SQL01			+	+		
Сервер SRV-MOS-SQL02			+	+		
Сервер			+	+		

SRV-MOS-SQL03						
АРМ ARM-MOS-UKM01		+		+	+	+
АРМ ARM-MOS-UKM02		+		+	+	+
АРМ ARM-MOS-UKM03				+		
АРМ ARM-MOS-UKM04	+	+	+	+		
АРМ ARM-MOS-UKM05				+		+
АРМ ARM-MOS-UKM06			+		+	
АРМ ARM-MOS-UKM07	+	+	+	+		+

5. Категорирование активов предприятия

Категорирование активов предприятия происходит по таким критериям:

- С – стоимость актива (в руб.);
- Д – доступность актива на рынке;
- СВ – сложность восстановления (установки актива) после выхода из строя/замены актива;
- Н – необходимость в постоянной технической поддержке квалифицированным персоналом.

Оценка активов переводится в баллы по следующей схеме:

- Стоимость (С):
  - 250 тыс. руб. и более – 10 баллов;
  - от 200 тыс. руб. до 250 тыс. руб. – 8 баллов;
  - от 150 тыс. руб. до 200 тыс. руб. – 6 баллов;
  - от 100 тыс. руб. до 150 тыс. руб. – 4 балла;
  - от 50 тыс. руб. до 100 тыс. руб. – 2 балла;
  - 50 тыс. руб. и менее – 1 балл.

- Наличие (Д, СВ, Н):
  - «+» (да) – 1 балл;
  - «-» (нет) – 0 баллов;

Результаты категорирования активов предприятия представлены в Табл. 5.

Таблица 5 – Категорирование активов предприятия

Критерий / Актив	С	Д	СВ	Н	Общая оценка (балльная)
Сервер SRV-MOS-1C00	200 000	+	+	+	11
Сервер SRV-MOS-1C01	200 000	+	+	+	11
Сервер SRV-MOS-1C02	240 000	+	+	+	11
Сервер SRV-MOS-1C03	240 000	+	+	+	11
Сервер SRV-MOS-MAIL01	145 000	+	+	+	7
Сервер SRV-MOS-MAIL02	145 000	+	+	+	7
Сервер SRV-MOS-SQL01	120 000	-	+	+	6
Сервер SRV-MOS-SQL02	120 000	-	+	+	6
Сервер SRV-MOS-SQL03	120 000	-	+	+	6
АРМ ARM-MOS-UKM01	35 000	+	-	-	3
АРМ ARM-MOS-UKM02	35 000	-	-	-	3
АРМ ARM-MOS-UKM03	40 000	+	-	-	3
АРМ ARM-MOS-UKM04	50 000	-	+	+	4
АРМ ARM-MOS-UKM05	20 000	+	-	-	3
АРМ ARM-MOS-UKM06	30 000	+	-	-	3
АРМ ARM-MOS-UKM07	70 000	-	+	+	4

6. Необходимость и целесообразность защиты активов

Необходимость и целесообразность защиты активов определяется на основании сопоставления общей оценки (балльной), полученной ранее, и критериальной оценки.

Для данной Лабораторной работы критериальная оценка для всех типов активов (серверов и АРМов) устанавливается равной 6.

Результаты оценки необходимости и целесообразности защиты активов предприятия представлены в Табл. 6.

Таблица 6 – Необходимость и целесообразность защиты активов предприятия

Параметр / Актив	Общая оценка (балльная)	Критериальная оценка	Решение	Примечание
Сервера				
Сервер SRV-MOS-1C00	11	6	Необходимо	Необходимо обеспечить защиту актива, оказывает

Сервер SRV-MOS-1C01	11	6	Необходимо	критическое влияние на бизнес- процессы предприятия
Сервер SRV-MOS-1C02	11	6	Необходимо	
Сервер SRV-MOS-1C03	11	6	Необходимо	
Сервер SRV-MOS-MAIL01	7	6	Необходимо	
Сервер SRV-MOS-MAIL02	7	6	Необходимо	
Сервер SRV-MOS-SQL01	6	6	Рекомендуется	Рекомендуется обеспечить защиту актива, оказывает важное влияние на бизнес-процессы предприятия
Сервер SRV-MOS-SQL02	6	6	Рекомендуется	
Сервер SRV-MOS-SQL03	6	6	Рекомендуется	
АРМ				
АРМ ARM-MOS-UKM01	3	6	Нецелесообразно	Обеспечение защиты актива нецелесообразно, так как влияние актива на бизнес-процессы минимально
АРМ ARM-MOS-UKM02	3	6	Нецелесообразно	
АРМ ARM-MOS-UKM03	3	6	Нецелесообразно	
АРМ ARM-MOS-UKM04	4	6	Нецелесообразно	
АРМ ARM-MOS-UKM05	3	6	Нецелесообразно	
АРМ ARM-MOS-UKM06	3	6	Нецелесообразно	
АРМ ARM-MOS-UKM07	4	6	Нецелесообразно	

1.4 Ошибки

1. При оценке необходимости и целесообразности защиты активов предприятия ошибочно может быть принято решение об отнесении всех активов к защищаемым. Это может привести к неоправданному увеличению стоимости всего проекта защиты (множество СЗИ и/или СКЗИ) в дальнейшем. Необходимо изменить критерии оценки или ввести раздельные критерии для разных типов активов.
2. При оценке необходимости и целесообразности защиты активов предприятия ошибочно может быть принято решение об отнесении конкретного актива к

защищаемым, даже несмотря на низкую общую балльную оценку. Это может привести к нарушению логики всего проекта защиты в дальнейшем и сложностям при проведении аудита. Необходимо изменить критерии оценки или ввести раздельные критерии для разных типов активов.

3. Завышение или занижение критерия, что может существенно повлиять на соответствие доли активов и средств защиты (СЗИ и/или СКЗИ) и привести к экономическому дисбалансу.

1.5 Вывод по лабораторной работе

В ходе лабораторной работы были изучены нормативно-методические документы, в соответствии с которыми выполняется идентификация и категорирование активов для последующего определения необходимости и целесообразности создания системы защиты.

2 Лабораторная работа № 2. «Оценка базового риска информационной безопасности»

2.1 Цель работы

Освоение навыков применения нормативно-методической документации по определению и оценке базовых рисков ИБ для идентифицированных активов 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
- ГОСТ Р ИСО 31000-2018 Менеджмент риска. Принципы и руководство
- ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности;
- ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.
- ГОСТ Р ИСО/МЭК 18045-2013 Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий;

Задача 2: Определение и оценка базовых рисков ИБ идентифицированных активов предприятия.

2.3 Ход работы

1. Определение необходимости и целесообразности защиты активов предприятия

Этот результат может быть получен из Лабораторной работы № 1 (Табл. 6), либо иначе, например, по итогам аудита ИБ на предприятии. Входные данные с учетом данных о владельце актива и аудиторе актива представлены в Табл. 1. Роль владельца актива крайне важна для определения базовых рисков каждого конкретного актива.

Таблица 1 – Необходимость и целесообразность защиты активов предприятия

Параметр / **Актив**	Общая оценка (балльная)	Критериальная оценка	Решение	Примечание	Владелец / Аудитор
Сервера					
Сервер SRV-MOS-1C00	11	6	Необходимо	Необходимо обеспечить защиту актива, оказывает критическое влияние на бизнес- процессы предприятия	А / К
Сервер SRV-MOS-1C01	11	6	Необходимо		
Сервер SRV-MOS-1C02	11	6	Необходимо		
Сервер SRV-MOS-1C03	11	6	Необходимо		
Сервер SRV-MOS-MAIL01	7	6	Необходимо		Б / К
Сервер SRV-MOS-MAIL02	7	6	Необходимо		
Сервер SRV-MOS-SQL01	6	6	Рекомендуется	Рекомендуется обеспечить защиту актива, оказывает важное влияние на бизнес- процессы предприятия	В / К
Сервер SRV-MOS-SQL02	6	6	Рекомендуется		
Сервер SRV-MOS-SQL03	6	6	Рекомендуется		
АРМ					
АРМ ARM-MOS-UKM01	3	6	Нецелесообразно	Обеспечение защиты актива нецелесообразно, так как влияние актива на бизнес-процессы минимально	Г / К
АРМ ARM-MOS-UKM02	3	6	Нецелесообразно		
АРМ ARM-MOS-UKM03	3	6	Нецелесообразно		
АРМ ARM-MOS-UKM04	4	6	Нецелесообразно		
АРМ ARM-MOS-UKM05	3	6	Нецелесообразно		
АРМ ARM-MOS-UKM06	3	6	Нецелесообразно		

АРМ ARM-MOS-UKM07	4	6	Нецелесообразно		

2. Идентификация существующих мер защиты на предприятии

Существующие технические меры защиты на предприятии:

- На всех серверах и АРМ установлен антивирус Kaspersky Endpoint Security 11 (KES), антивирусные базы обновляются из базы данных через сеть Интернет.
- На серверном оборудовании используются средства резервного копирования Veeam Backup & Recovery 11 (Veeam).
- Для серверного оборудования (в ЦОД) используются источники бесперебойного питания (ИБП).

Существующие организационные меры защиты на предприятии:

- На окнах первого этажа имеются решетки и жалюзи;
- Серверная (ЦОД) располагается на 3 этаже, помещение без окон;
- Для входа в серверную необходим электронный пропуск.
- Рабочие места сотрудников отделены перегородками;
- Территория предприятия ограждена забором;
- Проводится проверка и контроль проносимых вещей / оборудования;
- Кабельные линии проложены в защищенных лотках или закрытых кабель-каналах.

Реестр активов предприятия и существующих мер защиты представлен в Табл. 2.

Таблица 2. Реестр активов предприятия и существующих мер защиты

Меры защиты / **Актив**	Технические	Организационные	Общая стоимость мер защиты, руб.	Владелец актива / Аудитор
Сервер SRV-MOS-1C00	ИБП	– Находится в КЗ; – Защита прокладки кабелей; – Отдельное помещение (ЦОД); – Контроль переносимых вещей/оборудов	80 000	А / К
	KES			
	Veeam			
Сервер SRV-MOS-1C01	ИБП		80 000	
	KES			
	Veeam			
Сервер SRV-MOS-1C02	ИБП		80 000	
	KES			
	Veeam			
Сервер	ИБП		80 000	

SRV-MOS-1C03	KES	ания		
	Veeam			
Сервер SRV-MOS-MAIL01	ИБП		80 000	Б / К
	KES			
	Veeam			
Сервер SRV-MOS-MAIL02	ИБП		80 000	
	KES			
	Veeam			
Сервер SRV-MOS-SQL01	ИБП		80 000	В / К
	KES			
	Veeam			
Сервер SRV-MOS-SQL02	ИБП		80 000	
	KES			
	Veeam			
Сервер SRV-MOS-SQL03	ИБП		80 000	
	KES			
	Veeam			
АРМ ARM-MOS-UKM01	KES	– Все АРМ находятся в КЗ; – Перегородки между сотрудниками; – Контроль переносимых вещей/оборудования; – На первых этажах здания используются жалюзи и решетки на окнах	19 000	Г / К
АРМ ARM-MOS-UKM02	KES		19 000	
АРМ ARM-MOS-UKM03	KES		19 000	
АРМ ARM-MOS-UKM04	KES		19 000	
АРМ ARM-MOS-UKM05	KES		19 000	
АРМ ARM-MOS-UKM06	KES		19 000	
АРМ ARM-MOS-UKM07	KES		19 000	

3. Оценка уязвимости активов для перечня угроз

Оценка уязвимостей активов для перечня угроз выполняется по количественной методике, где для каждой угрозы из БДУ ФСТЭК России определяется по шкале по отношению конфиденциальности, целостности и/или доступности:

- 1 – низкая степень уязвимость;
- 2 – средняя степень уязвимости;

- 3 – высокая степень уязвимости.

Результаты оценки уязвимости активов предприятия представлены в Табл. 3.

Таблица 3. Оценка уязвимости актива для перечня угроз

№ УБИ в БДУ	**Активы**															
	SRV-MOS-1C00	SRV-MOS-1C01	SRV-MOS-1C02	SRV-MOS-1C03	SRV-MOS-MAIL01	SRV-MOS-MAIL02	SRV-MOS-SQL01	SRV-MOS-SQL02	SRV-MOS-SQL03	ARM-MOS-UKM01	ARM-MOS-UKM02	ARM-MOS-UKM03	ARM-MOS-UKM04	ARM-MOS-UKM05	ARM-MOS-UKM06	ARM-MOS-UKM07
-	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2
-	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2
004	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2
005	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3
006	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1
018	2	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2
024	1	1	1	1	2	1	2	1	1	2	2	2	2	2	2	2
027	2	3	1	2	1	1	1	1	1	1	1	1	1	1	1	1
034	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1
115	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
116	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
123	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
139	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
152	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
157	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
193	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2

4. Оценка вероятности реализации угроз

Оценка вероятности реализации угроз выполняется по количественной методике, где для каждой угрозы из БДУ ФСТЭК России определяется по шкале:

- 1 – угроза существует, но не встречалась в рассматриваемой инфраструктуре предприятия;
- 2 – угроза возникает в рассматриваемой инфраструктуре предприятия 2–3 раза в год;
- 3 – угроза была реализована в рассматриваемой системе;
- 4 – угроза возникает 2–3 раза в год в рассматриваемой системе.

Оценка вероятности реализации угроз для активов предприятия представлена в Табл. 4.

Таблица 4. Оценка вероятности реализации угроз ИБ

№ УБИ в БДУ	**Активы**															
	SRV-MOS-1C00	SRV-MOS-1C01	SRV-MOS-1C02	SRV-MOS-1C03	SRV-MOS-MAIL01	SRV-MOS-MAIL02	SRV-MOS-SQL01	SRV-MOS-SQL02	SRV-MOS-SQL03	ARM-MOS-UKM01	ARM-MOS-UKM02	ARM-MOS-UKM03	ARM-MOS-UKM04	ARM-MOS-UKM05	ARM-MOS-UKM06	ARM-MOS-UKM07
-	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
-	1	1	2	1	1	1	1	1	1	1	1	2	1	1	1	1
004	1	1	1	1	1	1	3	1	1	2	2	2	2	2	2	2
005	2	2	2	2	2	2	2	2	2	2	3	3	3	3	3	2
006	1	1	1	1	1	2	1	1	1	1	1	1	1	1	3	1
018	1	2	1	1	1	1	1	1	1	2	2	2	2	2	2	2
024	1	2	2	1	1	1	1	1	1	2	2	2	2	2	2	2
027	1	1	1	1	1	1	1	1	1	1	1	2	2	1	1	1
034	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2
115	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4

№ УБИ в БДУ	Активы															
116	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
123	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1
139	1	1	1	1	3	1	1	1	1	1	1	1	1	3	1	1
152	2	3	2	2	2	2	2	2	2	2	2	2	2	2	2	2
157	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3
193	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3

5. Определение базового риска ИБ

Для определения риска информационной безопасности воспользуемся формулой (1)

$$R = P_i * V_j \ , \qquad (1)$$

где:

Vi – величина уязвимости;

Pj – вероятность реализации угрозы.

Для определения значения риска применим численные и вербальные значения, указанные в Табл.5

Таблица 5. Определение значений риска

Значение риска, R	Вербальная величина риска	Стратегия
1 – 2	Приемлемый	Не требует внимания. Не требует обработки
3 – 5	Низкий	Требует внимания. Требует запланированных действий
6 – 8	Средний	Требует внимания. Требует срочных действий
9 – 12	Высокий	Требует внимания. Требует немедленных действий

Расчет всех базовых рисков с учетом ранее определенных значений уязвимостей и вероятностей реализации угроз представлен в Табл. 6.

Таблица 6. Оценка базовых рисков

№ УБИ в БДУ	Активы															
	SRV-MOS-1C00	SRV-MOS-1C01	SRV-MOS-1C02	SRV-MOS-1C03	SRV-MOS-MAIL01	SRV-MOS-MAIL02	SRV-MOS-SQL01	SRV-MOS-SQL02	SRV-MOS-SQL03	ARM-MOS-UKM01	ARM-MOS-UKM02	ARM-MOS-UKM03	ARM-MOS-UKM04	ARM-MOS-UKM05	ARM-MOS-UKM06	ARM-MOS-UKM07
-	2	2	2	2	2	2	2	2	2	4	4	4	4	4	4	4
-	1	1	2	1	1	1	1	1	1	2	2	4	2	2	2	2
004	1	1	1	1	1	1	3	1	1	4	4	4	4	4	4	4
005	4	4	4	4	4	4	4	4	4	6	9	9	9	9	9	6
006	1	2	1	1	1	2	1	1	1	1	1	1	1	1	3	1
018	2	2	1	1	1	1	1	1	1	4	4	4	4	4	4	4
024	1	2	2	1	6	6	2	1	1	4	4	4	4	4	4	4
027	2	3	1	2	1	1	1	1	1	1	1	2	2	1	1	1
034	1	1	1	1	1	1	1	1	1	2	2	2	2	4	2	2
115	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12
116	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12
123	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1
139	1	1	1	1	3	1	1	1	1	1	1	1	1	3	1	1
152	2	3	2	2	2	2	2	2	2	2	2	2	2	2	2	2
157	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3
193	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6

2.4 Дополнительные варианты

Оценка риска по последствиям может ранжироваться следующим образом (см. Табл. 7).

Таблица 7. Оценка риска по последствиям

Низкая	Средняя	Высокая
– Незначительное снижение показателей функционирования (<10%) системы; – Редкие кратковременные задержки в работе системы; – Увеличение объема технического обслуживания и ремонта системы; – Незначительный рост затрат и/или срыв сроков (<10%) программы; – Требуется заметно усилить работу по анализу и контролю	– Значительное снижение показателей функционирования (10-50%) системы; – Кратковременные выходы системы из строя; – Увеличение затрат на сопровождение системы; – Значительный рост затрат и/или срыв сроков (10-30%) программы; – Требуется очень серьезно усилить работу по анализу и контролю	– Резкое снижение показателей функционирования (50-100%) системы или полное прекращение основной деятельности, отказ в обслуживании; – Серьезные проблемы с безопасностью системы; – Резкий рост затрат и/или срыв сроков (30-70%) программы

Оценка риска по вероятности может ранжироваться следующим образом (см. Табл. 8).

Таблица 8. Оценка риска по вероятности

Низкая	Средняя	Высокая
– Вероятность возникновения является незначительной. Практически невозможно предположить, что подобный фактор может возникнуть.	– Вероятность возникновения находится на среднем уровне. Условия для этого могут реально и неожиданно возникнуть.	– Вероятность возникновения является очень высокой. Условия обязательно возникают на протяжении достаточно продолжительного промежутка времени (обычно в условиях нормальной эксплуатации).

2.5 Ошибки

1. При категорировании мер защиты может быть принято ошибочное решение, например: в качестве организационных рассматриваются меры для физической безопасности (обеспечение прочности внутренних стен зданий, использование кодовых дверных замков, систем пожаротушения и охранных служб).
2. При оценивании рисков может быть принято ошибочное решение, когда неверно определяются экспертным путем вероятности реализации угроз (например, некоторые данные замалчиваются в процессе внутреннего аудита), или при неверном определении степени значимости актива и способности конкретной угрозы нанести значительный (критический ущерб) при эксплуатации уязвимостей.

2.6 Вывод по лабораторной работе

В ходе лабораторной работы были изучены НМД, в соответствии с которыми выполняется оценка (идентификация, анализ и оценивание) базовых рисков ИБ для идентифицированных активов предприятия.

3 Лабораторная работа № 3. «Выбор дополнительных мер защиты»

3.1 Цель работы

Освоение навыков применения нормативно-методической документации для обоснования выбора дополнительных мер защиты с учетом оценки базовых рисков ИБ идентифицированных активов предприятия.

3.2 Задачи

В Лабораторной работе №3 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
- ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования
- ГОСТ Р ИСО 31000-2018 Менеджмент риска. Принципы и руководство
- ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.

Задача 2: Формирование обоснования выбора дополнительных мер защиты с учетом оценки базовых рисков ИБ идентифицированных активов предприятия.

3.3 Ход работы

1. Определение базовых рисков для активов

Этот результат может быть получен из Лабораторной работы № 2 (Таблица 6), либо иначе, например, по итогам аудита ИБ на предприятии. Входные данные с учетом оценки рисков и стратегии обработки рисков в зависимости от степени их критичности представлены в Табл. 1.

Таблица 1 – Оценка базовых рисков

№ УБИ в БДУ	Активы															
	SRV-MOS-1C00	SRV-MOS-1C01	SRV-MOS-1C02	SRV-MOS-1C03	SRV-MOS-MAIL01	SRV-MOS-MAIL02	SRV-MOS-SQL01	SRV-MOS-SQL02	SRV-MOS-SQL03	ARM-MOS-UKM01	ARM-MOS-UKM02	ARM-MOS-UKM03	ARM-MOS-UKM04	ARM-MOS-UKM05	ARM-MOS-UKM06	ARM-MOS-UKM07
-	2	2	2	2	2	2	2	2	2	4	4	4	4	4	4	4
-	1	1	2	1	1	1	1	1	1	2	2	4	2	2	2	2
004	1	1	1	1	1	1	3	1	1	4	4	4	4	4	4	4
005	4	4	4	4	4	4	4	4	4	6	9	9	9	9	9	6
006	1	2	1	1	1	2	1	1	1	1	1	1	1	1	3	1
018	2	2	1	1	1	1	1	1	1	4	4	4	4	4	4	4
024	1	2	2	1	6	6	2	1	1	4	4	4	4	4	4	4
027	2	3	1	2	1	1	1	1	1	1	1	2	2	1	1	1
034	1	1	1	1	1	1	1	1	1	2	2	2	2	4	2	2
115	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12
116	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12
123	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1
139	1	1	1	1	3	1	1	1	1	1	1	1	1	3	1	1
152	2	3	2	2	2	2	2	2	2	2	2	2	2	2	2	2
157	2	2	2	2	2	2	2	2	2	3	3	3	3	3	3	3
193	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6

2. Методика выбора дополнительных мер защиты

Методика выбора дополнительных мер защиты активов строится на основе ранее определенной степени критичности значения базового риска:

1. В первую очередь необходимо устранить риски с оценкой от 9 до 12;
2. Устранение рисков с оценкой от 6 до 8;
3. Устранение рисков с оценкой от 3 до 5;

4. Оценка от 1 до 2 является приемлемой и не требует дополнительных мер защиты.

Для устранения/снижения базовых рисков, намеченных к обработке, необходимо реализовать меры защиты, представленные в Таблице 2.

Таблица 2. Реестр активов предприятия и дополнительных мер защиты

Дополнительные меры защиты / **Актив**	Вариант	Технические	Организационные	Общая стоимость дополнительных мер защиты, руб.
Сервера				
Сервер SRV-MOS-1C00 Сервер SRV-MOS-1C01 Сервер SRV-MOS-1C02 Сервер SRV-MOS-1C03 Сервер SRV-MOS-MAIL01 Сервер SRV-MOS-MAIL02 Сервер SRV-MOS-SQL01 Сервер SRV-MOS-SQL02 Сервер SRV-MOS-SQL03	1	Мониторинг и периодический анализ состояния защищенности посредством применения специализированных программных или программно-аппаратных комплексов; – MaxPatrol 8	Регламентация управления доступом к ТС и ПО	500 000
	2	Обнаружение вредоносной активности, а также действия вредоносного ПО путем применения программно-аппаратных комплексов антивирусной защиты и обнаружения вторжений; – ViPNet IDS HW	Регламентация и контроль использования мобильных АРМ	375 000
	3	Применение средства межсетевого	Обслуживание и ремонт ТС осуществляют	295 700

		экранирования для защиты сегмента сетевого трафика; – VipNet Coordinator HW	уполномоченные лица	
	4	Управление доступом в ОС ТС путем применения специализированных средств защиты от НСД; – ViPNet SafePoint	Помещения, в которых установлены ТС, не остаются открытыми. Ведётся журнал. Ключи выдаются под роспись.	333 000
	5	Регистрация и учет событий сетевой инфраструктуры путем применения специализированных СрЗИ – MaxPatrol SIEM	Работники, не имеющие допуска к ТС, находятся в помещении с установленными ТС только в присутствии уполномоченных сотрудников СБ	400 000
АРМ				
АРМ ARM-MOS-UKM01 АРМ ARM-MOS-UKM02 АРМ ARM-MOS-UKM03 АРМ ARM-MOS-UKM04 АРМ ARM-MOS-UKM05 АРМ ARM-MOS-UKM06	6	Для доступа к BIOS используется аутентификация на основе пароля	Регламентация управления доступом к ТС и ПО, регламент и учет применения МН	50 000
	7	Резервирование системного ПО и прикладного ПО	Обслуживание и ремонт ТС осуществляют уполномоченные лица	100 000
	8	Управление доступом в ОС ТС путем применения специализированных средств защиты от НСД; – ViPNet SafePoint	Помещения, в которых установлены ТС, не остаются открытыми. Ведётся журнал. Ключи выдаются	259 000

АРМ ARM-MOS-UKM07			под роспись.	
	9	Регистрация и учет событий сетевой инфраструктуры путем применения специализированных СрЗИ – MaxPatrol SIEM	Расположение экранов мониторов и ТС обработки графической информации, способом, исключающим просмотр отображаемой информации	400 000
	10	Применение средства межсетевого экранирования для защиты сегмента сетевого трафика; – VipNet Coordinator HW	Регламент и инструктаж использования ТС и ПО для сотрудников	295 700

3. Определение остаточных рисков для активов

На основании выбора дополнительных мер защиты и критериев в соответствии с принятыми критериями оценки рисков (Лабораторная работа №2, Таблица 5) выполним пересчет базового риска и определим остаточный риск для каждого актива. Результаты представлены в Таблице 3.

Таблица 3. Переоценка рисков ИБ для активов предприятия с учетом дополнительных мер защиты

Критерии / **Актив**	Вариант	№ УБИ в БДУ	Остаточный риск	Владелец актива / Аудитор
Сервера				
Сервер SRV-MOS-1C00	1	005, 004, 018, 116, 193	Таблица 4	А / К Б / К В / К
Сервер SRV-MOS-1C01	2	024, 115, 116	Таблица 5	
Сервер SRV-MOS-1C02 Сервер SRV-MOS-1C03	3	005, 004, 018, 034, 115, 139, 157, 193	Таблица 6	
Сервер SRV-MOS-MAIL01	4	018, 024, 027, 115, 116, 152	Таблица 7	

Сервер SRV-MOS-MAIL02 Сервер SRV-MOS-SQL01 Сервер SRV-MOS-SQL02 Сервер SRV-MOS-SQL03	5	027, 115, 116, 139	Таблица 8	
АРМ				
АРМ ARM-MOS-UKM01	6	005, 004, 018	Таблица 9	Г / К
	7	139, 157	Таблица 10	
АРМ ARM-MOS-UKM02	8	018, 024, 027, 139, 152, 193	Таблица 11	
АРМ ARM-MOS-UKM03	9	027, 115, 116, 139	Таблица 12	
АРМ ARM-MOS-UKM04 АРМ ARM-MOS-UKM05 АРМ ARM-MOS-UKM06 АРМ ARM-MOS-UKM07	10	018, 034, 115	Таблица 13	

4. Дополнительные варианты

Представляется хорошей практикой графическое сопоставление оценок базового и остаточного риска (см. Рис. 1). Этот пример показывает для каждого актива текущее значение базового риска по количественной шкале слева (от 0 до 7) и значение остаточного риска, полученное после внедрения дополнительных мер защиты и переоценки базового риска. Важно принять во внимание, что иногда даже при принятии значительного перечня дополнительных мер защиты значение базового риска не удаётся изменить и, вероятно, владелец актива должен принять решение о допустимом текущем уровне данного риска.

Рисунок 1. – Сопоставление базового и остаточного риска для каждого актива

Также представляется хорошей практикой графическое сопоставление количества УБИ, которые могут быть успешно обработаны на уровне оценок базового риска, до приемлемого уровня остаточного риска (см. Рис. 2). Этот пример показывает для каждого актива текущее количество угроз (например, от 1 до 6), которые были определены на уровне оценок базового риска, и количество угроз после применения дополнительных мер защиты – на уровне остаточных рисков (остались только две угрозы 5 и 6). Важно принять во внимание, что иногда даже при принятии значительного перечня дополнительных мер защиты часть угроз не удается полностью привести с уровня базового риска к приемлемому уровню остаточного риска. Вероятно, владелец актива должен принять решение о допустимом текущем уровне данного риска.

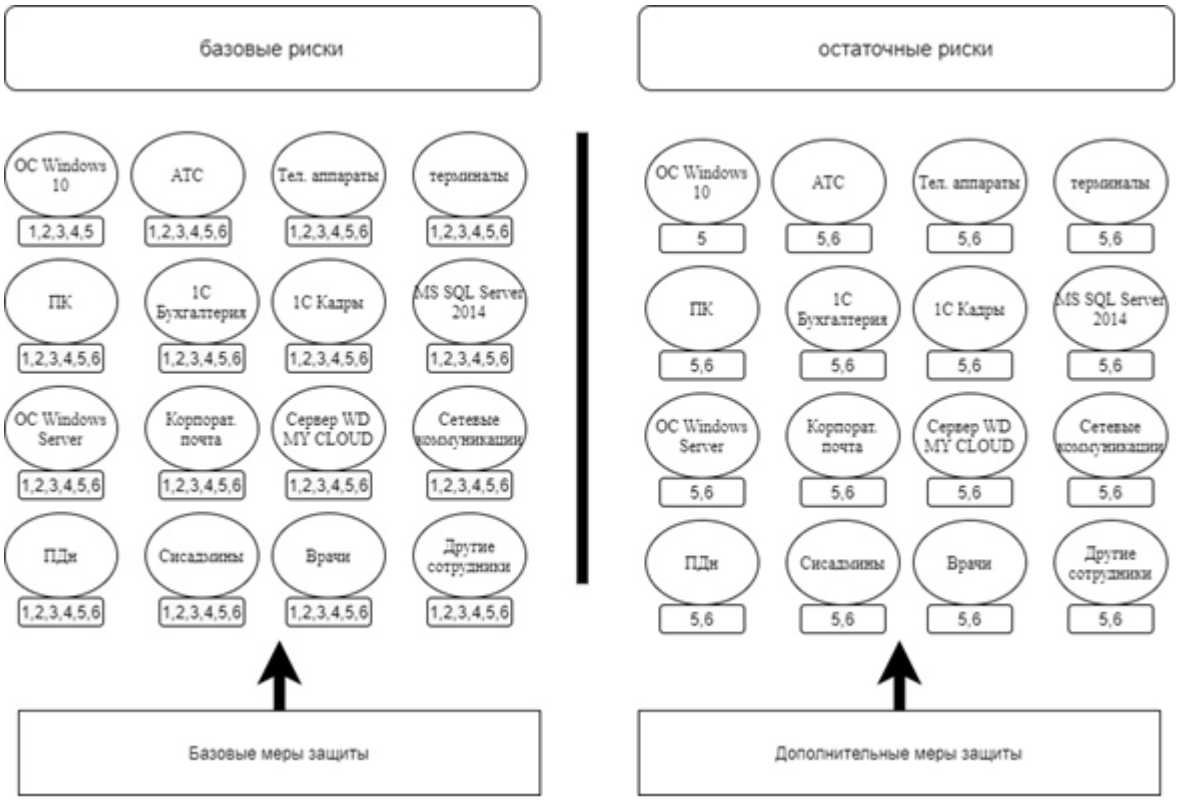


Рисунок 2. – Сопоставление базового и остаточного риска по перечню угроз

Также представляется хорошей практикой графическое сопоставление оценок базового риска, уровня остаточного риска при выборе различных вариантов выбора мер защиты (см. Рис. 3). Этот пример показывает для каждого актива значение базового риска (как начальной точки при обработке) и нескольких вариантов остаточного риска, достигаемого при выборе разных защитных мер. Важно принять во внимание, что иногда различные варианты выбора нескольких дополнительных мер защиты могут давать весьма различающиеся результаты и получать, соответственно, различные уровни остаточного риска. Вероятно, владелец актива должен принять решение о допустимом текущем уровне данного риска – например, как наименьший по приемлемому значению остаточного риска.

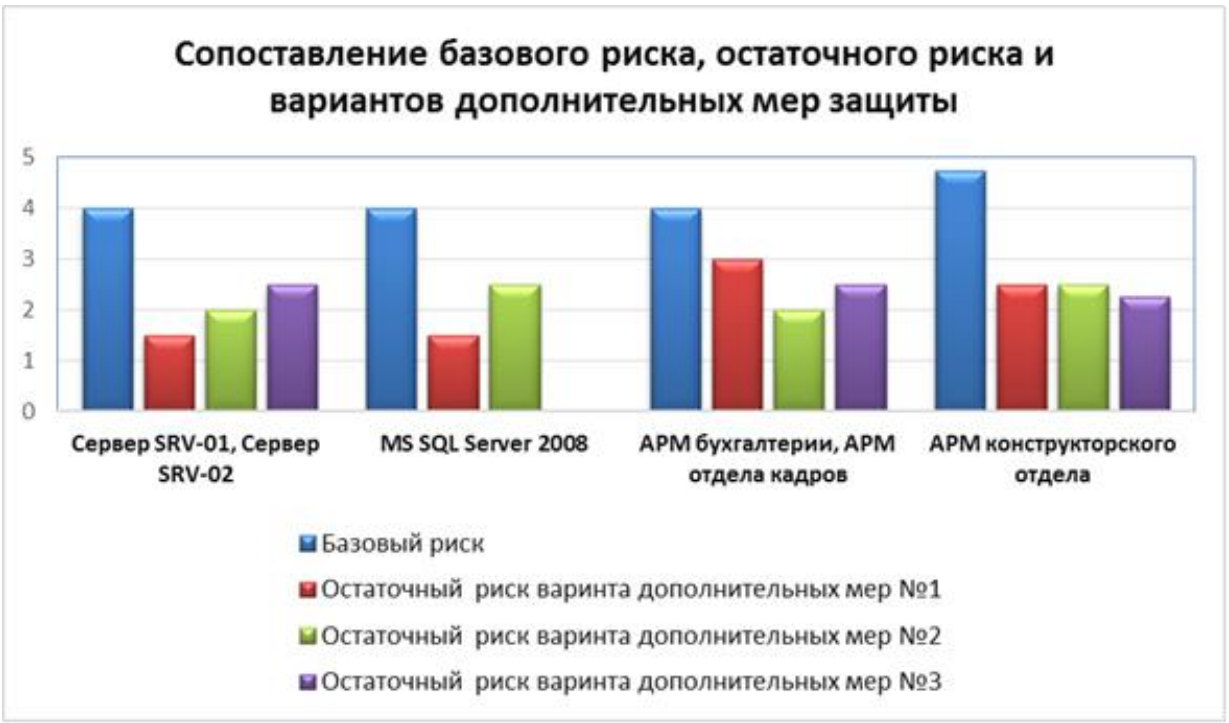


Рисунок 3. – Сопоставление базового и остаточного риска по вариантам дополнительных мер

5. Расчеты вариантов применения дополнительных мер защиты

В Таблице 3 представлено 10 вариантов выбора дополнительных мер защиты. Детальный расчет остаточного риска для каждого актива по каждому варианту представлен соответственно в Таблице 4 – Таблице 13. К верхней строке каждой таблицы показан перечень угроз, в отношении которых предпринимаются дополнительные меры защиты.

Таблица 4. Расчет остаточного риска для варианта 1

005, 004, 018, 116, 193									
№ УБИ в БДУ	SRV-MOS-1C00	SRV-MOS-1C01	SRV-MOS-1C02	SRV-MOS-1C03	SRV-MOS-MAIL01	SRV-MOS-MAIL02	SRV-MOS-SQL01	SRV-MOS-SQL02	SRV-MOS-SQL03
-	2	2	2	2	2	2	2	2	2
-	1	1	2	1	1	1	1	1	1
004	1	1	1	1	1	1	2	1	1

005	2	2	2	2	2	2	2	2	2
006	1	2	1	1	1	2	1	1	1
018	2	2	1	1	1	1	1	1	1
024	1	2	2	1	6	6	2	1	1
027	2	3	1	2	1	1	1	1	1
034	1	1	1	1	1	1	1	1	1
115	12	12	12	12	12	12	12	12	12
116	6	6	6	6	6	6	6	6	6
123	1	1	1	1	1	1	1	1	1
139	1	1	1	1	3	1	1	1	1
152	2	3	2	2	2	2	2	2	2
157	2	2	2	2	2	2	2	2	2
193	3	3	3	3	3	3	3	3	3

Таблица 5. Расчет остаточного риска для варианта 2

024, 115, 116									
№ УБИ в БДУ	SRV-MOS-1C00	SRV-MOS-1C01	SRV-MOS-1C02	SRV-MOS-1C03	SRV-MOS-MAIL01	SRV-MOS-MAIL02	SRV-MOS-SQL01	SRV-MOS-SQL02	SRV-MOS-SQL03
-	2	2	2	2	2	2	2	2	2
-	1	1	2	1	1	1	1	1	1
004	1	1	1	1	1	1	3	1	1
005	4	4	4	4	4	4	4	4	4
006	1	2	1	1	1	2	1	1	1
018	2	2	1	1	1	1	1	1	1
024	1	2	2	1	3	3	2	1	1
027	2	3	1	2	1	1	1	1	1
034	1	1	1	1	1	1	1	1	1
115	6	6	6	6	6	6	6	6	6
116	6	6	6	6	6	6	6	6	6
123	1	1	1	1	1	1	1	1	1
139	1	1	1	1	3	1	1	1	1
152	2	3	2	2	2	2	2	2	2
157	2	2	2	2	2	2	2	2	2

024, 115, 116									
№ УБИ в БДУ	SRV-MOS-1C00	SRV-MOS-1C01	SRV-MOS-1C02	SRV-MOS-1C03	SRV-MOS-MAIL01	SRV-MOS-MAIL02	SRV-MOS-SQL01	SRV-MOS-SQL02	SRV-MOS-SQL03
193	6	6	6	6	6	6	6	6	6

Таблица 6. Расчет остаточного риска для варианта 3

005, 004, 018, 034, 115, 139, 157, 193									
№ УБИ в БДУ	SRV-MOS-1C00	SRV-MOS-1C01	SRV-MOS-1C02	SRV-MOS-1C03	SRV-MOS-MAIL01	SRV-MOS-MAIL02	SRV-MOS-SQL01	SRV-MOS-SQL02	SRV-MOS-SQL03
-	2	2	2	2	2	2	2	2	2
-	1	1	2	1	1	1	1	1	1
004	1	1	1	1	1	1	2	1	1
005	2	2	2	2	2	2	2	2	2
006	1	2	1	1	1	2	1	1	1
018	2	2	1	1	1	1	1	1	1
024	1	2	2	1	6	6	2	1	1
027	2	3	1	2	1	1	1	1	1
034	1	1	1	1	1	1	1	1	1
115	6	6	6	6	6	6	6	6	6
116	12	12	12	12	12	12	12	12	12
123	1	1	1	1	1	1	1	1	1
139	1	1	1	1	3	1	1	1	1
152	2	3	2	2	2	2	2	2	2
157	2	2	2	2	2	2	2	2	2
193	4	4	4	4	4	4	4	4	4

Таблица 7. Расчет остаточного риска для варианта 4

018, 024, 027, 115, 116, 152									
№ УБИ в БДУ	SRV-MOS-1C00	SRV-MOS-1C01	SRV-MOS-1C02	SRV-MOS-1C03	SRV-MOS-MAIL01	SRV-MOS-MAIL02	SRV-MOS-SQL01	SRV-MOS-SQL02	SRV-MOS-SQL03
-	2	2	2	2	2	2	2	2	2
-	1	1	2	1	1	1	1	1	1
004	1	1	1	1	1	1	3	1	1
005	4	4	4	4	4	4	4	4	4
006	1	2	1	1	1	2	1	1	1
018	2	2	1	1	1	1	1	1	1
024	1	2	2	1	4	4	2	1	1
027	2	2	1	2	1	1	1	1	1
034	1	1	1	1	1	1	1	1	1
115	6	6	6	6	6	6	6	6	6
116	6	6	6	6	6	6	6	6	6
123	1	1	1	1	1	1	1	1	1
139	1	1	1	1	3	1	1	1	1
152	2	2	2	2	2	2	2	2	2
157	2	2	2	2	2	2	2	2	2
193	6	6	6	6	6	6	6	6	6

Таблица 8. Расчет остаточного риска для варианта 5

027, 115, 116, 139									
№ УБИ в БДУ	SRV-MOS-1C00	SRV-MOS-1C01	SRV-MOS-1C02	SRV-MOS-1C03	SRV-MOS-MAIL01	SRV-MOS-MAIL02	SRV-MOS-SQL01	SRV-MOS-SQL02	SRV-MOS-SQL03
-	2	2	2	2	2	2	2	2	2
-	1	1	2	1	1	1	1	1	1

027, 115, 116, 139									
№ УБИ в БДУ	SRV-MOS-1C00	SRV-MOS-1C01	SRV-MOS-1C02	SRV-MOS-1C03	SRV-MOS-MAIL01	SRV-MOS-MAIL02	SRV-MOS-SQL01	SRV-MOS-SQL02	SRV-MOS-SQL03
004	1	1	1	1	1	1	3	1	1
005	4	4	4	4	4	4	4	4	4
006	1	2	1	1	1	2	1	1	1
018	2	2	1	1	1	1	1	1	1
024	1	2	2	1	6	6	2	1	1
027	2	2	1	2	1	1	1	1	1
034	1	1	1	1	1	1	1	1	1
115	6	6	6	6	6	6	6	6	6
116	6	6	6	6	6	6	6	6	6
123	1	1	1	1	1	1	1	1	1
139	1	1	1	1	2	1	1	1	1
152	2	3	2	2	2	2	2	2	2
157	2	2	2	2	2	2	2	2	2
193	6	6	6	6	6	6	6	6	6

Таблица 9. Расчет остаточного риска для варианта 6

005, 004, 018									
№ УБИ в БДУ	SRV-MOS-1C00	SRV-MOS-1C01	SRV-MOS-1C02	SRV-MOS-1C03	SRV-MOS-MAIL01	SRV-MOS-MAIL02	SRV-MOS-SQL01	SRV-MOS-SQL02	SRV-MOS-SQL03
-	2	2	2	2	2	2	2	2	2
-	2	2	2	2	2	2	2	2	2
004	2	2	2	2	2	2	2	2	2
005	3	6	6	6	6	6	6	3	6
006	1	1	1	1	1	3	1	1	1

005, 004, 018									
№ УБИ в БДУ	SRV-MOS-1C00	SRV-MOS-1C01	SRV-MOS-1C02	SRV-MOS-1C03	SRV-MOS-MAIL01	SRV-MOS-MAIL02	SRV-MOS-SQL01	SRV-MOS-SQL02	SRV-MOS-SQL03
018	2	2	2	2	2	2	2	2	2
024	4	4	4	4	4	4	4	4	4
027	1	1	2	2	1	1	1	1	1
034	2	2	2	2	4	2	2	2	2
115	12	12	12	12	12	12	12	12	12
116	12	12	12	12	12	12	12	12	12
123	1	1	2	1	1	1	1	1	1
139	1	1	1	1	3	1	1	1	1
152	2	2	2	2	2	2	2	2	2
157	3	3	3	3	3	3	3	3	3
193	6	6	6	6	6	6	6	6	6

Таблица 10. Расчет остаточного риска для варианта 7

139, 157									
№ УБИ в БДУ	SRV-MOS-1C00	SRV-MOS-1C01	SRV-MOS-1C02	SRV-MOS-1C03	SRV-MOS-MAIL01	SRV-MOS-MAIL02	SRV-MOS-SQL01	SRV-MOS-SQL02	SRV-MOS-SQL03
-	4	4	4	4	4	4	4	4	4
-	2	2	4	2	2	2	2	2	2
004	4	4	4	4	4	4	4	4	4
005	6	9	9	9	9	9	6	6	9
006	1	1	1	1	1	3	1	1	1
018	4	4	4	4	4	4	4	4	4
024	4	4	4	4	4	4	4	4	4
027	1	1	2	2	1	1	1	1	1

139, 157									
№ УБИ в БДУ	SRV-MOS-1C00	SRV-MOS-1C01	SRV-MOS-1C02	SRV-MOS-1C03	SRV-MOS-MAIL01	SRV-MOS-MAIL02	SRV-MOS-SQL01	SRV-MOS-SQL02	SRV-MOS-SQL03
034	2	2	2	2	4	2	2	2	2
115	12	12	12	12	12	12	12	12	12
116	12	12	12	12	12	12	12	12	12
123	1	1	2	1	1	1	1	1	1
139	1	1	1	1	3	1	1	1	1
152	2	2	2	2	2	2	2	2	2
157	2	2	2	2	2	2	2	2	2
193	6	6	6	6	6	6	6	6	6

Таблица 11. Расчет остаточного риска для варианта 8

018, 024, 027, 139, 152, 193									
№ УБИ в БДУ	SRV-MOS-1C00	SRV-MOS-1C01	SRV-MOS-1C02	SRV-MOS-1C03	SRV-MOS-MAIL01	SRV-MOS-MAIL02	SRV-MOS-SQL01	SRV-MOS-SQL02	SRV-MOS-SQL03
-	2	2	2	2	2	2	2	2	2
-	2	2	4	2	2	2	2	2	2
004	4	4	4	4	4	4	4	4	4
005	6	9	9	9	9	9	6	6	9
006	1	1	1	1	1	3	1	1	1
018	2	2	2	2	2	2	2	2	2
024	2	2	2	2	2	2	2	2	2
027	1	1	2	2	1	1	1	1	1
034	2	2	2	2	4	2	2	2	2
115	12	12	12	12	12	12	12	12	12

018, 024, 027, 139, 152, 193									
№ УБИ в БДУ	SRV-MOS-1C00	SRV-MOS-1C01	SRV-MOS-1C02	SRV-MOS-1C03	SRV-MOS-MAIL01	SRV-MOS-MAIL02	SRV-MOS-SQL01	SRV-MOS-SQL02	SRV-MOS-SQL03
116	12	12	12	12	12	12	12	12	12
123	1	1	2	1	1	1	1	1	1
139	1	1	1	1	3	1	1	1	1
152	2	2	2	2	2	2	2	2	2
157	3	3	3	3	3	3	3	3	3
193	3	3	3	3	3	3	3	3	3

Таблица 12. Расчет остаточного риска для варианта 9

027, 115, 116,139									
№ УБИ в БДУ	SRV-MOS-1C00	SRV-MOS-1C01	SRV-MOS-1C02	SRV-MOS-1C03	SRV-MOS-MAIL01	SRV-MOS-MAIL02	SRV-MOS-SQL01	SRV-MOS-SQL02	SRV-MOS-SQL03
-	2	2	2	2	2	2	2	2	2
-	2	2	4	2	2	2	2	2	2
004	4	4	4	4	4	4	4	4	4
005	6	9	9	9	9	9	6	6	9
006	1	1	1	1	1	2	1	1	1
018	4	4	4	4	4	4	4	4	4
024	4	4	4	4	4	4	4	4	4
027	1	1	2	2	1	1	1	1	1
034	2	2	2	2	2	2	2	2	2
115	6	6	6	6	6	6	6	6	6
116	6	6	6	6	6	6	6	6	6
123	1	1	2	1	1	1	1	1	1
139	1	1	1	1	2	1	1	1	1

027, 115, 116,139									
№ УБИ в БДУ	SRV-MOS-1C00	SRV-MOS-1C01	SRV-MOS-1C02	SRV-MOS-1C03	SRV-MOS-MAIL01	SRV-MOS-MAIL02	SRV-MOS-SQL01	SRV-MOS-SQL02	SRV-MOS-SQL03
152	2	2	2	2	2	2	2	2	2
157	3	3	3	3	3	3	3	3	3
193	3	3	3	3	3	3	3	3	3

Таблица 13. Расчет остаточного риска для варианта 10

018, 034, 115									
№ УБИ в БДУ	SRV-MOS-1C00	SRV-MOS-1C01	SRV-MOS-1C02	SRV-MOS-1C03	SRV-MOS-MAIL01	SRV-MOS-MAIL02	SRV-MOS-SQL01	SRV-MOS-SQL02	SRV-MOS-SQL03
-	4	4	4	4	4	4	4	4	4
-	2	2	4	2	2	2	2	2	2
004	4	4	4	4	4	4	4	4	4
005	6	9	9	9	9	9	6	6	9
006	1	1	1	1	1	3	1	1	1
018	2	2	2	2	2	2	2	2	2
024	4	4	4	4	4	4	4	4	4
027	1	1	2	2	1	1	1	1	1
034	2	2	2	2	2	2	2	2	2
115	6	6	6	6	6	6	6	6	6
116	12	12	12	12	12	12	12	12	12
123	1	1	2	1	1	1	1	1	1
139	1	1	1	1	2	1	1	1	1
152	2	2	2	2	2	2	2	2	2
157	3	3	3	3	3	3	3	3	3
193	6	6	6	6	6	6	6	6	6

3.4 Ошибки

1. При обработке рисков может быть принято ошибочное решение по итогам сопоставления базовой оценки риска и критерия (см. Табл. 14). Очевидно, что в случае превышения базовой оценки риска над критерием такой риск нецелесообразно обрабатывать. В дальнейшем такая ошибка может привести к излишним финансовым издержкам при обработке рисков ИБ и возможному увеличению длительности цикла менеджмента рисков в компании;
2. При обработке рисков может быть принято последовательное второе ошибочное решение о неприемлемости риска для владельца актива и продолжении обработки риска до уровня остаточного риска. В дальнейшем такая ошибка может привести к излишним финансовым издержкам при обработке рисков ИБ и возможному увеличению длительности цикла менеджмента рисков в компании.

Таблица 14. Оценивание остаточного риска активов с учетом дополнительных мер защиты

Меры защиты / **Актив**	Риск	Базовая оценка риска	Критерий	Суждение владельца актива	Стратегия	Остаточный риск (по вариантам)	Суждение владельца актива
Сервер SRV-01, Сервер SRV-02	УБ-11	4	3	Неприемлем	Принимаем	1	Приемлем
	УБ-19	4	3	Неприемлем	Принимаем	2	Приемлем
	УБ-11	4	3	Неприемлем	Принимаем	2	Приемлем
	УБ-19	4	3	Неприемлем	Принимаем	2	Приемлем
	УБ-11	4	3	Неприемлем	Принимаем	2	Приемлем
	УБ-19	4	3	Неприемлем	Принимаем	3	Приемлем

3.5 Вывод по лабораторной работе

В ходе лабораторной работы были изучены НМД для обоснования выбора дополнительных мер защиты с учетом оценки базовых рисков ИБ для идентифицированных активов предприятия.

4 Лабораторная работа № 4. «Экономическое обоснование выбора дополнительных мер защиты»

4.1 Цель работы

Освоение навыков применения НМД для формирования экономического обоснования выбора дополнительных мер защиты с учетом оценки базовых и остаточных рисков ИБ для идентифицированных активов предприятия.

4.2 Задачи

В Лабораторной работе №4 установлены следующие задачи:

Задача 1: Ознакомление с:

- ГОСТ Р ИСО/МЭК 27000-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология
- ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования
- ГОСТ Р ИСО 31000-2018 Менеджмент риска. Принципы и руководство
- ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.

Задача 2: Формирование экономического обоснования выбора дополнительных мер защиты с учетом оценки базовых рисков ИБ идентифицированных активов предприятия.

4.3 Ход работы

1. Переоценка базовых рисков для активов предприятия по вариантам

Данные по переоценке базовых рисков для активов предприятия могут быть получены из Лабораторной работы № 3 (Таблица 3), либо иначе, например, по итогам аудита ИБ на предприятии. Входные данные по переоценке рисков ИБ для активов предприятия с учетом дополнительных мер защиты представлены в Табл.1.

Таблица 1. Переоценка рисков ИБ для активов предприятия с учетом дополнительных мер защиты

Критерии / **Актив**	Вариант	№ УБИ в БДУ	Остаточный риск	Владелец актива / Аудитор
Сервера				
Сервер SRV-MOS-1C00 Сервер SRV-MOS-1C01 Сервер SRV-MOS-1C02 Сервер SRV-MOS-1C03 Сервер SRV-MOS-MAIL01 Сервер SRV-MOS-MAIL02 Сервер SRV-MOS-SQL01 Сервер SRV-MOS-SQL02 Сервер SRV-MOS-SQL03	1	005, 004, 018, 116, 193	Таблица 4	А / К Б / К В / К
	2	024, 115, 116	Таблица 5	
	3	005, 004, 018, 034, 115, 139, 157, 193	Таблица 6	
	4	018, 024, 027, 115, 116, 152	Таблица 7	
	5	027, 115, 116, 139	Таблица 8	
АРМ				
АРМ ARM-MOS-UKM01 АРМ ARM-MOS-UKM02 АРМ ARM-MOS-UKM03 АРМ ARM-MOS-UKM04 АРМ ARM-MOS-UKM05 АРМ ARM-MOS-UKM06 АРМ ARM-MOS-UKM07	6	005, 004, 018	Таблица 9	Г / К
	7	139, 157	Таблица 10	
	8	018, 024, 027, 139, 152, 193	Таблица 11	
	9	027, 115, 116, 139	Таблица 12	
	10	018, 034, 115	Таблица 13	

2. Модель выбора наиболее экономически оптимального варианта

Данные по вариантам выбора дополнительных мер защиты для активов предприятия могут быть получены из Лабораторной работы № 3 (Таблица 2), либо

иначе, например, по итогам аудита ИБ на предприятии. Расчет и выбор наиболее экономически оптимального варианта выполнен с учетом оценки NPV (Net Present Value), обобщенные результаты представлены в Табл. 2.

Применим модель выбора наиболее экономически оптимального варианта с учетом оценки NPV (Net Present Value) или чистой текущей стоимости по каждому из рассматриваемых проектов.

Применим метод Cash Flow для сопоставления прибыли и затрат для k-варианта:

$$CF = CI - CO$$

где:

CF – денежный поток;

CI – входящий денежный поток (прибыль);

CO – исходящий денежный поток (затраты для k-варианта).

Тогда:

$$NPV = \sum_{k=0}^{n} \frac{CF_k}{(1+R)^t} - CF$$

где:

R – ставка дисконтирования;

t – количество месяцев.

Таблица 2. Данные по прибыли и затратам каждого варианта

Данные / **Вариант**	Прибыль (CI) за год, руб.	Затраты (CO) на внедрение мер защиты, руб.	Длительность проекта, мес.	Результаты подсчета
1	250 000	500 000	6	Таблица 3
2	250 000	375 000	6	Таблица 4
3	250 000	295 700	12	Таблица 5
4	250 000	333 000	5	Таблица 6
5	250 000	400 000	8	Таблица 7
6	250 000	50 000	6	Таблица 8
7	250 000	100 000	4	Таблица 9
8	250 000	259 000	4	Таблица 10
9	250 000	400 000	8	Таблица 11
10	250 000	295 700	12	Таблица 12

3. Расчеты NPV для вариантов применения дополнительных мер защиты

Детальный расчет NPV для каждого из 10 вариантов применения дополнительных мер защиты представлен соответственно в Таблице 3 – Таблице 12. В каждой таблице отдельно показана строка, в которой значение NPV становится положительным.

Таблица 3. Данные по расчету NPV для варианта 1

Вариант	t	Прибыль (CI)	Затраты (CO)	CF	$(1 + R)^{(1-t)}$	CF^{disc}	NPV
1	0	0	500000	-500000	1	-500000	-500000
	1	50000	0	50000	0,909	45454,55	-454545
	2	100000	0	100000	0,826	82644,63	-371901
	3	150000	0	150000	0,751	112697,2	-259204
	4	200000	0	200000	0,683	136602,7	-122601
	5	250000	0	250000	0,620	155230,3	32629,42
	6	300000	0	300000	0,564	169342,2	201971,6

Таблица 4. Данные по расчету NPV для варианта 2

Вариант	t	Прибыль (CI)	Затраты (CO)	CF	$(1 + R)^{(1-t)}$	CF disc	NPV
2	0	0	375000	-375000	1	-375000	-375000
	1	50000	0	50000	0,909	45454,55	-329545
	2	100000	0	100000	0,826	82644,63	-246901
	3	150000	0	150000	0,751	112697,2	-134204
	4	200000	0	200000	0,683	136602,7	2399,085
	5	250000	0	250000	0,620	155230,3	157629,4
	6	300000	0	300000	0,564	169342,2	326971,6

Таблица 5. Данные по расчету NPV для варианта 3

Вариант	t	Прибыль (CI)	Затраты (CO)	CF	$(1 + R)^{(1-t)}$	CF disc	NPV
3	0	0	297500	-297500	1	-297500	-297500
	1	50000	0	50000	0,909	45454,545	-252045,45
	2	100000	0	100000	0,826	82644,62	-169400,82
	3	150000	0	150000	0,751	112697,22	-56703,60
	4	200000	0	200000	0,683	136602,69	79899,08
	5	250000	0	250000	0,620	155230,33	235129,41
	6	300000	0	300000	0,564	169342,17	404471,59
	7	350000	0	350000	0,513	179605,34	584076,93
	8	400000	0	400000	0,466	186602,95	770679,88
	9	450000	0	450000	0,424	190843,92	961523,81

Вариант	t	Прибыль (CI)	Затраты (CO)	CF	$(1 + R)^{(1-t)}$	CF disc	NPV
	10	500000	0	500000	0,385	192771,64	1154295,46
	11	550000	0	550000	0,350	192771,64	1347067,10
	12	600000	0	600000	0,318	191178,49	1538245,59

Таблица 6. Данные по расчету NPV для варианта 4

Вариант	t	Прибыль (CI)	Затраты (CO)	CF	$(1 + R)^{(1-t)}$	CF disc	NPV
4	0	0	333000	-333000	1	-333000	-333000
	1	50000	0	50000	0,909	45454,54	-287545,45
	2	100000	0	100000	0,826	82644,62	-204900,82
	3	150000	0	150000	0,751	112697,22	-92203,60
	4	200000	0	200000	0,683	136602,69	44399,08
	5	250000	0	250000	0,620	155230,33	199629,41

Таблица 7. Данные по расчету NPV для варианта 5

Вариант	t	Прибыль (CI)	Затраты (CO)	CF	$(1 + R)^{(1-t)}$	CF disc	NPV
5	0	0	400000	-400000	1	-400000	-400000
	1	50000	0	50000	0,909	45454,54	-354545,45
	2	100000	0	100000	0,826	82644,62	-271900,82
	3	150000	0	150000	0,751	112697,22	-159203,60
	4	200000	0	200000	0,683	136602,69	-22600,91
	5	250000	0	250000	0,620	155230,33	132629,41
	6	300000	0	300000	0,564	169342,17	301971,59
	7	350000	0	350000	0,513	179605,34	481576,93
	8	400000	0	400000	0,466	186602,95	668179,88

Таблица 8. Данные по расчету NPV для варианта 6

Вариант	t	Прибыль (CI)	Затраты (CO)	CF	$(1 + R)^{(1-t)}$	CF disc	NPV
6	0	0	50000	-50000	1	-50000	-50000
	1	50000	0	50000	0,909	45454,54	-4545,45
	2	100000	0	100000	0,826	82644,62	78099,17
	3	150000	0	150000	0,751	112697,22	190796,39
	4	200000	0	200000	0,683	136602,69	327399,08
	5	250000	0	250000	0,620	155230,33	482629,41
	6	300000	0	300000	0,564	169342,17	651971,59

Таблица 9. Данные по расчету NPV для варианта 7

Вариант	t	Прибыль (CI)	Затраты (CO)	CF	$(1 + R)^{(1-t)}$	CF disc	NPV
7	0	0	100000	-100000	1	-100000	-100000
	1	50000	0	50000	0,909	45454,55	-54545,5
	2	100000	0	100000	0,826	82644,63	28099,17
	3	150000	0	150000	0,751	112697,2	140796,4
	4	200000	0	200000	0,683	136602,7	277399,1

Таблица 10. Данные по расчету NPV для варианта 8

Вариант	t	Прибыль (CI)	Затраты (CO)	CF	$(1 + R)^{(1-t)}$	CF disc	NPV
8	0	0	259000	-259000	1	-259000	-259000
	1	50000	0	50000	0,909	45454,55	-213545
	2	100000	0	100000	0,826	82644,63	-130901
	3	150000	0	150000	0,751	112697,2	-18203,6
	4	200000	0	200000	0,683	136602,7	118399,1

Таблица 11. Данные по расчету NPV для варианта 9

Вариант	t	Прибыль (CI)	Затраты (CO)	CF	$(1 + R)^{(1-t)}$	CF disc	NPV
9	0	0	400000	-400000	1	-400000	-400000
	1	50000	0	50000	0,909	45454,54	-354545,45
	2	100000	0	100000	0,826	82644,62	-271900,82
	3	150000	0	150000	0,751	112697,22	-159203,60
	4	200000	0	200000	0,683	136602,69	-22600,91
	5	250000	0	250000	0,620	155230,33	132629,41
	6	300000	0	300000	0,564	169342,17	301971,59
	7	350000	0	350000	0,513	179605,34	481576,93
	8	400000	0	400000	0,466	186602,95	668179,88

Таблица 12. Данные по расчету NPV для варианта 10

Вариант	t	Прибыль (CI)	Затраты (CO)	CF	$(1 + R)^{(1-t)}$	CF disc	NPV
10	0	0	295700	-295700	1	-295700	-295700
	1	50000	0	50000	0,909	45454,55	-250245
	2	100000	0	100000	0,826	82644,63	-167601
	3	150000	0	150000	0,751	112697,2	-54903,6
	4	200000	0	200000	0,683	136602,7	81699,08
	5	250000	0	250000	0,620	155230,3	236929,4

Вариант	t	Прибыль (CI)	Затраты (CO)	CF	(1 + R) (1-t)	CF disc	NPV
	6	300000	0	300000	0,564	169342,2	406271,6
	7	350000	0	350000	0,513	179605,3	585876,9
	8	400000	0	400000	0,466	186603	772479,9
	9	450000	0	450000	0,424	190843,9	963323,8
	10	500000	0	500000	0,385	192771,6	1156095
	11	550000	0	550000	0,350	192771,6	1348867
	12	600000	0	600000	0,318	191178,5	1540046

4. Определение оптимального варианта по критерию NPV

Общие данные для определения оптимального варианта выбора мер защиты для снижения базового риска активов предприятия по критерию NPV представлены в Таблице 13. Оптимальные варианты показаны отдельной строкой.

Таблица 13. Определение оптимального варианта по критерию NPV

Данные / **Вариант**	Длительность проекта, мес.	NPV_k, > 0, мес.	Z_k, руб.	NPV_k, руб.
1	6	5	500 000	201 971
2	6	4	375 000	326 971
3	12	4	295 700	1 538 245
4	5	4	333 000	199 629
5	8	5	400 000	668 179
6	6	2	50 000	651 971
7	4	2	100 000	277 399
8	4	4	259 000	118 399
9	8	5	400 000	668 179
10	12	4	295 700	1 540 046

4.4 Дополнительные варианты

Определение оптимального варианта по критерию NPV удобно представить в графическом виде (см. Рис. 1). График позволяет визуально оценить точку перехода значения NPV через нуль по оси абсцисс для всех вариантов независимо от длительности каждого проекта.

В случае, если каждый вариант длится равное время и состав дополнительных мер защиты касается только одного конкретного типа активов, можно получить изображение группы кривых NPV, достаточно плотно расположенных на графике (см. Рис. 2). В этом случае оптимальным вариантом также будет график, первым пересекающий ось абсцисс (NPV становится положительным).

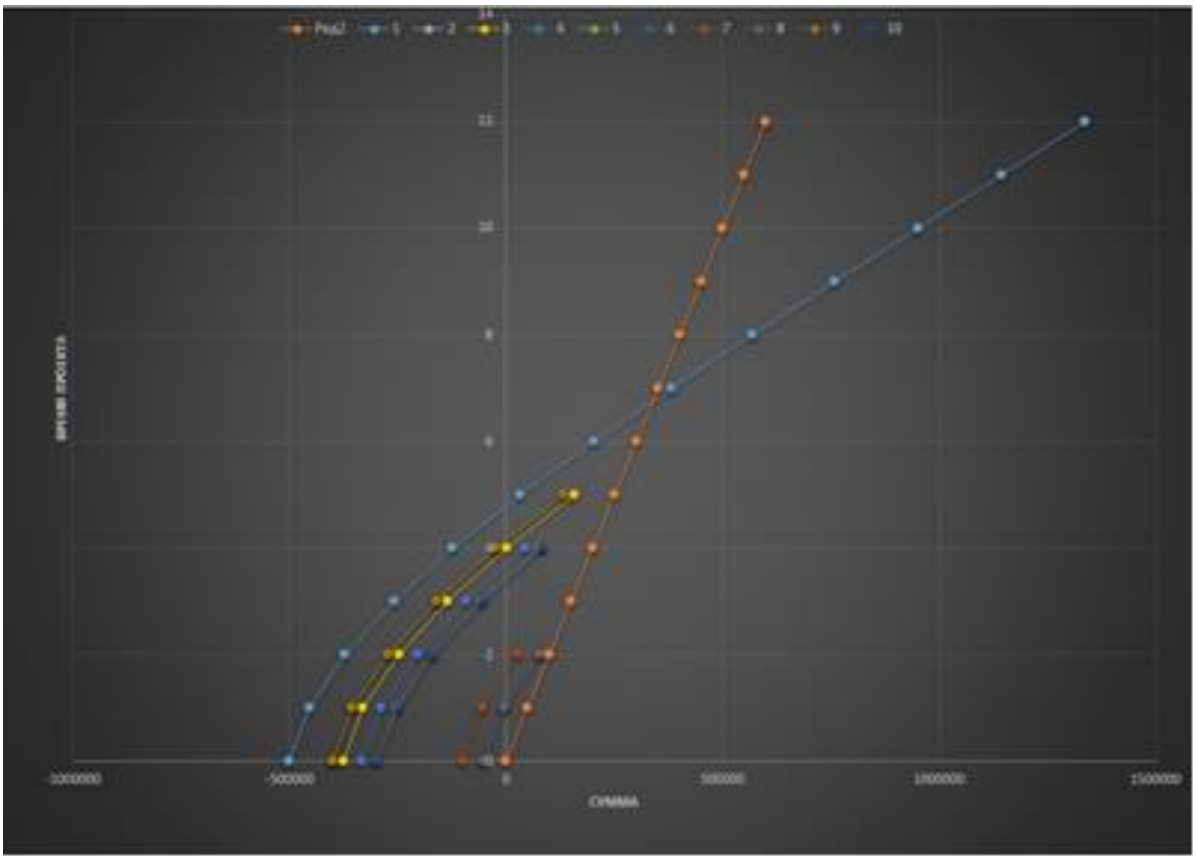


Рисунок 1. График NPV для разных вариантов

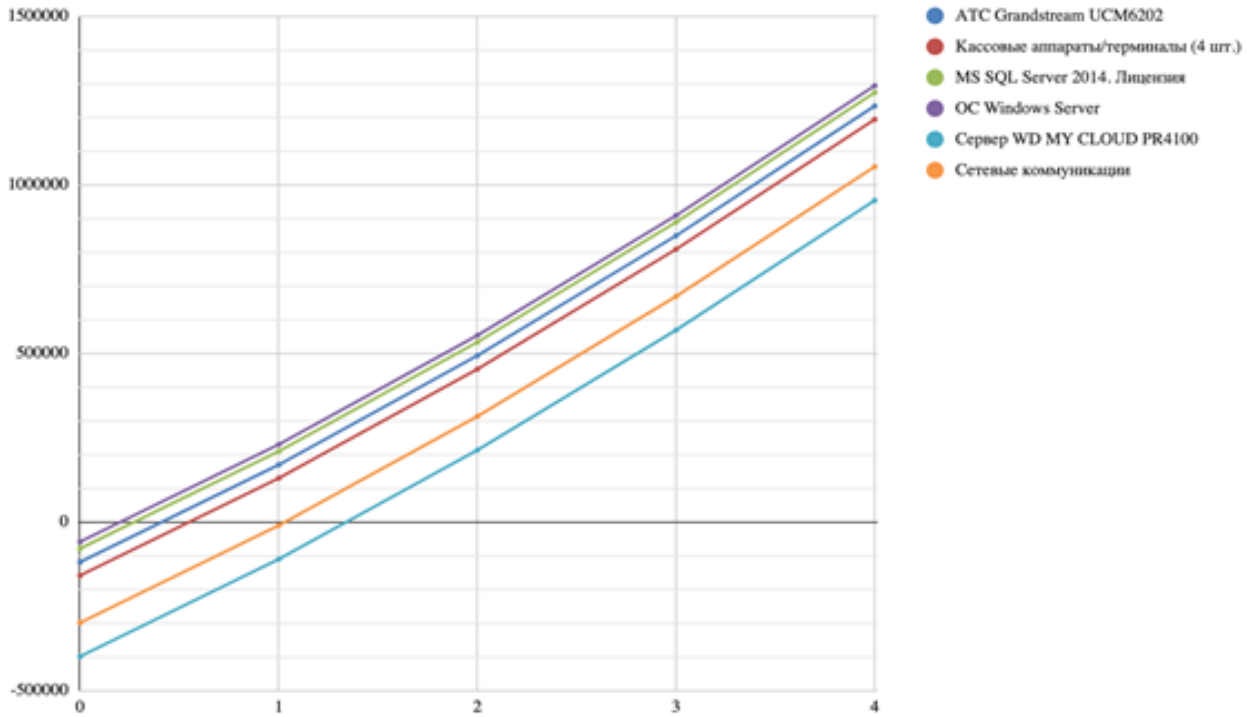


Рисунок 2. График NPV для вариантов проектов, одинаковых по длительности

4.5 Ошибки

1. Ошибки в неверном выборе периода проекта, при котором значение NPV все еще остается отрицательным (см. Табл.14). Очевидно, что реализация проекта, не имеющего положительного финансового результата в установленный период, бессмысленна.
2. Ошибки в выборе слишком короткого и/или слишком длинного периода проекта – поскольку для снижения значительного базового риска нет возможности ждать достаточно долго (12 месяцев), и в равной мере можно не получить существенное снижение базового риска до уровня приемлемого остаточного риска за короткий интервал (2 месяца).

Таблица 14. Данные по расчету NPV для каждого варианта

t	Прибыль (CI)	Затраты (CO)	CF	$(1 + R)^{(1-t)}$	CF^{disc}	NPV
0	0	430000	-430 000	1,00	-430 000	-430 000
1	50 000	0	50 000	0,91	45 500	-346 121
2	100 000	0	100 000	0,83	83 000	-275 333
3	150 000	0	150 000	0,75	112 500	-213 257
4	200 000	0	200 000	0,68	136 000	-160 551
5	250 000	0	250 000	0,62	155 000	-154 729

4.6 Вывод по лабораторной работе

В ходе лабораторной работы были изучены НМД для формирования экономического обоснования по критерию NPV для выбора дополнительных мер защиты с учетом оценки базовых и остаточных рисков ИБ для идентифицированных активов предприятия.

5 Заключение

В данном учебно-методическом пособии представлен набор лабораторных работ для обучения по курсу «Экономика защиты информации» 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 нормативно-методические материалы. Список рекомендуемой литературы соответствует теоретическому курсу «Экономика защиты информации» и включает актуальные статьи на русском и английских языках. В приложении приведены дополнительные материалы (национальные ГОСТ Р и международные стандарты ISO, ISO/IEC). Эти дополнительные материалы могут быть изучены как в рамках курса «Экономика защиты информации», так и в качестве дополнительных материалов при самообучении.

Основными тенденциями развития учебной дисциплины можно полагать дальнейшее углубленное изучение всего спектра экономических методов защиты 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 подготовке 10.04.01 «Информационная безопасность» должны лежать в плоскости не чисто технической, а юридической и экономической, поскольку от правильного выбора ИТ и корректного построения системы обеспечения безопасности зависит экономическая эффективность 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 формированием оптимального метода экономической защиты объектов критической инфраструктуры, даже при наличии профильных Федеральных законов (ФЗ-187) и Постановления Правительства (ПП-127). Важными характеристиками данных проблем можно полагать значительный охват по отраслям промышленности, значительное количество объектов, подлежащих категорированию и учету, сложность

выявления существующих закономерностей развития ИТ и соответствующих встроенных мер защиты 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.

6 Список рекомендуемой литературы

1) ГОСТ Р ИСО/МЭК 27000-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология
2) ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования;
3) ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности;
4) ГОСТ Р ИСО/МЭК 27003-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности;
5) ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.
6) ГОСТ Р ИСО/МЭК 27007-2014 Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности.
7) ГОСТ Р ИСО/МЭК 18045—2013 Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий;
8) ГОСТ Р ИСО 22301-2014 Системы менеджмента непрерывности бизнеса. Общие требования.
9) ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности.
10) ГОСТ Р 55.0.02-2014/ИСО 55001:2014 Управление активами. Национальная система стандартов. Системы менеджмента
11) Лившиц И.И. Оценка степени влияния General Data Protection Regulation на безопасность предприятий РФ // Вопросы кибербезопасности - 2020. - №4(38). - С. 66-74
12) Лившиц И.И. Оценка уровня обеспечения информационной безопасности в кредитном предприятии // Стандарты и качество - 2020. - № 7. - С. 44-49
13) 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

14) 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
15) 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
16) Лившиц И.И. Применение систем менеджмента как эффективного инструмента менеджмента рисков и обеспечения экономического роста // В сборнике: Архитектура Финансов. Сборник материалов VI Международной научно-практической конференции. 2015. С. 77-80.
17) Лившиц И.И. Современные риск-ориентированные стандарты как эффективный инструмент обеспечения экономического роста // Управление корпоративными финансами. 2015. № 5. С. 356-360.

7 Приложения

7.1 Процесс менеджмента риска информационной безопасности

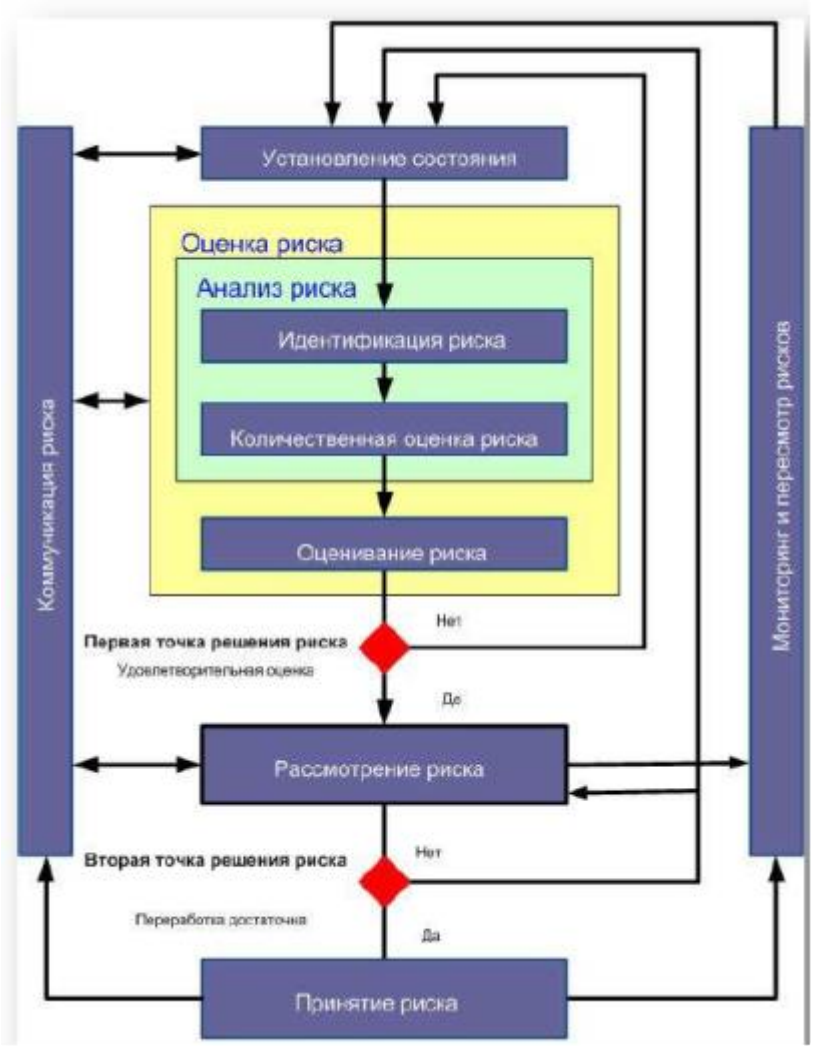


Рисунок 1. Процесс менеджмента риска ИБ по ГОСТ Р ИСО/МЭК 27005

7.2 Примеры типичных угроз

Тип	Угрозы	Обозначение
Физическое повреждение	Огонь	A, D, E
	Повреждения водой	A, D, E
	Загрязнение	A, D, E
	Значительный инцидент	A, D, E
	Уничтожение оборудования или носителей	A, D, E
	Пыль, коррозия и обледенение	A, D, E
Естественные события	Климатические явления	E
	Сейсмическое явление	E
	Вулканическое явление	E
	Метеорологическое явление	E
	Наводнение	E
Потеря необходимых сервисов	Отказ кондиционирования или системы водоснабжения	A, D
	Потеря электропитания	A, D, E
	Отказ телекоммуникационного оборудования	A, D
Радиационные неисправности	Электромагнитная радиация	A, D, E
	Тепловая радиация	A, D, E
	Электромагнитный импульс	A, D, E
Компрометация информации	Перехват и отправка компрометированного сигнала	D
	Удалённый шпионаж	D
	Подслушивание	D

Рисунок 2. Примеры типичных угроз по ГОСТ Р ИСО/МЭК 27005

7.3 Примеры уязвимостей

Тип	Примеры уязвимости	Примеры угроз
Аппаратные средства	Недостаточное обслуживание / дефектная инсталляция с носителей данных	Брешь в ремонтопригодности информационной системы
	Изъяны схем для периодических замен	Разрушение оборудования или носителей
	Восприимчивость к влажности, пыли, загрязнению	Пыль, коррозия, обледенение
	Чувствительность к электромагнитной радиации	Электромагнитная радиация
	Изъяны эффективного контроля внесения изменений конфигурации	Ошибка в использовании
	Восприимчивость к изменениям напряжения	Потеря источника питания
	Восприимчивость к температурным изменениям	Метеорологическое явление
	Незащищённое хранение	Воровство носителей или документов
	Недостаток в осторожности при уничтожении	Воровство носителей или документов
	Неконтролируемое копирование	Воровство носителей или документов

Тип	Примеры уязвимости	Примеры угроз
Программное обеспечение	Отсутствие или недостаточное программное тестирование	Злоупотребление правами
	Известные недостатки в программном обеспечении	Злоупотребление правами
	Нет 'выхода из системы' при оставлении рабочей станции	Злоупотребление правами
	Передача или многократное использование носителей данных без надлежащего стирания	Злоупотребление правами
	Малое число ревизий	Злоупотребление правами
	Неправильное распределение прав доступа	Злоупотребление правами

Рисунок 3. Примеры типичных уязвимостей по ГОСТ Р ИСО/МЭК 27005

7.4 Оценка и ранжирование рисков

Дескриптор(ы) опасностей	Последствия (активы) ценность (b)	Вероятность распространения угроз (c)	Мера риска (d)	Ранжирование опасности (e)
Угроза A	5	2	10	2
Угроза B	2	4	8	3
Угроза C	3	5	15	1
Угроза D	1	3	3	5
Угроза E	4	1	4	4
Угроза F	2	4	8	3

Рисунок 4. Пример оценки и ранжирования рисков по ГОСТ Р ИСО/МЭК 27005

7.5 Пример диаграммы "галстук-бабочка" для нежелательных последствий

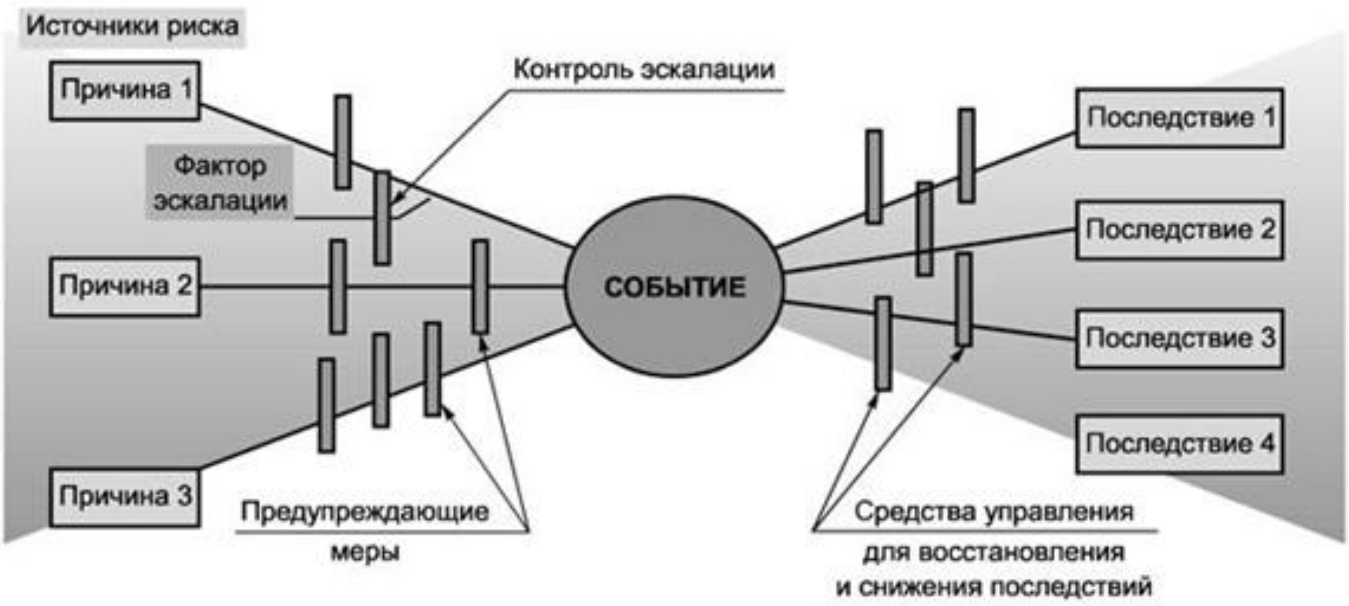


Рисунок 5. Пример диаграммы «галстук-бабочка» по ГОСТ Р ИСО/МЭК 31010

7.6 Пример диаграммы ALAPR

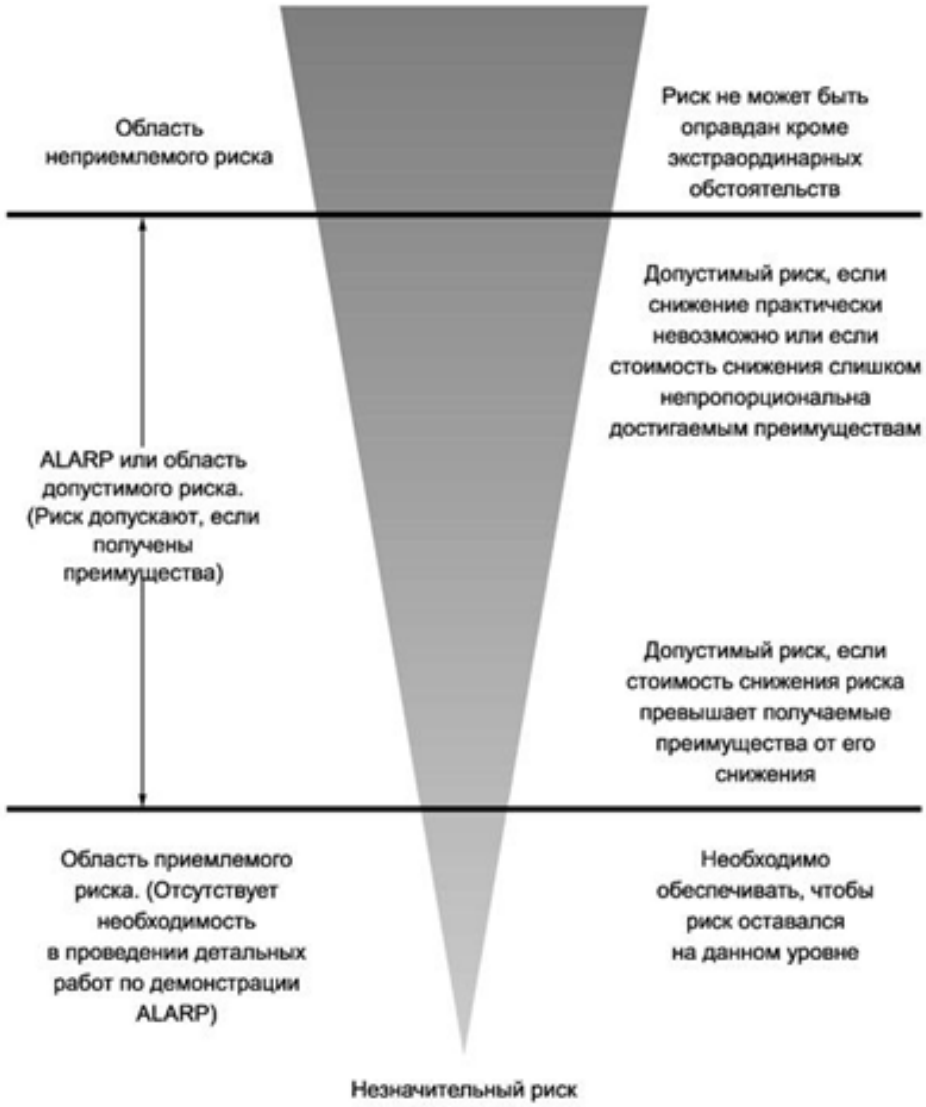
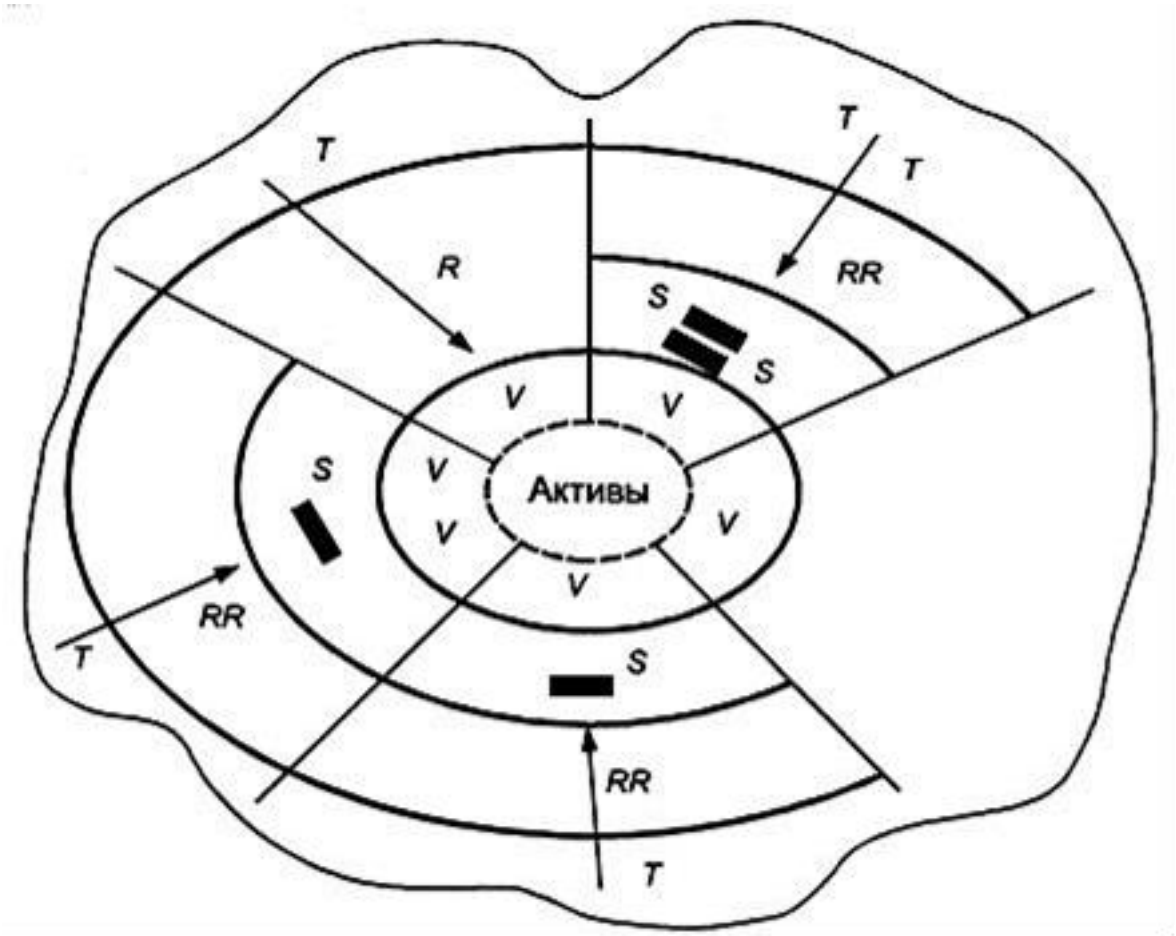


Рисунок 6. Пример диаграммы ALARP по ГОСТ Р ИСО/МЭК 31010

7.7 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.7.



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

Рисунок 7. Взаимосвязь компонентов безопасности по ГОСТ Р ИСО/МЭК 13335-1-2006

Лившиц Илья Иосифович

Экономическое 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