МИНОБРНАУКИ РОССИИ

Федеральное государственное автономное образовательное

учреждение высшего образования «Южный федеральный университет»

(ЮЖНЫЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

**Безопасность информационных технологий**

Ростов-на-Дону – Таганрог 2020

**СОДЕРЖАНИЕ**

[I. Цели и задачи освоения дисциплины 4](#_Toc50316770)

[II. Место дисциплины в структуре образовательной программы 4](#_Toc50316771)

[III. Требования к результатам освоения дисциплины 5](#_Toc50316772)

[IV. Содержание и структура дисциплины 6](#_Toc50316773)

[4.1. Содержание дисциплины, структурированное по темам 6](#_Toc50316774)

[4.2. План внеаудиторной самостоятельной работы 9](#_Toc50316775)

[4.3. Содержание учебного материала 12](#_Toc50316776)

[V. Образовательные технологии 14](#_Toc50316777)

[VI. Учебно-методическое обеспечение дисциплины 14](#_Toc50316778)

[6.1. Основная литература 14](#_Toc50316779)

[6.2. Дополнительная литература 14](#_Toc50316780)

[6.3. Перечень ресурсов сети Интернет 15](#_Toc50316781)

[VII. Материально-техническое обеспечение дисциплины 15](#_Toc50316782)

[VIII. Методические указания для обучающихся по освоению дисциплины 16](#_Toc50316783)

[IX. Учебная карта дисциплины 17](#_Toc50316784)

[X. Фонд оценочных средств 18](#_Toc50316785)

[10.1. Паспорт фонда оценочных средств 18](#_Toc50316786)

[10.2 Доклады по модулям 1 и 2 18](#_Toc50316787)

[10.3 Практические задания 24](#_Toc50316788)

[10.4 Контрольные работы по модулям 1 и 2 33](#_Toc50316789)

# Цели и задачи освоения дисциплины

Цели освоения дисциплины:

* формирование у студентов базовых знаний в области информационной безопасности в части решения задач обеспечения конфиденциальности, целостности и доступности данных и применения современных методов защиты информации.

Задачи освоения дисциплины:

* изучение основных аспектов обеспечения информационной безопасности предприятия как объекта информатизации;
* освоение методологии разработки модели угроз и модели нарушителя информационной безопасности автоматизированных и телекоммуникационных систем;
* изучение основ реализации политики информационной безопасности и организации технологического процесса комплексного обеспечения безопасности объекта защиты в соответствии с нормативными и методическими документами;
* освоение методологии создания систем управления информационной безопасностью предприятий и телекоммуникационных систем на основе риск-ориентированного подхода;
* получение навыков оценки защищенности продуктов информационных технологий и проектных решений по обеспечению безопасности телекоммуникационных систем;
* освоение методологии анализа информационной безопасности автоматизированных и телекоммуникационных систем на соответствие требованиям стандартов, а также нормам их интеграции в государственную и международную информационную среду;
* освоение методики подбора, изучения и обобщения научно-технической литературы, нормативных и методических материалов, составления обзоров по вопросам обеспечения информационной безопасности.
* получение понимания социальной значимости профессии, целей и смысла государственной службы, соблюдение норм профессиональной этики.

# Место дисциплины в структуре образовательной программы

Дисциплина относится к модулю вариативной профессиональной компетенции образовательной программы.

Данная дисциплина опирается на базовые знания, умения и навыки, формируемые при получении предшествующего уровня образования.

Знания, умения и навыки, формируемые данной дисциплиной, потребуются в научно-исследовательской работе магистрантов, при выполнении выпускных квалификационных работ, а также в дальнейшей профессиональной деятельности.

# Требования к результатам освоения дисциплины

Освоение дисциплины направлено на формирование следующих компетенций в соответствии с образовательным стандартом и образовательной программой:

Перечень планируемых результатов обучения по дисциплине, соотнесённых с индикаторами достижения компетенций

| Компетенция | Индикаторы достижения компетенции | Результаты обучения |
| --- | --- | --- |
| ВПК-1. Способен принимать меры по обеспечению защиты информации в информационных системах и оценивать уровень защищённости информации в таких системах в процессе их эксплуатации | ВПК-1.1. Разрабатывает модель угроз безопасности информационной системы, проводит моделирование различных сценариев атак, разрабатывает сценарии устранения выявленных угроз | Разработка информационных систем с обеспечением защиты обрабатываемой в них информации |
| ВПК-1.2. Разрабатывает проектные решения по защите информации в информационных системах и проводит анализ уровня защищённости информационных систем в процессе их эксплуатации | Разработка информационных систем с обеспечением защиты обрабатываемой в них информации |

# Содержание и структура дисциплины

Трудоёмкость дисциплины составляет 5 зачётных единиц, 180 часов.

в том числе 3 зачётных единицы, 108 часов с использованием онлайн-курса «Защита информации» (https://openedu.ru/course/hse/DATPRO/)

Форма промежуточной аттестации: дифференцированный зачёт

## Содержание дисциплины, структурированное по темам

| № п/п | Темы дисциплины | Семестр | Виды учебной работы и их трудоёмкость, часы  (в том числе с использованием онлайн-курсов) | | | | Наименования оценочных средств |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Контактная работа | | | Самостоя­тельная работа |
| Лекции | Практические занятия | Лабораторные занятия |
| **Модуль 1.** «Основы защиты информации в компьютерных системах» | | | | | | | |
| 1 | Тема 1. Национальная безопасность РФ, государственная информационная политика, виды безопасности, проблемы информационных войн, концепция национальной безопасности, нормативная база и стандарты в области ИБ. | 3 | 2 | 4 | - | 12 | * работа на лекционных занятиях по модулю 1 (дискуссия); * практические занятия по модулю 1 (защита практического задания №1 «Предварительный анализ объекта информатизации»). * Прохождение онлайн-курса «Защита информации» |
| 2 | Тема 2. Причины, виды и каналы утечки информации и факторы, воздействующие на информацию. | 3 | 2 | 4 | - | 13 | * практические занятия по модулю 1 (защита практического задания №2 «Разработка «Положение о защите конфиденциальной информации», «Перечень сведений конфиденциального характера» и «Модель угроз безопасности информации» (основании методических документов ФСТЭК России и банка данных угроз безопасности информации).»). * Прохождение онлайн-курса «Защита информации» |
| 3 | Тема 3. Элементы теории компьютерной безопасности. | 3 | 1 | 2 | - | 12 | практические занятия по модулю 1 (защита практического задания №3 «Применение Microsoft Security Assessment Tool для оценки рисков информационной безопасности (MSAT)»).  Прохождение онлайн-курса «Защита информации» |
| 4 | Тема 4. Показатели и классы защищенности средств вычислительной техники | 3 | 1 | 4 | - | 12 | практические занятия по модулю 1 (доклад).  Прохождение онлайн-курса «Защита информации» |
| 5 | Тема 5. Развитие стандартов по информационной безопасности. Критерии и стандарты защиты данных. | 3 | 2 | 4 | - | 14 | * практические занятия по модулю 1 (защита практических заданий №1-3). * контрольная работа по модулю 1. * Прохождение онлайн-курса «Защита информации» |
| **Модуль 2.** «Методология обеспечения и оценки безопасности информационных систем» | | | | | | | |
| 7 | Тема 6. Критерии защищенности компьютерных систем (РД ГТК, ГОСТ 15408). | 3 | 2 | 4 | - | 12 | * практические занятия по модулю 2 (защита практического задания №4 «Технический паспорт объекта информатизации»). * Прохождение онлайн-курса «Защита информации» |
|  | Тема 7. Контекст оценки безопасности информационных технологий (ГОСТ 15408). | 3 | 2 | 4 | - | 12 | * практические занятия по модулю 2 (защита практического задания №4 «Технический паспорт объекта информатизации»). * Прохождение онлайн-курса «Защита информации» |
|  | Тема 8. Оценка информационной безопасности предприятия. | 3 | 2 | 4 | - | 14 | * практические занятия по модулю 2 (защита практического задания №4 «Технический паспорт объекта информатизации»). * Прохождение онлайн-курса «Защита информации» |
|  | Тема 9. Аудит информационной безопасности организаций и систем. | 3 | 2 | 2 | - | 12 | * практические занятия по модулю 2 (доклад). * Прохождение онлайн-курса «Защита информации» |
|  | Тема 10. Аттестация объектов информатизации по требованиям безопасности информации. | 3 | 2 | 4 | - | 13 | * контрольная работа по модулю 2. * Прохождение онлайн-курса «Защита информации» |
| **Итого часов** | | 3 | 18 | 36 | 0 | 126 | – |

## План внеаудиторной самостоятельной работы

| № п/п | Темы дисциплины | Семестр | Вид самостоятельной работы | Сроки выполнения (нед.) | Затраты времени (часы) | Учебно-методическое обеспечение |
| --- | --- | --- | --- | --- | --- | --- |
| **Модуль 1.** «Основы защиты информации в компьютерных системах» | | | | | | |
| 1 | Тема 1. Национальная безопасность РФ, государственная информационная политика, виды безопасности, проблемы информационных войн, концепция национальной безопасности, нормативная база и стандарты в области ИБ. | 3 | * проработка и повторение материала лекционных занятий; * выполнение практического задания №1; * изучение материалов онлайн-курса «Защита информации». | 1–2 | 12 | Задание к практической работе №1, основная и дополнительная литература, материалы онлайн курса «Защита информации» |
| 2 | Тема 2. Причины, виды и каналы утечки информации и факторы, воздействующие на информацию. | 3 | * проработка и повторение материала лекционных занятий; * выполнение практического задания №2; * изучение материалов онлайн-курса «Защита информации». | 3–4 | 13 | Задание к практической работе №2, основная и дополнительная литература, материалы онлайн курса «Защита информации» |
| 3 | Тема 3. Элементы теории компьютерной безопасности. | 3 | * проработка и повторение материала лекционных занятий; * выполнение практического задания №3; * изучение материалов онлайн-курса «Защита информации». | 5 | 12 | Задание к практической работе №3, основная и дополнительная литература, материалы онлайн курса «Защита информации» |
| 4 | Тема 4. Показатели и классы защищенности средств вычислительной техники | 3 | * проработка и повторение материала лекционных занятий; * подготовка доклада; * изучение материалов онлайн-курса «Защита информации». | 6 | 12 | Основная и дополнительная литература, список тем докладов, материалы онлайн курса «Защита информации» |
| 5 | Тема 5. Развитие стандартов по информационной безопасности. Критерии и стандарты защиты данных. | 3 | * проработка и повторение материала лекционных занятий; * подготовка к контрольной работе; * изучение материалов онлайн-курса «Защита информации». | 7-8 | 14 | Основная и дополнительная литература, материалы онлайн курса «Защита информации» |
| **Модуль 2.** «Методология обеспечения и оценки безопасности информационных систем» | | | | | | |
| 6 | Тема 6. Критерии защищенности компьютерных систем (РД ГТК, ГОСТ 15408). | 3 | * проработка и повторение материала лекционных занятий; * выполнение практического задания №4; * изучение материалов онлайн-курса «Защита информации». | 9-10 | 12 | Задание к практической работе №4, основная и дополнительная литература, материалы онлайн курса «Защита информации» |
| 7 | Тема 7. Контекст оценки безопасности информационных технологий (ГОСТ 15408). | 3 | * проработка и повторение материала лекционных занятий; * выполнение практического задания №4; * изучение материалов онлайн-курса «Защита информации». | 11-12 | 12 | Задание к практической работе №4, основная и доп. литература, материалы онлайн курса «Защита информации» |
| 8 | Тема 8. Оценка информационной безопасности предприятия. | 3 | * проработка и повторение материала лекционных занятий; * выполнение практического задания №4; * изучение материалов онлайн-курса «Защита информации». | 13-14 | 14 | Основная и дополнительная литература, список тем докладов, материалы онлайн курса «Защита информации» |
| 9 | Тема 9. Аудит информационной безопасности организаций и систем. | 3 | * проработка и повторение материала лекционных занятий; * подготовка доклада; * изучение материалов онлайн-курса «Защита информации». | 15-16 | 12 | Основная и дополнительная литература, материалы онлайн курса «Защита информации» |
| 10 | Тема 10. Аттестация объектов информатизации по требованиям безопасности информации. | 3 | * проработка и повторение материала лекционных занятий; * подготовка к контрольной работе; * изучение материалов онлайн-курса «Защита информации». | 17-18 | 13 | Основная и дополнительная литература, материалы онлайн курса «Защита информации» |
| **Общая трудоёмкость самостоятельной работы по дисциплине** | | | | | 126 | – |

## Содержание учебного материала

**Модуль 1. «Основы защиты информации в компьютерных системах»**

**4.3.1. Национальная безопасность РФ, государственная информационная политика, виды безопасности, проблемы информационных войн, концепция национальной безопасности, нормативная база и стандарты в области ИБ.** Угрозы и уязвимости ИС. Классификация угроз безопасности ИС. Методы оценивания угроз безопасности КС. Классификация злоумышленников. Модель нарушителя. Классификация каналов проникновения в систему и утечки информации. Классификация методов и средств защиты информации. Основы организации защиты государственной тайны.

**4.3.2. Причины, виды и каналы утечки информации и факторы, воздействующие на информацию.** ГОСТ Р 50922-96, ГОСТ Р 51275-99. Характеристика видов утечки информации: разглашение информации, несанкционированный доступ, получение защищаемой информации разведками. Характеристика каналов утечки информации: электромагнитный, акустический (виброакустический), визуальный и информационный.

**4.3.3. Элементы теории компьютерной безопасности.** Требования по защите информации. Модели безопасности. Методы и средства аутентификации и контроля доступа**.** Модели безопасности. Дискреционная модель безопасности. Мандатная модель безопасности. Ролевая модель безопасности. Основные понятия в технологиях идентификации и аутентификации. Парольные системы. Методы компрометации паролей и защиты от нее. Количественная оценка стойкости парольных систем.

**4.3.4. Показатели и классы защищенности средств вычислительной техники (РД ГТК РФ)**. Классификация межсетевых экранов**.** Анализ программного обеспечения на недекларированные возможности Уровни контроля и требования к ним. Классификация антивирусных средства защиты информации. Показатели защищенности и требования по защите от вирусов. Виды вирусов и методы испытаний программных средств на наличие компьютерных вирусов (ГОСТ Р 51188-98).

**4.3.5. Развитие стандартов по информационной безопасности. Критерии и стандарты защиты данных**. TCSEC, ITSEC, FCITS, CTCPEC, СС И РД ГТК РФ. Задачи стандартов и основные понятия. Взаимодействие между производителями, потребителями и экспертами по квалификации продуктов информационных технологий.

**Модуль 2. «Методология обеспечения и оценки безопасности информационных систем»**

**4.3.6. Критерии защищенности компьютерных систем (РД ГТК, ГОСТ 15408).**

Базовые понятия и принципы Общих Критериев. Представление функциональных требования и требований доверия к ИТ-продуктам. Парадигма функциональных требований. Парадигма доверия в стандарте ГОСТ 15408. Обзор классов и семейств функциональных требований и требований доверия. Обзор оценочных уровней доверия (ОУД1–ОУД7).

**4.3.7. Контекст оценки безопасности информационных технологий (ГОСТ 15408).** Разработка объекта оценки, процесс оценки, эксплуатация. Виды оценок: профиль защиты (ПЗ), задание по безопасности (ЗБ). Структура ПЗ: введение, описание ОО. среда безопасности ОО, цели безопасности, требования безопасности ОО, замечания по применению, обоснование. Особенности и структура ЗБ. Краткая спецификация. Оценка безопасности ИТ-продукта с использованием ПЗ, ЗБ и сертификата по безопасности на основе ГОСТ 15408 и РД ГТК.

**4.3.8. Оценка информационной безопасности предприятия.** Концепция защиты от НСД к информации (РД ГТК РФ). Два направления: АС и СВТ. Модель нарушителя: уровни возможностей. Классификация автоматизированных систем (АС) и требования по защите информации. Основные подсистемы СЗИ (связь функций и классов АС): управления доступом, регистрации и учета, криптоподсистема, сохранения целостности. Организационные мероприятия по защите информации от НСД. Специальные защитные знаки. Классификация по возможности подделки, идентифицируемости и стойкости защитных свойств. Применение на объектах различной категории.

**4.3.9. Аудит информационной безопасности организаций и систем.** Международные правовые аспекты, стандарты и руководства по основам аудита информационной безопасности. Анализ рисков как часть аудита ИБ. Менеджмент событий и инцидентов информационной безопасности. Обеспечение непрерывности бизнеса. Практическая реализация требования к системам управления безопасностью. SIEM-системы. Работа после внедрения системы управления ИБ. GRC-системы управления информационной безопасностью. GRC парадигма управления ИБ. Security GRC-системы управления ИБ. Обзор российских SGRC-продуктов.

**4.3.10. Аттестация объектов информатизации по требованиям безопасности информации.** Структура системы аттестации по требованиям безопасности информации. Функции ФСТЭК России в рамках системы аттестации. Обязательная и добровольная аттестация по требованиям безопасности информации. Исходные данные и документация аттестуемого объекта информатизации. Порядок проведения аттестации объектов информатизации по требованиям безопасности информации. Структура протокола аттестационных испытаний и аттестата соответствия.

Перечень тем практических занятий

| №  п/п | Тема практического занятия | Количество часов |
| --- | --- | --- |
| **Модуль 1. Основы защиты информации в компьютерных системах** | | |
| 1 | Практическое задание №1 «Предварительный анализ объекта информатизации». | 4 |
| 2 | Практическое задание №2 «Разработка «Положение о защите конфиденциальной информации», «Перечень сведений конфиденциального характера» и «Модель угроз безопасности информации» (основании методических документов ФСТЭК России и банка данных угроз безопасности информации)». | 4 |
| 3 | Практическое задание №3 «Применение Microsoft Security Assessment Tool для оценки рисков информационной безопасности (MSAT)». | 2 |
| 4 | Доклады. | 4 |
| 5 | Защита практических работ №1-3. | 2 |
| 6 | Контрольная работа по модулю 1. | 2 |
| **Модуль 2. Методология обеспечения и оценки безопасности информационных систем** | | |
| 7 | Практическое задание №4 «Технический паспорт объекта информатизации». | 12 |
| 9 | Доклады | 4 |
| 11 | Контрольная работа по модулю 2. | 2 |
| **Всего часов** | | **36** |

# Образовательные технологии

По дисциплине предусмотрены следующие методы обучения и интерактивные формы проведения занятий:

По дисциплине предусмотрены следующие активные формы обучения:

* лекции-визуализации – с использованием презентационного материала;
* практические занятия, в рамках которых обучающиеся делают доклады по заданным темам, обсуждаются вопросы выполнения практических заданий и представление проделанной работы.

Наряду с традиционными образовательными технологиями, для реализации дисциплины могут использоваться технологии электронного обучения и дистанционные образовательные технологий в электронной информационно-образовательной среде Южного федерального университета и образовательной платформы «Открытое образование» (https://openedu.ru). Лекционные занятия и другие формы контактной работы обучающихся с преподавателем могут проводиться с использованием платформы Microsoft Teams, OneDrive и системы электронного обучения ИКТИБ ЮФУ (lms.sfedu.ru), что позволяет обеспечить онлайн и офлайн взаимодействие преподавателя с обучающимися в рамках дисциплины.

Основными методами контроля являются письменные контрольные работы, отчеты к практическим заданиям, презентации докладов, сертификат о прохождении онлайн курса «Защита информации», а также электронный учёт и контроль учебных достижений студентов (использование средств сервиса балльно-рейтинговой системы; ведение электронного журнала успеваемости и применение других средств контроля с использованием системы электронного обучения).

# Учебно-методическое обеспечение дисциплины

## Основная литература

1. Аверченков, В.И. Служба защиты информации: организация и управление :

учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - 3-е изд., стереотип. - М. :

Флинта, 2016. - 186 с. http://biblioclub.ru/index.php?page=book&amp;id=93356.

## Дополнительная литература

2. Основы информационной безопасности. Часть 1: учебно-методическое пособие; сост. А.К.Шилов. – Ростов-на-Дону: Изд-во ЮФУ, 2014. – 167 с. *–* <http://hub.sfedu.ru/allocator/files/9f46f770-793a-4610-b15f-a2fb9be7fff1/predisplay/>.

3. Комплексная защита информации на предприятии: учебно-методическое пособие; сост. А.К.Шилов. – Таганрог: Изд-во ЮФУ, 2013. – 86 с. – <http://hub.sfedu.ru/allocator/files/90c09aa4-2e49-408a-b1d7-4e8cea8bf2b7/predisplay/>

4. [Нестеров, С.А.](https://biblioclub.ru/index.php?page=author_red&id=133708) Основы информационной безопасности: учебное пособие. – Санкт-Петербург: [Издательство Политехнического университета](https://biblioclub.ru/index.php?page=publisher_red&pub_id=18012), 2014. – 322 с. – <https://biblioclub.ru/index.php?page=book_view_red&book_id=363040>.

5. [Загинайлов, Ю. Н.](https://biblioclub.ru/index.php?page=author_red&id=106232) Основы информационной безопасности: курс визуальных лекций: учебное пособие. – Москва, Берлин: [Директ-Медиа](https://biblioclub.ru/index.php?page=publisher_red&pub_id=1), 2015. – 105 с. *–* <https://biblioclub.ru/index.php?page=book_view_red&book_id=362895>.

6. Бабенко Л.К., Маро Е.А. Методы защиты приложений от несанкционированного использования с помощью аппаратных ключей HАSР HL. Учебное пособие. Изд-во ЮФУ, 2015. 87 стр. Электронный ресурс, ссылка: http://hub.sfedu.ru/allocator/files/d652ba29-ba89-4179-b82a-0a8a317a331f/predisplay/

7. Шилов, А.К. Современная методология оценки безопасности информационных технологий: учебное пособие. – Таганрог: Изд-во ТТИ ЮФУ, 2007. – 170 с. *–* <http://hub.sfedu.ru/allocator/files/e52b5794-ac2c-435e-932d-00ff4d978c53/predisplay/>.

8. Шилов, А.К. Анализ рисков информационной безопасности: учебно-методическое пособие / Г.Е.Веселов, Е.С.Абрамов, А.К.Шилов. – Таганрог: Изд-во ЮФУ, 2015. – 108 с. *–*  <http://hub.sfedu.ru/allocator/files/db776d4d-524d-4178-a7b8-b0437e250e61/predisplay/>

9. Методические указания к проведению лабораторных работ по методологии защиты информации; сост. А. К. Шилов. – Таганрог: Изд-во ТРТУ, 2004. – 12 с. <http://hub.sfedu.ru/allocator/files/13fba8e0-de53-44c9-8d23-34833072665c/predisplay/>

10. Доступ к нормативно-правовым документам осуществляется с использованием информационно-правового портала «Гарант» (<http://ivo.garant.ru>), справочной правовой системы КонсультантПлюс (http://www.consultant.ru), официального сайта Федерального агентства по техническому регулированию и метрологии (https://www.gost.ru/), официального сайта Федеральной службы по техническому и экспортному контролю (https://fstec.ru/), официального сайта Федеральной службы безопасности Российской Федерации (http://www.fsb.ru/), Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (<http://rkn.gov.ru/>).

## Перечень ресурсов сети Интернет

<http://fstec.ru/> – Федеральная служба по техническому и экспортному контролю (ФСТЭК России).

<http://www.fsb.ru/> – Федеральная служба безопасности Российской Федерации.

<http://rkn.gov.ru/> – Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций.

# Материально-техническое обеспечение дисциплины

При реализации дисциплины используются следующие помещения, оборудование и программное обеспечение:

1. аудитория лекционного типа:

* Компьютер преподавателя - 1 шт.;
* Экран для проектора с электроприводом – 1 шт.;
* Мультимедийный проектор – 1 шт.;
* Сетевое оборудование – 1 шт.;
* Microsoft Windows, Microsoft Office PowerPoint.

1. аудитория практических занятий, индивидуальных и групповых консультаций, промежуточной аттестации:

* Доска интерактивная – 1 шт.,
* Компьютер преподавателя – 1 шт.;
* Компьютер – 17 шт.;
* Сетевое оборудование – 1 шт.;
* OneDrive;
* Microsoft Teams;
* Система электронного обучения ИКТИБ ЮФУ (lms.sfedu.ru);
* Ubuntu, Open Office.

# Методические указания для обучающихся по освоению дисциплины

Учебный процесс обучения дисциплине включает в себя аудиторные занятия (лекции, практические занятия) и самостоятельную работу. Промежуточная аттестация по дисциплине – дифференциальный зачет. Лектор и преподаватели, ведущие занятия, контролируют посещение всех видов аудиторных занятий.

Чтение лекций проводится с демонстрацией слайдов. Материалы лекционных занятий (презентации), практических занятий и заданий своевременно предоставляются в пользование студентов посредством размещения в электронном пространстве (облачные хранилища – OneDrive, lms.sfedu.ru, Microsoft Teams).

Практические занятия проводятся в аудитории, оснащенной интерактивной доской, и иллюстрируются презентациями и наглядной демонстрацией выполнения соответствующих задач. Практические занятия требуют предварительной теоретической подготовки по соответствующей теме: изучения основной и дополнительной литературы по дисциплине. На практических занятиях осуществляется периодические дискуссии по ранее изученному материалу, обучающиеся делают доклады по темам практических занятий, преподаватель разбирает качество сделанных докладов, осуществляется разбор практических заданий и обзор выполнения контрольной работы.

Самостоятельная работа студентов включает в себя подготовку к лекционным, практическим занятиям, контрольным работам, выполнение практических заданий, а так еж изучение материалов онлайн-курса «Защита информации». Контроль усвоения материала осуществляется на аудиторных занятиях путем обсуждения теоретического материала по теме занятия, обсуждения вопросов, разобранных по предыдущей теме, при проверке и защите практических заданий и контрольный работ.

Максимальное количество баллов по каждому виду работ указано в учебной карте дисциплины.

Студенты, которые по уважительной причине не смогли набрать необходимое число баллов по текущему и рубежному контролю модуля, могут по согласованию с преподавателем ликвидировать задолженности до конца последней недели обучения соответствующего семестра.

# Учебная карта дисциплины

Курс 2, семестр 3, очная форма обучения

|  |  |  |  |
| --- | --- | --- | --- |
| №  п/п | Виды контрольных мероприятий  (наименования оценочных средств) | Количество баллов | |
| Текущий контроль | Рубежный контроль |
| Модуль 1. Основы защиты информации в компьютерных системах | | | |
| 1 | Практическое задание №1 «Предварительный анализ объекта информатизации». | 8 | - |
| 3 | Практическое задание №2 «Разработка «Положение о защите конфиденциальной информации», «Перечень сведений конфиденциального характера» и «Модель угроз безопасности информации» ( на основании методических документов ФСТЭК России и банка данных угроз безопасности информации)». | 10 | - |
| 4 | Практическое задание №3 «Применение Microsoft Security Assessment Tool для оценки рисков информационной безопасности (MSAT)». | 6 | - |
| 5 | Доклады. | 3 |  |
| 6 | Контрольная работа по модулю 1 | - | 10 |
| Модуль 2. Методология обеспечения и оценки безопасности информационных систем | | | |
| 8 | Практическое задание №4 «Технический паспорт объекта информатизации». | 10 | - |
| 9 | Доклады. | 3 | - |
| 10 | Контрольная работа по модулю 2. | - | 10 |
| **Всего** | | 40 | 20 |
| Бонусные баллы | | Бонусные баллы назначаются за успешное прохождение онлайн-курса «Защита информации» (набрано более 85 баллов) | |
| **Промежуточная аттестация  в форме дифференцированного зачёта** | | Оценка по дисциплине выставляется по сумме баллов за текущий контроль и рубежный контроль:   * 85–100 баллов – оценка «отлично»; * 71–84 балла – оценка «хорошо»; * 60–70 баллов – оценка «удовлетворительно»;   менее 60 баллов – оценка «неудовлетворительно» | |

# Фонд оценочных средств

## Паспорт фонда оценочных средств

| № п/п | Индикатор достижения компетенции | Наименование оценочного средства |
| --- | --- | --- |
| 1 | ВПК-1.1. Разрабатывает модель угроз безопасности информационной системы, проводит моделирование различных сценариев атак, разрабатывает сценарии устранения выявленных угроз | * практические задания №2, 3. * контрольные работы. |
| 2 | ВПК-1.2. Разрабатывает проектные решения по защите информации в информационных системах и проводит анализ уровня защищённости информационных систем в процессе их эксплуатации | * практические задания №1-4. * контрольные работы. |

10.2 Доклады по модулям 1 и 2

Темы для докладов на практических занятиях по дисциплине   
«Безопасность информационных технологий»

**Модуль 1.** «Основы защиты информации в компьютерных системах»

1. Актуальность защиты информации. Предпосылки кризиса систем защиты информации (СЗИ). Современные требования к СЗИ.

2. Уровни рассмотрения вопросов информационной безопасности (ИБ). Предприятие как объект информатизации (категории), АС и СВТ. Состав типовой комплексной системы защиты информации на предприятии (КСЗИ): СКУД, ОТ, ОПС, ПЭШ, КС. Уровни секретности (ГТ: С, СС, ОВ) и конфиденциальности (К: служебная, коммерческая и общедоступная) информации. Политика безопасности предприятия (ГОСТ 27001).

3. Анализ проблем защиты информации (ЗИ) на предприятии. Системно-концептуальный подход. Условия реализации Концепции защиты информации в Российской Федерации. Надежность информации. Характер сохраняемой тайны. Виды защищаемой информации. Цели ЗИ: конфиденциальность, целостность и доступность.

4. Причины, виды и каналы утечки информации (ГОСТ Р 50922-96). Характеристика видов утечки информации: разглашение информации, несанкционированный доступ, получение защищаемой информации разведками. Характеристика каналов утечки информации: электромагнитный, акустический (виброакустический), визуальный и информационный.

5. Факторы, воздействующие на информацию (ГОСТ Р 51275-99). Внешние, внутренние, объективные и субъективные.

6. Подходы и принципы обеспечения информационной безопасности. Системность, комплексность, непрерывность защиты, гибкость управления и применения, открытость алгоритмов и механизмов защиты, разумная достаточность, простота применения защитных мер и средств. Структуризация методов обеспечения ИБ по уровням: носителей информации, средствам взаимодействия с носителем, представления информации и содержания информации.

7. Основные функции типовой системы защиты информации компьютерной системы (СЗИ КС). Политика безопасности. Разграничение и управление доступом: дискреционная и мандатная модели. Идентификация. Аутентификация. Авторизация. Аудит.

8. Парольные системы. Методы компрометации паролей и защиты от нее. Количественная оценка стойкости парольных систем.

9. Аудит: регистрация потенциально опасных событий в компьютерной системе, необходимость, требования, политика аудита.

10. Дискреционное управление доступом (DAC). Дискреционная политика безопасности. Матрица доступа: О-С-М, О-С-М-П, изолированная программная среда. Основные свойства: произвольностьуправления доступом. Достоинства и недостатки. Области применения.

11. Мандатное управление доступом (MAC). Мандатная политика безопасности. Метки безопасности: структура, назначение полей. Основные свойства: *принудительность* управления доступом, правила NRU и NWD, основная теорема безопасности. Достоинства и недостатки в сравнении с дискреционной моделью. Области применения.

12. Ролевое управление доступом (RBAS). Основные понятия. Статическое и динамическое разделение обязанностей.

13. Защита от угрозы нарушения целостности информации. Принципы сохранения целостности данных в АС.

14. Развитие стандартов по информационной безопасности (TCSEC, ITSEC, FCITS, CTCPEC, СС И РД ГТК РФ). Задачи стандартов и основные понятия. Взаимодействие между производителями, потребителями и экспертами по квалификации продуктов информационных технологий.

15. Стандарты «Радужной серии». Оранжевая книга (TCSEC). Цели создания. Таксономия требований по безопасности компьютерных систем: политика безопасности, повторное использования объектов, анализ скрытых каналов, прямое взаимодействие с ядром безопасности, подотчетность, гарантированность, документация. Классификация трастовых компьютерных систем. Красная, розовая и желтая книги.

16. Европейские (гармонизированные) критерии безопасности информационных технологий (ITSEC).

17. Федеральные критерии безопасности информационных технологий (FCITS). Цели разработки. Понятие профиля защиты (ПЗ).

18. Канадские критерии безопасности компьютерных систем (CTCPEC).

19. Концепция защиты от НСД к информации (РД ГТК РФ). Два направления - АС и СВТ. Модель нарушителя: уровни возможностей.

20. Классификация автоматизированных систем (АС) и требования по защите информации (РД ГТК РФ). Система классификации защищенных АС. Основные подсистемы СЗИ (связь функций и классов АС): управления доступом, регистрации и учета, криптоподсистема, сохранения целостности. Организационные мероприятия по защите информации от НСД.

21. Показатели и классы защищенности средств вычислительной техники (СВТ) (РД ГТК РФ). Классификация защищенных СВТ.

22. Межсетевые экраны (МЭ) (РД ГТК РФ). Классификация МЭ. Связь классов с показателями: управление доступом, идентификация и аутентификация, регистрация, администрирование (идентификация, аутентификация, регистрация), простота использования, целостность, восстановление, тестирование, руководство администратора, тестовая и конструкторская (проектная) документация. Связь классов с уровнями базовой эталонной модели сетей.

23. Анализ программного обеспечения (ПО) (РД ГТК РФ). Недекларированные возможности ПО. Уровни контроля и требования к ним. Требования к документации. Содержание испытаний: статический и динамический анализ.

24. Испытания программных средств на наличие компьютерных вирусов (ГОСТ Р 51188-98).

25. Антивирусные средства (АВС) защиты информации (РД ГТК РФ). Показатели защищенности и требования по защите от вирусов. Виды вирусов. Классификация АВС. Характеристика основных подсистем: контроля целостности; блокирования внедрения; обнаружения; удаления; обеспечения гарантированности свойств АВС; регистрации. Особенности требований к АВС 3, 2 и 1 групп.

26. Специальные защитные знаки (СЗЗ) (РД ГТК РФ). Классификация по возможности подделки, идентифицируемости и стойкости защитных свойств. Применение на объектах различной категории.

**Модуль 2.** «Методология обеспечения и оценки безопасности информационных систем»

27. ГОСТ Р 15408:2002. Часть 1. МЕТОДОЛОГИЯ ОЦЕНКИ БЕЗОПАСНОСТИ ИТ. Области применения стандарта «Общие критерии».

28. ГОСТ Р 15408:2002. Часть 1. Контекст оценки безопасности информационных технологий: разработка ОО, процесс оценки, эксплуатация.

29. ГОСТ Р 15408:2002. Часть 1. ПОСЛЕДОВАТЕЛЬНОСТЬ ФОРМИРОВАНИЯ ТРЕБОВАНИЙ И СПЕЦИФИКАЦИЙ: среда безопасности, цели безопасности, требования безопасности ИТ и краткая спецификация ОО.

30. ГОСТ Р 15408:2002. Часть 1. ПРЕДСТАВЛЕНИЕ ТРЕБОВАНИЙ БЕЗОПАСНОСТИ: КЛАССЫ, СЕМЕЙСТВА, КОМПОНЕНТЫ, ЭЛЕМЕНТЫ. Виды связей и зависимостей между компонентами, разрешенные операции с элементами.

31. ГОСТ Р 15408:2002. Часть 1. ИСТОЧНИКИ ТРЕБОВАНИЙ БЕЗОПАСНОСТИ. Виды оценок: ПЗ, ЗБ, ОО. Поддержка доверия.

32. ГОСТ Р 15408:2002. Часть 1. Особенности ПЗ. Структура ПЗ: введение, описание ОО. среда безопасности ОО, цели безопасности, требования безопасности ОО, замечания по применению, обоснование.

33. ГОСТ Р 15408:2002. Часть 1. Особенности ЗБ. Структура ЗБ: введение, описание ОО, среда безопасности ОО, цели безопасности, требования безопасности ИТ, краткая спецификация ОО, утверждения о соответствии ПЗ, обоснование.

34. ГОСТ Р 15408:2002. Часть 2. ОСОБЕННОСТИ ФУНКЦИОНАЛЬНЫХ ТРЕБОВАНИЙ. Представление функциональных требований. Структура класса. Структура семейства (ранжирование, управление, аудит). Структура компонента (подчиненность по иерархии, зависимости - прямые, косвенные, выбираемые, операции - итерация, назначение, выбор, уточнение). Функциональный элемент.

35. ГОСТ Р 15408:2002. Часть 2. ПАРАДИГМА ФУНКЦИОНАЛЬНЫХ ТРЕБОВАНИЙ. Виды объектов оценки и политик безопасности. Функции безопасности: стойкость, область действия, интерфейс, типы ПФБ. ФБО единого, локального и распределенного ОО. Виды пользователей. Роли. Ресурсы. Сущности: активные и пассивные. Атрибуты безопасности. Данные ОО: пользователя и ФБО. Аутентификационные данные и секреты.

36. ГОСТ Р 15408:2002. Часть 2. ОБЗОР КЛАССОВ ФУНКЦИОНАЛЬНЫХ ТРЕБОВАНИЙ. Класс FAU - Аудит безопасности. Реакция и генерация данных аудита. Анализ аудита: выявление аномалии по профилю, простая и сложная эвристики атаки. Ограниченный и выборочный просмотр аудита. Выбор событий, защищенное хранение данных, гарантии доступности данных аудита.

37. ГОСТ Р 15408:2002. Часть 2. ОБЗОР КЛАССОВ ФУНКЦИОНАЛЬНЫХ ТРЕБОВАНИЙ. Класс FCO - Связь, его семейств и компонент. Неотказуемость отправления. Неотказуемость получения.

38. ГОСТ Р 15408:2002. Часть 2. ОБЗОР КЛАССОВ ФУНКЦИОНАЛЬНЫХ ТРЕБОВАНИЙ. Класс FCS - Криптографическая поддержка. Управление криптографическими ключами. Криптографические операции.

39. ГОСТ Р 15408:2002. Часть 2. ОБЗОР КЛАССОВ ФУНКЦИОНАЛЬНЫХ ТРЕБОВАНИЙ. Класс FDP - Защита данных пользователя. Политика управления доступом. Политика управления информационными потоками. Функции управления доступом. Функции управления информационными потоками. Передача в пределах ОО. Защита остаточной информации. Откат. Целостность хранимых данных. Аутентификация данных. Экспорт данных за пределы действия ФБО. Импорт данных из-за пределов действия ФБО. Защита конфиденциальности данных пользователя при передаче между ФБО. Защита целостности данных пользователя при передаче между ФБО.

40. ГОСТ Р 15408:2002. Часть 2. ОБЗОР КЛАССОВ ФУНКЦИОНАЛЬНЫХ ТРЕБОВАНИЙ. Класс FIA - Идентификация и аутентификация. Отказы аутентификации. Определение атрибутов пользователя. Спецификация секретов. Аутентификация пользователя. Идентификация пользователя. Связывание пользователь-субъект.

41. ГОСТ Р 15408:2002. Часть 2. ОБЗОР КЛАССОВ ФУНКЦИОНАЛЬНЫХ ТРЕБОВАНИЙ. Класс FMT - Управление безопасностью. Управление отдельными функциями ФБО. Управление атрибутами безопасности. Управление данными ФБО. Отмена. Срок действия атрибута безопасности. Роли управления безопасностью.

42. ГОСТ Р 15408:2002. Часть 2. ОБЗОР КЛАССОВ ФУНКЦИОНАЛЬНЫХ ТРЕБОВАНИЙ. Класс FPR - Приватность. Анонимность. Псевдонимность. Невозможность ассоциации. Скрытность.

43. ГОСТ Р 15408:2002. Часть 2. ОБЗОР КЛАССОВ ФУНКЦИОНАЛЬНЫХ ТРЕБОВАНИЙ. Класс FPT - Защита ФБО. Тестирование базовой абстрактной машины. Безопасность при сбое. Доступность экспортируемых данных ФБО. Конфиденциальность экспортируемых данных ФБО. Целостность экспортируемых данных ФБО. Передача данных ФБО в пределах ОО. Физическая защита ФБО. Надежное восстановление.

44. ГОСТ Р 15408:2002. Часть 2. ОБЗОР КЛАССОВ ФУНКЦИОНАЛЬНЫХ ТРЕБОВАНИЙ. Класс FRU - Использование ресурсов. Отказоустойчивость. Приоритет обслуживания. Распределение ресурсов.

45. ГОСТ Р 15408:2002. Часть 2. ОБЗОР КЛАССОВ ФУНКЦИОНАЛЬНЫХ ТРЕБОВАНИЙ. Класс FTA - Доступ к ОО. Ограничение области выбираемых атрибутов. Ограничение на параллельные сеансы. Блокирование сеанса. Предупреждения перед предоставлением доступа к ОО. История доступа к ОО. Открытие сеанса с ОО.

46. ГОСТ Р 15408:2002. Часть 2. ОБЗОР КЛАССОВ ФУНКЦИОНАЛЬНЫХ ТРЕБОВАНИЙ. Класс FTP - Доверенный маршрут/канал. Доверенный канал передачи между ФБО. Доверенный маршрут.

47. ГОСТ Р 15408:2002. Часть 3. ПАРАДИГМА ДОВЕРИЯ В СТАНДАРТЕ. Основные принципы стандарта. Значимость уязвимостей. Причины возникновения уязвимостей. Подход к доверию в стандарте. Роль оценки.

48. ГОСТ Р 15408:2002. Часть 3. ПРЕДСТАВЛЕНИЕ ТРЕБОВАНИЙ ДОВЕРИЯ К БЕЗОПАСНОСТИ. Структура класса, семейства, компонента, элемента и оценочных уровней доверия.

49. ГОСТ Р 15408:2002. Часть 3. ОБЗОР КЛАССОВ И СЕМЕЙСТВ ДОВЕРИЯ. Класс ACM –: Управление конфигурацией. Возможности УК. Область УК. Класс ADO – Поставка и эксплуатация. Поставка. Установка, генерация и запуск.

50. ГОСТ Р 15408:2002. Часть 3. ОБЗОР КЛАССОВ И СЕМЕЙСТВ ДОВЕРИЯ. Класс ADV – Разработка. Функциональная спецификация. Проект верхнего уровня. Представление реализации. Внутренняя структура ФБО. Проект нижнего уровня. Соответствие представлений. Моделирование политики безопасности.

51. ГОСТ Р 15408:2002. Часть 3. ОБЗОР КЛАССОВ И СЕМЕЙСТВ ДОВЕРИЯ. Класс AGD – Руководства. Руководство администратора. Руководство пользователя. Класс ALC – Поддержка жизненного цикла. Безопасность разработки. Устранение недостатков. Определение жизненного цикла. Инструментальные средства и методы.

52. ГОСТ Р 15408:2002. Часть 3. ОБЗОР КЛАССОВ И СЕМЕЙСТВ ДОВЕРИЯ. Класс ATE – Тестирование. Покрытие. Глубина. Функциональное тестирование. Независимое тестирование.

53. ГОСТ Р 15408:2002. Часть 3. ОБЗОР КЛАССОВ И СЕМЕЙСТВ ДОВЕРИЯ. Класс AVA – Оценка уязвимостей. Анализ скрытых каналов. Неправильное применение. Стойкость функций безопасности ОО. Анализ уязвимостей.

54. ГОСТ Р 15408:2002. Часть 3. ОБЗОР КЛАССА И СЕМЕЙСТВ ПОДДЕРЖКИ ДОВЕРИЯ. Класс AMA – Поддержка доверия. План поддержки доверия. Отчет о категорировании компонентов ОО. Свидетельство поддержки доверия. Анализ влияния на безопасность.

55. ГОСТ Р 15408:2002. Часть 3. КРИТЕРИИ ОЦЕНКИ ПРОФИЛЯ ЗАЩИТЫ. Оценка профиля защиты. Соотношение с критериями оценки задания по безопасности. Задачи оценщика. Обзор класса APE – Оценка профиля защиты.

56. ГОСТ Р 15408:2002. Часть 3. КРИТЕРИИ ОЦЕНКИ ЗАДАНИЯ ПО БЕЗОПАСНОСТИ. Оценка задания по безопасности. Задачи оценщика. Обзор класса ASE – Оценка задания по безопасности.

57. ГОСТ Р 15408:2002. Часть 3. ПАРАДИГМА ПОДДЕРЖКИ ДОВЕРИЯ. Цикл поддержки доверия. Приемка ОО. Мониторинг ОО. Переоценка. Обзор класса AMA - Поддержка доверия. План поддержки доверия. Отчет о категорировании компонентов ОО. Свидетельство поддержки доверия. Анализ влияния на безопасность.

58. ГОСТ Р 15408:2002. Часть 3. ОБЗОР ОЦЕНОЧНЫХ УРОВНЕЙ ДОВЕРИЯ (ОУД1 - ОУД7). Примерное соответствие классам «Оранжевой книги», Европейских критериев и РД ГТК РФ.

59. ГОСТ Р 15408:2002. Часть 3. ОЦЕНОЧНЫЙ УРОВЕНЬ ДОВЕРИЯ ОУД1 – Функциональное тестирование. Область применения. Основные действия по свойства. Взаимодействие разработчика, пользователя и оценщика. Реализующие компоненты.

60. ГОСТ Р 15408:2002. Часть 3. ОЦЕНОЧНЫЙ УРОВЕНЬ ДОВЕРИЯ ОУД2 – Структурное тестирование. Область применения. Основные иерархические свойства - отличия от ОУД1. Взаимодействие разработчика, пользователя и оценщика. Реализующие компоненты.

61. ГОСТ Р 15408:2002. Часть 3. ОЦЕНОЧНЫЙ УРОВЕНЬ ДОВЕРИЯ ОУД3 – Методическое тестирование и проверка. Область применения. Основные иерархические свойства - отличия от ОУД1,2. Взаимодействие разработчика, пользователя и оценщика. Реализующие компоненты.

62. ГОСТ Р 15408:2002. Часть 3. ОЦЕНОЧНЫЙ УРОВЕНЬ ДОВЕРИЯ ОУД4 – Методическое проектирование, тестирование и просмотр. Область применения. Основные иерархические свойства - отличия от ОУД1-3. Взаимодействие разработчика, пользователя и оценщика. Реализующие компоненты.

63. ГОСТ Р 15408:2002. Часть 3. ОЦЕНОЧНЫЙ УРОВЕНЬ ДОВЕРИЯ ОУД5 – Полуформальное проектирование и тестирование. Область применения. Основные иерархические свойства - отличия от ОУД1-4. Взаимодействие разработчика, пользователя и оценщика. Реализующие компоненты.

64. ГОСТ Р 15408:2002. Часть 3. ОЦЕНОЧНЫЙ УРОВЕНЬ ДОВЕРИЯ ОУД6 – Полуформальная верификацию проекта и тестирование. Область применения. Основные иерархические свойства - отличия от ОУД1-5. Взаимодействие разработчика, пользователя и оценщика. Реализующие компоненты.

65. ГОСТ Р 15408:2002. Часть 3. ОЦЕНОЧНЫЙ УРОВЕНЬ ДОВЕРИЯ ОУД7 – Формальная верификация проекта и тестирование. Область применения. Основные иерархические свойства - отличия от ОУД1-6. Взаимодействие разработчика, пользователя и оценщика. Реализующие компоненты.

66. Структура системы аттестации по требованиям безопасности информации.

67. Порядок проведения аттестации объектов информатизации по требованиям безопасности информации.

Студенты должны на первом практическом занятии выбрать наиболее близкую им тему доклада (темы докладов в пределах одной группы не должны повторяться). Следует подобрать литературу по рассматриваемой проблеме и проанализировать собранный материал, составить общее впечатление о проблеме:

1. обосновать актуальность темы и отразить ее во введении.
2. написать основное содержание работы;
3. изложить основные выводы по рассматриваемой теме;
4. оформить список используемой литературы (в случае, если на нее ссылался автор доклада).

***Оформление работы. Работа выполняется в виде отчета.*** Работа должна включать: титульный лист, оглавление, разбиение текста согласно плану, заключение, библиографический список литературы, приложения (в случае необходимости). Объем работы колеблется от 5 до 10 машинописных страниц.

Текст печатается, согласно соответствующему стандарту: через 1,5 интервала, 1800 знаков на странице, включая пробелы и знаки препинания. Размер левого поля – 20 мм, правого – 20 мм, верхнего и нижнего – по 20 мм.

При написании работы следует учитывать технические детали оформления, касающиеся правил цитирования, правил оформления таблиц (схем, диаграмм), правил сокращения и т. п.

Для устного доклада по выбранной теме следует подготовить презентацию, отражающую основные результаты (10–15 слайдов).

**Критерии оценивания:**

Количество возможных докладов в течение семестра - два. Доклады делаются на практических занятиях и публично обсуждаются. Баллы выставляются обучающимся согласно следующим критериям за один доклад:

**3 балла** – обучающийся подготовил и выступил с докладом, ответил на все вопросы слушателей по теме доклада, что позволяет высоко оценить уровень владения материалом;

**2 балла** – обучающийся подготовил и выступил с докладом, верно ответил на большинство вопросов слушателей по теме доклада, что позволяет оценить уровень владения материалом;

**1 балл** – обучающийся подготовил и выступил с докладом, ответил на большинство вопросов слушателей по теме доклада, но даваемые им ответы принципиально неверны;

**0 баллов** – обучающийся не делает доклад.

10.3 Практические задания

**Практическое задание №1.**

**«Предварительный анализ объекта информатизации»**

Задание:

1. В соответствии с номером в списке группы выбрать вариант объекта информатизации.

Вариант – номер по списку группы.

|  |  |
| --- | --- |
| **Номер варианта** | **Объект информатизации** |
| 1 | Отделение коммерческого банка |
| 2 | Поликлиника |
| 3 | Университет |
| 4 | Офис страховой компании |
| 5 | Рекрутинговое агентство |
| 6 | Интернет-магазин |
| 7 | Многофункциональный центр оказания государственных услуг (МФЦ) |
| 8 | Отделение полиции |
| 9 | Аудиторская компания |
| 10 | Дизайнерская фирма |
| 11 | Офис интернет-провайдера |
| 12 | Офис адвоката |
| 13 | Компания по разработке ПО для сторонних организаций |
| 14 | Агентство недвижимости |
| 15 | Туристическое агентство |
| 16 | Офис благотворительного фонда |
| 17 | Издательство |
| 18 | Консалтинговая фирма |
| 19 | Рекламное агентство |
| 20 | Отделение налоговой службы |
| 21 | Офис нотариуса |
| 22 | Паспортный стол (Управление Федеральной миграционной службы) |
| 23 | Научно-конструкторское бюро |
| 24 | Завод по производству металлопрокатного оборудования |
| 25 | Редакция газеты |
| 26 | Гостиница |
| 27 | Праздничное агентство |
| 28 | Городской архив |
| 29 | Диспетчерская служба такси |
| 30 | Железнодорожная касса |
| 31 | Городской суд |
| 32 | Городская Теплоэлектроцентраль (ТЭЦ) |
| 33 | Городской отдел судебных приставов |
| 34 | *Свой вариант (согласовывается с преподавателем)* |

1. Провести предварительное описание объекта информатизации по следующим пунктам:

Наименование объекта информатизации:

Тип деятельности:

Специфика организации работы:

Режим работы объекта:

Режим доступа на объект:

Штат сотрудников:

Посетители:

Инженерные системы:

Информационные системы:

Сведения, которые имеют конфиденциальный характер и требующие зашиты:

1. Подготовить Приказ «Об организации защиты информации на объекте информатизации», включающий в себя:
   * должностное лицо, ответственное за объект информатизации;
   * должностное лицо, назначенное администратором безопасности на объекте информатизации;
   * функциональные обязанности ответственных лиц по поддержанию заданного уровня безопасности информации на объекте информатизации;
   * перечень документов, которыми ответственные лица обязаны руководствоваться по вопросам защиты информации.

Контрольные вопросы:

1. Раскройте принципы государственной информационной политики.
2. Дайте определение понятию «национальная безопасность».
3. Опишите основные принципы обеспечения национальной безопасности России.
4. Перечислите национальные интересы и стратегические национальные приоритеты в соответствии со Стратегией национальной безопасности РФ.
5. Раскройте национальные интересы РФ в информационной сфере.
6. Опишите область применения Федерального закона «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ.
7. Дайте определение термину «конфиденциальность информации».
8. Опишите классификацию информации в зависимости от категории доступа к ней.
9. Опишите классификацию информации в зависимости от порядка ее предоставления или распространения.
10. Опишите базовые свойства (характеристики) информации.
11. Какими правами наделяется обладатель информации по №149-ФЗ?
12. Какие обязанности возложены на обладателя информации №149-ФЗ?
13. Опишите, к какой информации не может быть ограничен доступ.
14. Что является общедоступной информацией, какие права есть у обладателя общедоступной информации?
15. Дайте определение понятию «защита информации».
16. Какие требования обязан соблюдать обладатель информации в части ее защиты?

**Практическое задание 2.**

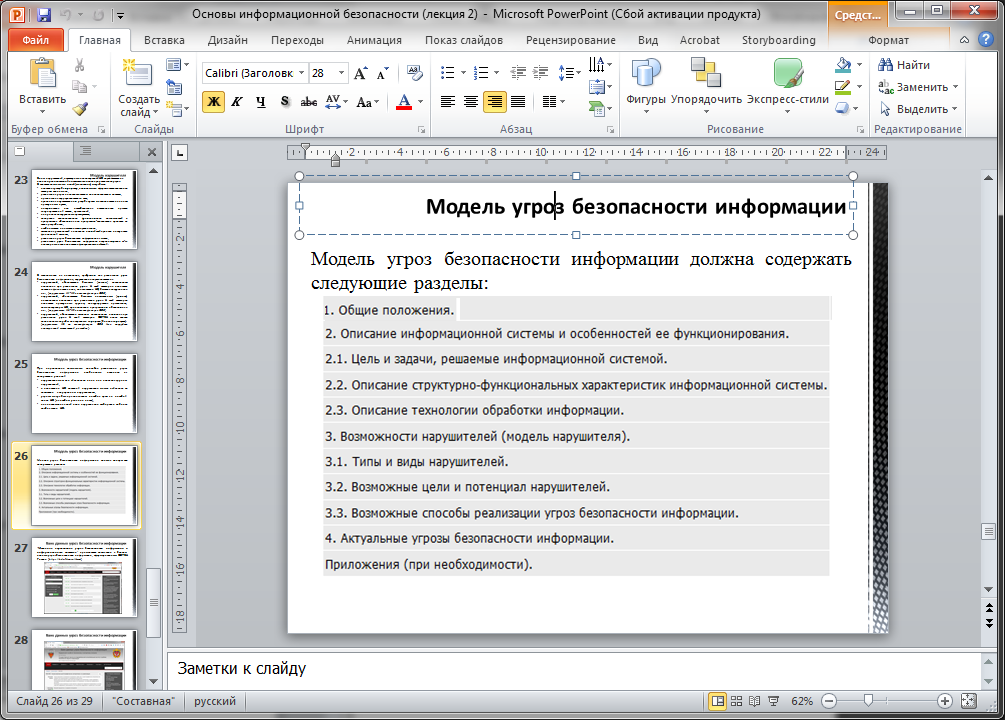
**«Разработка «Положение о защите конфиденциальной информации», «Перечень сведений конфиденциального характера» и «Модель угроз безопасности информации» (основании методических документов ФСТЭК России и банка данных угроз безопасности информации)».**

Задание:

1. В соответствии вариантом из практического занятия 1, разработать «Положение о защите конфиденциальной информации», содержащее разделы:

* общие сведения о документе, включая цель его разработки;
* коммерческая тайна (опционально);
* сведения служебного характера (опционально);
* информация банковского типа (опционально);
* налоговые данные (опционально);
* охрана конфиденциальных сведений;
* порядок предоставления и использования конфиденциальной информации;
* заключительные положения (виды санкций, которые применяются в отношении лиц, нарушивших режим работы с конфиденциальными сведениями).

1. В соответствии вариантом из практического занятия 1, разработать документ «Перечень сведений конфиденциального характера», содержащий таблицу с полями: № п/п, Наименование сведений, Примечание (отдел/наименование информационной системы).
2. На основании методического документа «Методика определения угроз безопасности информации в информационных системах» (https://fstec.ru/component/attachments/download/812) и банка данных угроз безопасности информации ФСТЭК (https://bdu.fstec.ru/threat) разработать в соответствии с вариантом «Модель угроз безопасности информации», содержащую следующие разделы:



Контрольные вопросы:

1. Опишите методику определения угроз безопасности информации в информационных системах при наличии статистических данных о реализации угроз.
2. Опишите методику определения угроз безопасности информации в информационных системах при отсутствии статистических данных о реализации угроз.
3. Опишите методику определения угроз безопасности информации в информационных системах на этапе создания информационных систем.
4. Как определяется итоговая степень возможного ущерба при обработке в информационной системе двух и более видов информации?
5. Перечислите случаи, при которых происходит переоценка угроз безопасности информации.
6. Перечислите основные виды нарушителей.
7. Раскройте основные цели (мотивы) при реализации угроз нарушителями.
8. Опишите принцип формирования модели нарушителя в соответствии с рекомендациями ФСТЭК.
9. Опишите этапы создания частной модели угроз при работе с базой данных угроз ФСТЭК.
10. Дайте общую классификацию факторов, воздействующих на защищаемую информацию.
11. Опишите классификацию технических каналов утечки информации.
12. Раскройте уровни защиты информации в соответствии с №149-ФЗ.
13. Перечислите основные виды защиты информации от несанкционированного доступа и неправомерных действий.
14. Опишите принцип формирования модели нарушителя в соответствии с методическими документами ФСБ.

**Практическое занятие 3.**

**Применение Microsoft Security Assessment Tool для оценки рисков информационной безопасности**

**Цель работы:**

Приобретение практических навыков оценки рисков организации (в соответствии с вариантом), связанных с информационной безопасность, на основе применения программного обеспечения Microsoft Security Assessment Tool (MSAT).

**Технические требования для выполнения работы:**

Компьютер или виртуальная машина с установленной ОС Windows, программа Microsoft Security Assessment Tool, подключение к сети Интернет.

**Описание работы:**

Установить и ознакомиться с программой Microsoft Security Assessment Tool для проведения оценки рисков, связанных с информационной безопасностью. Программное обеспечение Microsoft Security Assessment Tool доступно по ссылке:

<https://www.microsoft.com/ru-ru/download/confirmation.aspx?id=12273>

Данное приложение предназначено для анализа рисков информационной безопасности организаций, число сотрудников в которой не превышает 1000 человек. Данное ПО направлено на повышение уровня проработки потенциальных рисков в сфере безопасности.

В ходе работы пользователь, выполняющий роль аналитика, ответственного за вопросы безопасности, отвечает на две группы вопросов.

Первая группа вопросов посвящена бизнес-модели компании и направлена на оценку риска для бизнеса, с которым компания может столкнуться в данной отрасли и в условиях выбранной бизнес-модели. Создается профиль риска для бизнеса (ПРБ). Окно ввода сведений о компании представлено на рисунке 1.

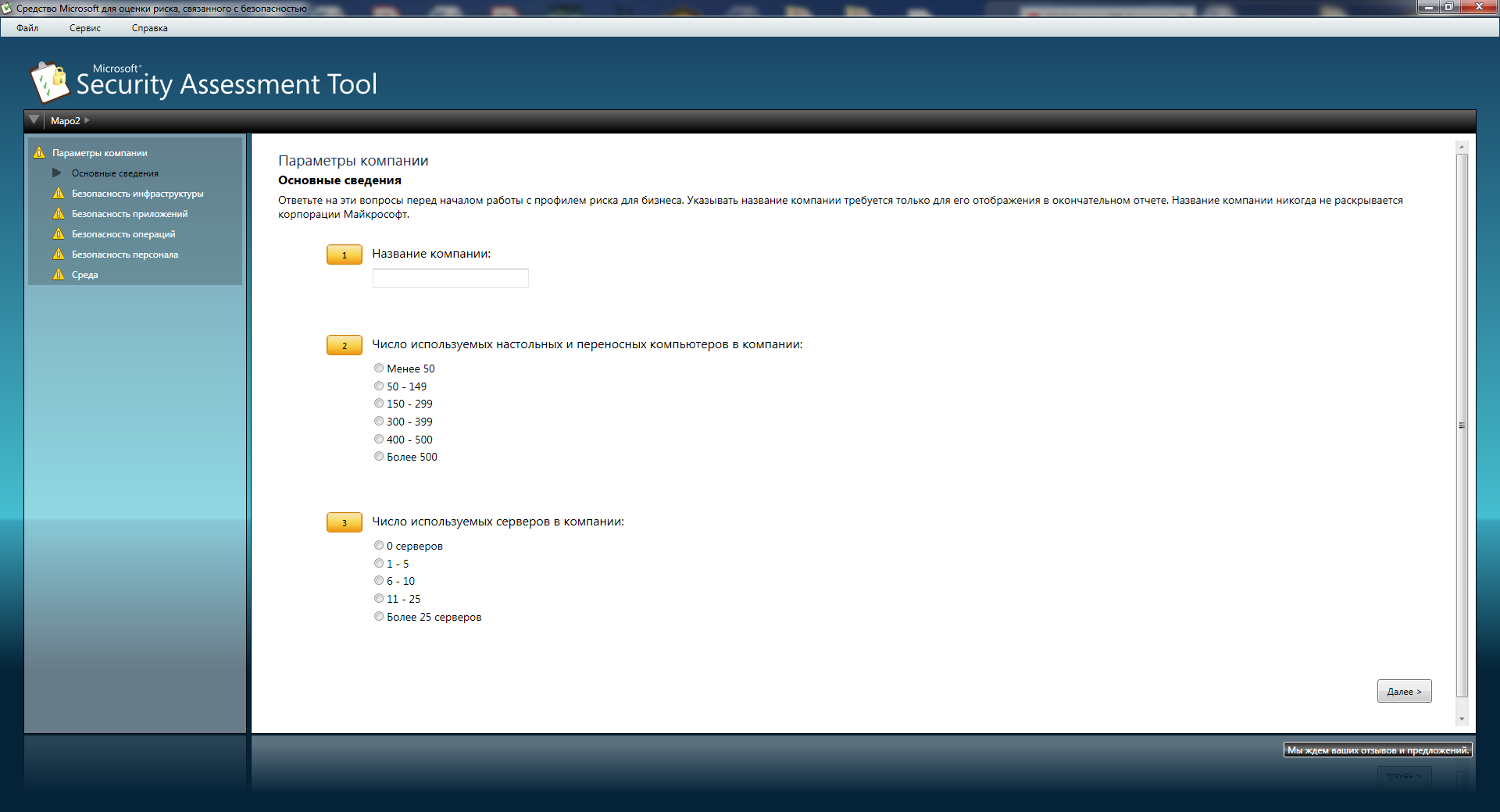


Рисунок 1. Ввод информации об организации.

Вопросы данного этапа разбиты на 6 групп:

* Основные сведения.
* Безопасность инфраструктуры.
* Безопасность приложений.
* Безопасность операций.
* Безопасность персонала.
* Среда.

Первая группа вопросов касается общих сведений о компании: название, число компьютеров, серверов и т.д.

Когда завершен первый этап оценки, полученная информация обрабатывается (для этого требуется подключение к сети Интернет), после чего начинается второй этап анализа. Для технический специалистов он является более понятным, так как касается используемых в компании политик, средств и механизмов защиты (рисунок 2). Данная группа вопросов подразделена на 4 блока:

* Инфраструктура.
* Приложения.
* Операции.
* Персонал.

Тематика вопросов соответствует разделам стандарта ISO 177799 и ISO 27001.

После ответа на все вопросы программа генерирует отчет (требуется подключение к сети Интернет). Наибольший интерес для специалистов по защите информации представляет формируемый «Полный отчет». В том числе данный отчет содержит предлагаемый список приоритетных действий для минимизации рисков. Фрагмент списка представлен на рисунке 3.

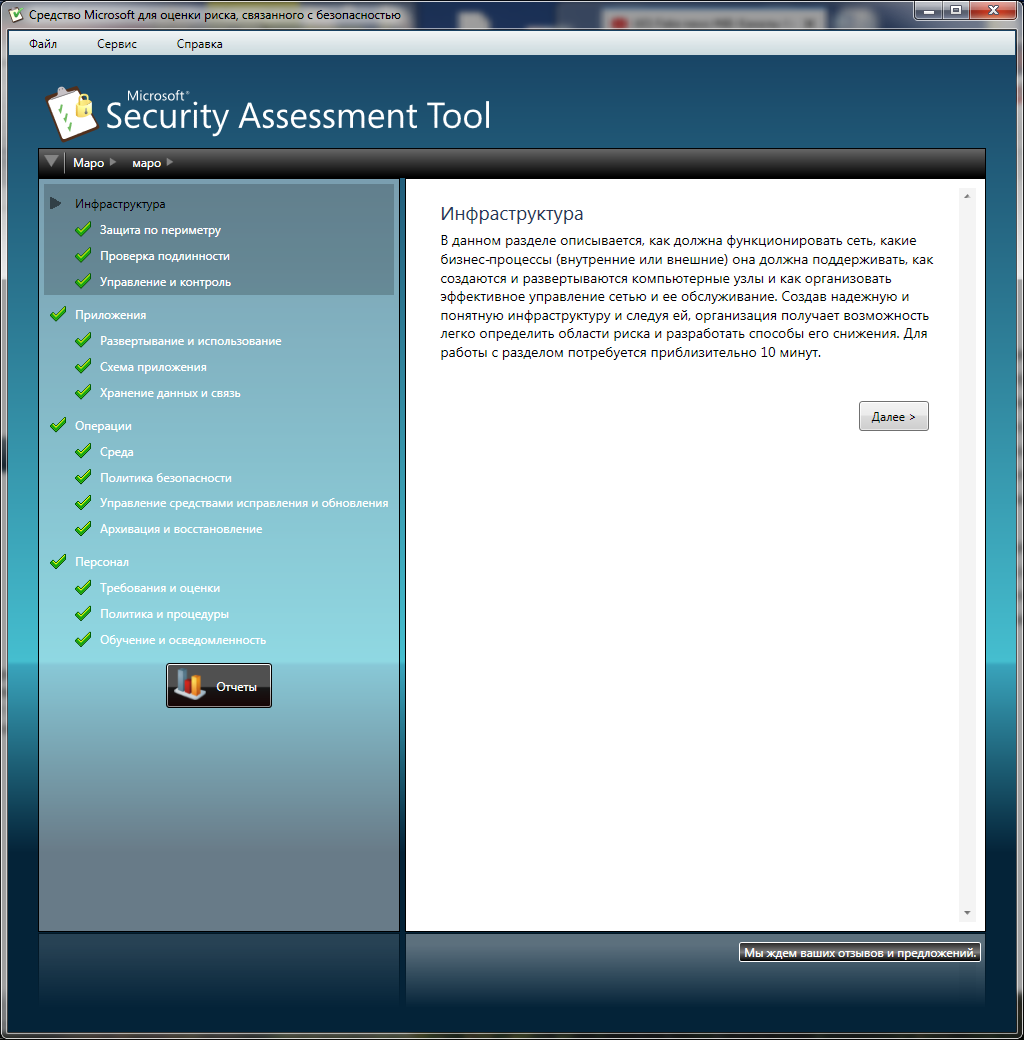


Рисунок 2. Анализ применяемых механизмов защиты информации.

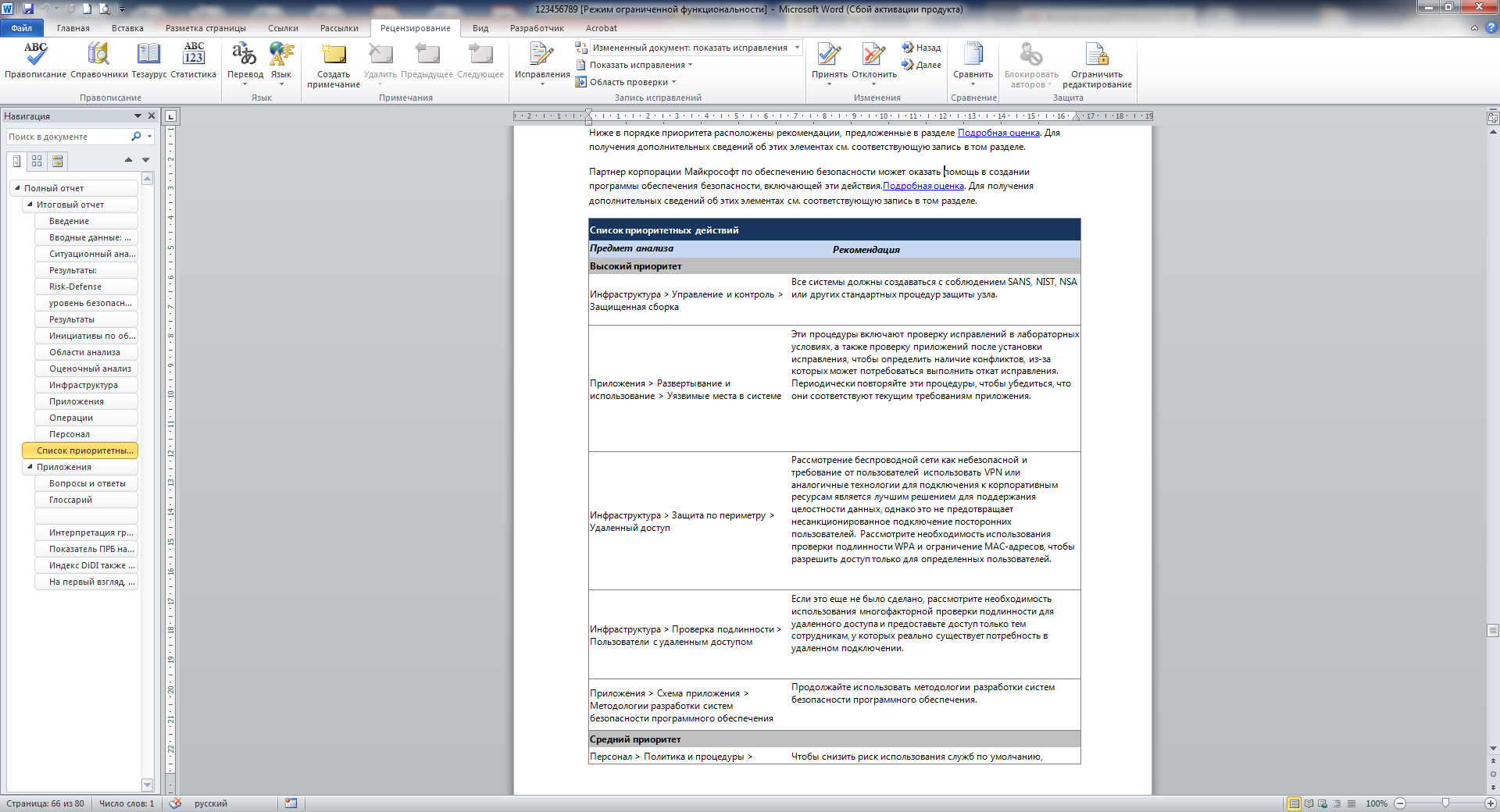


Рисунок 3. Рекомендации о приоритетных действиях.

**Задание:**

***!!! При работе с программой студенты должны создать новый профиль проверки в соответствии со своей фамилией и номером варианта исследуемой организации (рисунок 4).***

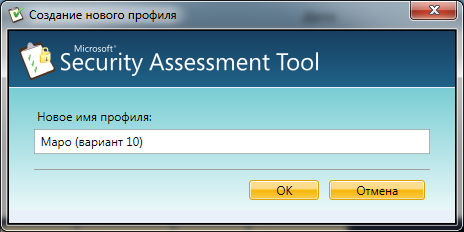


Рисунок 4. Создание нового профиля.

Провести с помощью программного обеспечения Microsoft Security Assessment Tool оценку рисков организации в соответствии с вариантом. Проанализировать полученный отчет и выделить основные риски информационной безопасности.

В печатную версию отчета следует включить:

1. Печатную версию Сводного ответа (рисунок 5).
2. Итоговые результаты рейтинга применяемых защитных мер (рисунок 6).
3. Инициативы по обеспечению безопасности (рисунок 7.)
4. Список приоритетных действий (рисунок 8).

**!!! На защите должна быть представлена электронная версия полного отчета.**

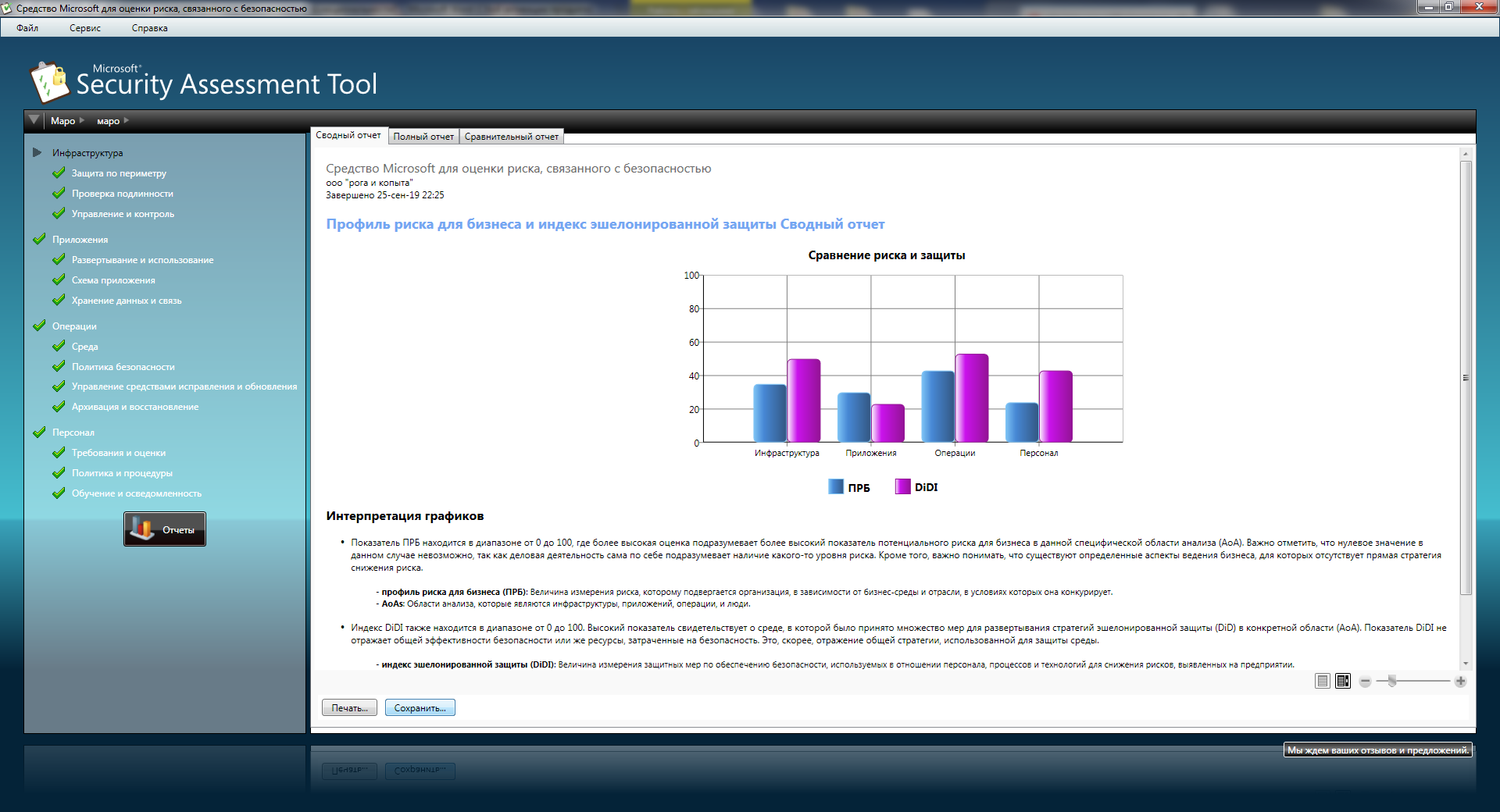


Рисунок 5. Окно просмотра сводного отчета.

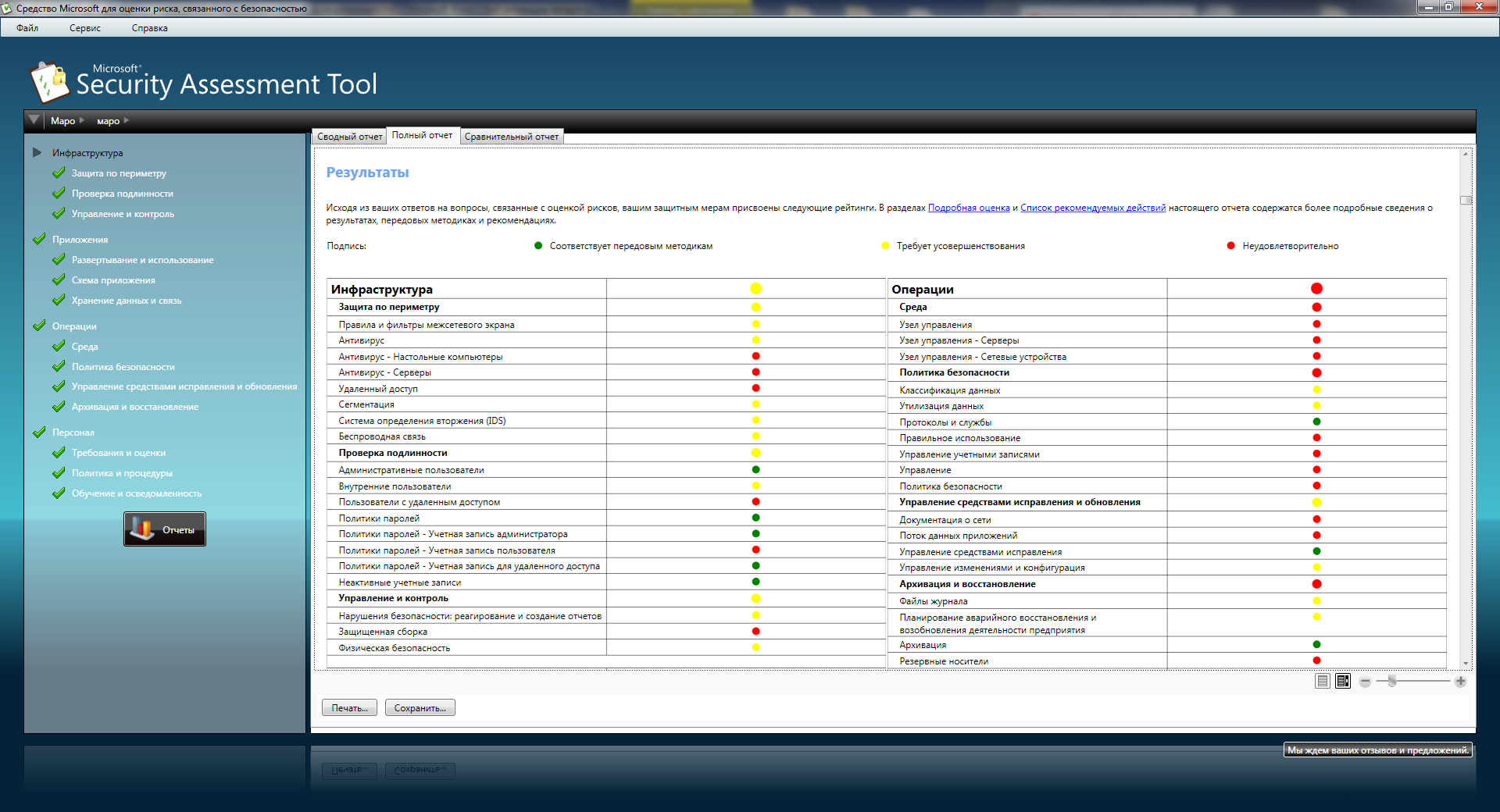


Рисунок 6. Рейтинг применяемых защитных мер.

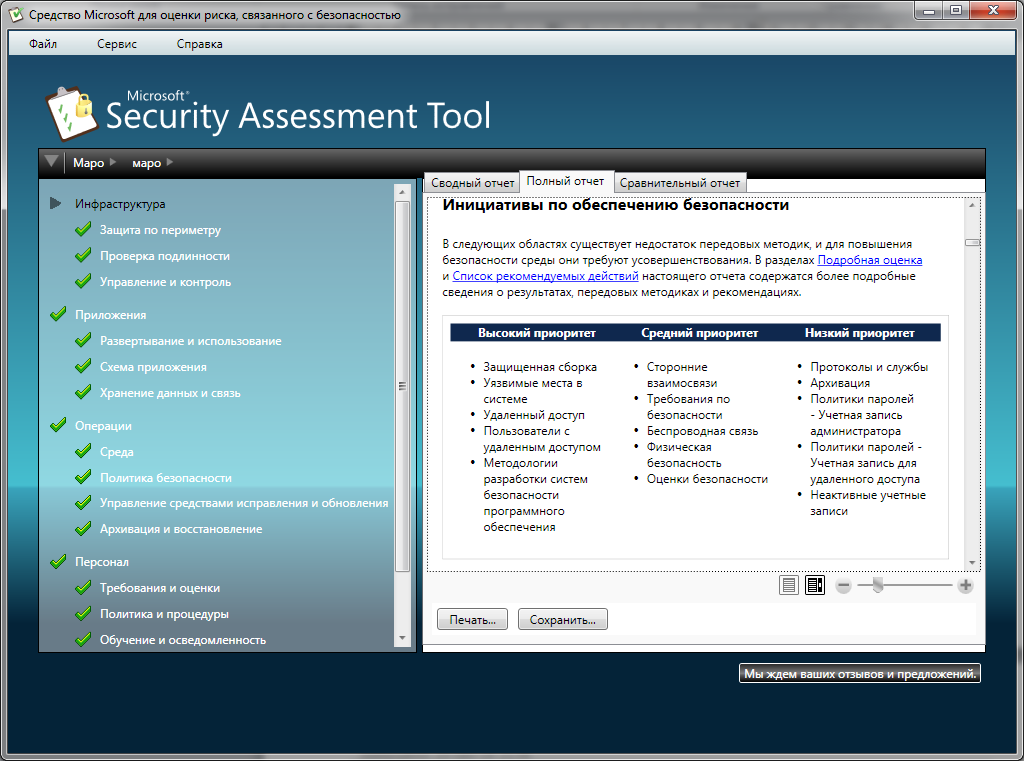


Рисунок 7. Инициативы по обеспечения безопасности.

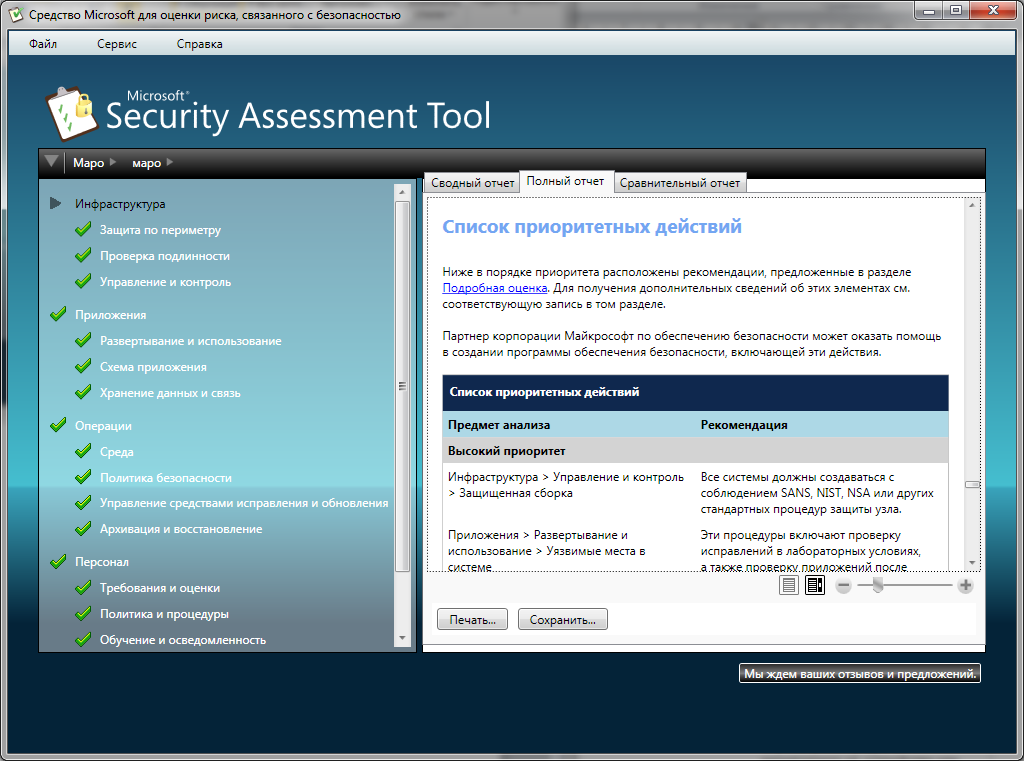


Рисунок 8. Список приоритетных действий.

Контрольные вопросы:

1. Дайте определения понятиям «угроза безопасности информации» и «уязвимость».
2. Раскройте классификацию уязвимостей информационных систем по области происхождения.
3. Раскройте классификацию уязвимостей информационных систем по типам недостатков.
4. Раскройте классификацию уязвимостей информационных систем по месту возникновения (проявления).
5. Опишите этапы определения угроз безопасности информации.
6. Перечислите источники угроз безопасности информации.

10.4 Контрольные работы по модулям 1 и 2

Контрольные работы предназначены для проведения рубежного контроля по модулю 1 и модулю 2 и позволяют оценить уровень сформированных знаний в рамках формируемых модулями дисциплины компетенций, в том числе в ходе самостоятельной работы обучающегося. Ниже приводятся вопросы, предлагаемые обучающимся в ходе выполнения контрольных работ. На каждой контрольной работе обучающемуся предлагается письменно подготовить ответы на два вопроса.

**Модуль 1.** «Основы защиты информации в компьютерных системах»

**Раздел 1.** **Национальная безопасность РФ, государственная информационная политика, виды безопасности, проблемы информационной безопасности, концепция национальной безопасности.**

1. Что такое концепция национальной безопасности?

2. В чем проблемы информационной безопасности?

3. Какова классификация защищаемой информации по видам?

4. Что понимается под информационной безопасностью и защитой информации?

5. Основные составляющие информационной безопасности?

6. Что понимается под угрозой безопасности информации?

7. По каким критериям осуществляется классификация угроз безопасности информации?

8. Основные методы реализации угроз информационной безопасности?

9. Что такое модель нарушителя?

**Раздел 2.** **Причины, виды и каналы утечки информации и факторы, воздействующие**

1. Каковы основные положения стандарта ГОСТ Р 50922-96?

2. Каковы основные причины, виды и каналы утечки информации?

3. Какова основная характеристика видов утечки информации: разглашение информации, несанкционированный доступ, получение защищаемой информации разведками?

4. Какова основная характеристика каналов утечки информации: электромагнитный, акустический (виброакустический), визуальный и информационный?

5. Каковы основные положения стандарта ГОСТ Р 50922-96?

6. Какова классификация факторов, влияющих на безопасность информации на предприятии?

**Раздел 3. Элементы теории компьютерной безопасности.**

1. Каковы процедуры входа в защищенную автоматизированную систему?

2. Каковы основные методы и средства аутентификации и контроля доступа?

3. Какие основные требования предъявляются к парольным системам аутентификации субъекта?

4. Каковы методы компрометации паролей и защиты от нее?

5. Как количественно оценить стойкость парольной системы?

6. Каковы основные модели безопасности и их отличительные особенности?

7. Каковы области применения мандатной, дискреционной и ролевой моделей управления доступом?

8. В чем состоят особенности биометрических средств аутентификации субъекта, их преимущества, недостатки и сфера применения?

**Раздел 4. Показатели и классы защищенности средств вычислительной техники (РД ГТК РФ).**

1. Классификация межсетевых экранов.

2. Анализ программного обеспечения на недекларированные возможности. Уровни контроля и требования к ним.

3. Классификация антивирусных средства защиты информации. Показатели защищенности и требования по защите от вирусов.

4. Виды вирусов и методы испытаний программных средств на наличие компьютерных вирусов (ГОСТ Р 51188-98).

**Раздел 5. Развитие стандартов по информационной безопасности.**

1. Каковы основные понятия и задачи стандартов по ИБ?

2. Как отражены критерии информационной безопасности в стандартах?

3. Каково взаимодействие между производителями, потребителями и экспертами по квалификации продуктов информационных технологий?

4. Каковы особенности Оранжевой книги (TCSEC)?

5. Какова структура и основные положения Федеральных (FCITS) и Канадских критериев (CTCPEC)?

6. В чем особенности Европейских критериев (ITSEC)?

7. Как современная методология оценки защищенность информационных технологий включает идеи предыдущих стандартов (Общие критерии и РД ГТК РФ)?

**Модуль 2.** «Методология обеспечения и оценки безопасности информационных систем»

**Раздел 6. Критерии защищенности компьютерных систем (РД ФСТЭК, ГОСТ 15408).**

1. Что такое концепция защиты от несанкционированного доступа?

2. Какова классификация защищенности автоматизированных систем и средств вычислительной техники?

3. Какова классификация защищенности межсетевых экранов, антивирусных средств?

4. Какова методика анализа программ на отсутствие недекларированных возможностей?

5. Каковы стандартные подходы для испытания программных средств на отсутствие вирусной инфекции?

**Раздел 7. Контекст оценки безопасности информационных технологий (ГОСТ 15408).**

1. Каковы базовые понятия и принципы Общих критериев (ГОСТ Р 15408)?

2. Что такое функциональные требования безопасности?

3. В чем особенности требования доверия безопасности?

4. Какова структура профиля защиты и как он используется?

5. В чем особенности задания по безопасности и какова область его применения?

**Раздел 8. Оценка информационной безопасности предприятия.**

1. Каковы основные аспекты стандартизации систем и процессов управления информационной безопасностью (ГОСТ 19791, ГОСТ 27001, СоbiT, NIST)?

2. Какова роль аудит информационной безопасности как инструмента обеспечения информационной безопасности?

3. Что такое процессный подход к обеспечению информационной безопасности?

4. Каковы особенности перехода от линейной модели управления качеством процессов и систем к замкнутой циклической модели менеджмента качества процессов и систем?

5. Каковы основные способы контроля и проверки процессов и систем?

6. Каковы цели контроля и проверки процессов и систем?

7. Каковы основные мероприятия по аудит информационной безопасности организаций и систем?

8. Каковы международные правовые аспекты, стандарты и руководства по основам аудита информационной безопасности?

**Раздел 9. Аудит информационной безопасности организаций и систем.**

1. Каков алгоритм менеджмента риска в системе управления информационной безопасностью по ГОСТ Р 27005?

2. Что такое оценка, обработка, принятие, коммуникация, мониторинг и пересмотр рисков?

3. Что такое системный подход к управлению рисками?

4. Что такое базовые критерии принятия решений по управлению рисками?

5. Как проводится идентификация активов, существующих средств управления рисками и последствий?

6. Что такое количественная оценка рисков?

7. Что такое базовый, неформальный, детальный и комбинированный виды анализа риска?

8. Какова область применения высокоуровневой и детальной оценок рисков информационной безопасности?

9. Каковы цели и задачи управления инцидентами ИБ?

10. Какова структура системы управления инцидентами?

11. Каково планирование и каковы этапы процесса управления инцидентами?

12. Что такое первая оценка и вторая оценка, подтверждение инцидента и реагирование на инциденты (немедленное, контролируемое, последующее реагирование)?

13. Как организуется на предприятии политика и программа управления инцидентами?

14. Каковы основные стандарты по управлению непрерывностью бизнеса (УНБ)?

**Раздел 10. Аттестация объектов информатизации по требованиям безопасности информации.** Функции ФСТЭК в рамках системы аттестации.

1. Какова структура системы аттестации по требованиям безопасности информации?

2. В каких случаях аттестация объекта информатизации является обязательной?

3. Опишите порядок проведения аттестации объектов информатизации по требованиям безопасности информации.

4. Какие функции в рамках системы аттестации выполняет испытательная лаборатория?

5. Какие функции в рамках системы аттестации выполняет орган по аттестации?

**Критерии оценки выполнения контрольных работ в каждом модуле.**

**7-10 баллов** – выставляется студенту, если он своевременно письменно ответил на все вопросы, предусмотренные в задании к контрольной работе, и сумел ответить на дополнительные вопросы, связанные не только с темами вопросов контрольной, но и с пониманием близких тем;

**5-6 балла** – выставляется студенту, если он выполнил все задания контрольной работы, и в процессе защиты продемонстрировал наличие достаточных теоретических знаний в объеме содержания учебной дисциплины, относящейся к данному модулю.

**1-4 баллов** – выставляется студенту, если он более чем на половину ответил на поставленные в контрольной работе вопросы, способен ответить на вопросы, касающиеся теоретической составляющей в объеме содержания данного модуля;

**0 баллов** – выставляется студенту в случае, если он не ответил ни на один вопрос контрольной работы.