Негосударственное образовательное частное учреждение высшего образования
«МЕЖДУНАРОДНЫЙ УНИВЕРСИТЕТ
ПСИХОЛОГО-ПЕДАГОГИЧЕСКИХ ИННОВАЦИЙ»

УТВЕРЖДАЮ:
Ректор
НОЧУ ВО «МУППИ»
_____ В.В. Борисова
подпись
«24» апреля 2025 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Основы управления информационной безопасностью

направление подготовки
38.03.02 Менеджмент

Профиль подготовки:
Менеджмент цифровых технологий

Квалификация (степень) выпускника – *бакалавр*

Форма обучения
очно-заочная

Москва 2025 г.

1. Перечень планируемых результатов изучения дисциплины, соотнесенных с планируемыми результатами освоения образовательной программы

В рамках освоения основной профессиональной образовательной программы бакалавриата обучающийся должен овладеть следующими результатами обучения по дисциплине «Основы управления информационной безопасностью»

Код и наименование компетенций	Индикаторы достижения компетенции
ПК-3. Способен разрабатывать, реализовывать и оценивать эффективность мероприятий по воздействию на риск реализации цифровых решений.	ИПК-3.1. Способен описывать бизнес-процессы с учетом риска, проводить качественную и количественную оценку рисков. ИПК-3.2. Способен обосновывать мероприятия по воздействию на риски и управлять их реализацией. ИПК-3.3. Способен проводить мониторинг системы управления рисками, актуализировать карты рисков по бизнес-процессам и направлениям бизнеса.

2. Место дисциплины в структуре ОПОП

Учебная дисциплина Б1.В.09 «Основы управления информационной безопасностью» относится к части, формируемой участниками образовательных отношений цикла Б.1 «Дисциплины (модули)».

3. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам занятий) и на самостоятельную работу обучающихся

Общая трудоемкость (объем) дисциплины «Основы управления информационной безопасностью» составляет 4 зачетные единицы.

Объём дисциплины по видам учебных занятий (в часах) – очно-заочная форма обучения

Вид учебной работы	Всего часов	Семестры	
		8	-
Аудиторные занятия (всего)	**36**	**36**	-
В том числе:	-	-	-
Лекции	18	18	-
Практические занятия (ПЗ)	18	18	-
Семинары (С)	-	-	-
Лабораторные работы (ЛР)	-	-	-
Самостоятельная работа (всего)	**72**	**72**	-
В том числе:	-	-	-
Курсовой проект (работа)	-	-	-
Расчетно-графические работы	-	-	-
Реферат	-	-	-
Подготовка к практическим занятиям	54	54	-
Тестирование	18	18	-
Вид промежуточной аттестации – экзамен	**36**	**36**	-
Общая трудоемкость час / зач. ед.	**144/4**	**144/4**	-

4. Содержание дисциплины

4.1. Разделы дисциплины и трудоемкость по видам учебных занятий

Очно-заочная форма обучения

№ п/п	Раздел/тема Дисциплины	Общая трудоёмкость	Виды учебных занятий, включая самостоятельную работу обучающихся, час		
			Контактная работа		Самостоятельная работа обучающихся
		Всего	лекции	практические занятия	
1.	Тема 1. Введение в информационную безопасность	8	2	-	6
2.	Тема 2. Обеспечение информационной безопасности общества как основа государственной информационной политики	8	-	2	6
3.	Тема 3. Информационная безопасность как предмет философско-политологического осмысления	8	2	-	6
4.	Тема 4. Информационная война: сущность, разновидности, средства и методы ведения	8	-	2	6
5.	Тема 5. Информационная безопасность политического пространства	8	2	-	6
6.	Тема 6. Информационная ответственность субъектов политических отношений	8	-	2	6
7.	Тема 7. Экономика информационной безопасности Идентификация рисков.	10	2	2	6
8.	Тема 8. Технические средства защиты информации	10	2	2	6
9.	Тема 9. Средства защиты информации в автоматизированных информационных системах	10	2	2	6
10.	Тема 10. Основы защиты данных персонального	10	2	2	6

№ п/п	Раздел/тема Дисциплины	Общая трудоёмкость	Виды учебных занятий, включая самостоятельную работу обучающихся, час		
			Контактная работа		Самостоятельная работа обучающихся
		Всего	лекции	практические занятия	
	компьютера				
11.	Тема 11. Основы безопасности в Интернете	10	2	2	6
12.	Тема 12. Методология построения защищенных автоматизированных информационных систем	10	2	2	6
Всего		**108**	**18**	**18**	**72**
Экзамен		**36**	**-**	**-**	**-**
Итого		**144**	**18**	**18**	**72**

4.2. Содержание разделов дисциплины

Тема 1. Введение в информационную безопасность

Назначение, задачи и общая характеристика курса, общие понятия и определения, краткая историческая справка. Данные и информация. Свойства информации. Представление информации и процессы ее обработки. Виды и формы представления информации. Носители информации. Информация как объект защиты. Определение и цели, механизмы, инструментарий, основные направления информационной безопасности. Информация и ресурсы. Информация как объект права собственности. Информация как коммерческая тайна. Информация как рыночный продукт.

Тема 2. Обеспечение информационной безопасности общества как основа государственной информационной политики

Государственная информационная политика, ее определение, сущность. Особенности государственной информационной политики в современной России. «Доктрина информационной безопасности Российской Федерации». Функциональные различия типов массово-информационной деятельности. Информационная агрессия и способы ее нейтрализации.

Понятие системы защиты информации. Виды обеспечения защиты информации. Служба информационной безопасности. Критерии необходимости создания. Основные понятия, задачи, функции, структура, принципы и этапы создания. Уровень подготовки специалистов. Подбор кадров. Взаимодействие с другими подразделениями организации. Оценка эффективности службы информационной безопасности.

Тема 3. Информационная безопасность как предмет философско-политологического осмысления

Определения понятия «безопасность» представителей разных философских школ. Динамика развития понятийного аппарата «безопасность». Информационная безопасность, ее специфика. Определение информационной безопасности. Объекты обработки и защиты информации. Классификация информационных систем и объектов, модель классификации. Классификация средств обработки информации: стандарт CCITSE. Требования к функциональности безопасности. Требования к достоверности безопасности. Проверка соответствия информации средствам работы с ней.

Тема 4. Информационная война: сущность, разновидности, средства и методы ведения

Понятия «информационная война», «информационное оружие». Разновидности информационной войны. «Стратегическое информационное противоборство первого поколения» и «Стратегическое информационное противоборство второго поколения», их сущность и различия. Технологии манипулятивного воздействия. «Пятая колонна», ее значение при ведении информационной войны. Понятие угрозы. Естественные и искусственные, случайные и преднамеренные, пассивные и активные, внешние и внутренние и т.п. угрозы. Источники угроз. Виды угроз: нарушение конфиденциальности, нарушение целостности, нарушение уровня доступности. Виды противников или "нарушителей". Модель нарушителя (злоумышленника). Типовые модели нападения. Классификация атак. Типовая атака: снаружи и внутри. Локальные атаки. Удаленные атаки. Атаки на поток данных: пассивные и активные.

Тема 5. Информационная безопасность политического пространства

Понятие политического пространства, различные подходы к его изучению. Трансформация политического пространства в информационное пространство политики. Границы информационного пространства политики. Субъекты информационного пространства политики, их способы взаимодействия, инструменты реализации интересов. Принципы и технологии обеспечения информационной безопасности, применяемые в разных странах мира.

Тема 6. Информационная ответственность субъектов политических отношений

Субъекты политики с точки зрения традиционной политологии. Особенности и значение СМИ как субъекта политики на современном этапе развития общества. Трансформация роли традиционных политических институтов. Информационное пространство, порождаемое субъектом политики.

Тема 7. Экономика информационной безопасности Идентификация рисков.

Объективные и субъективные вероятности реализации угроз посредством уязвимостей и их оценка. Измерение рисков, шкалы рисков. Формирование качественных и количественных оценок рисков. Оценки потерь. Технологии оценки угроз, уязвимостей, рисков и потерь. Оптимизация потерь, обоснование прогноза потерь и ущерба. Методика выбора компонентов системы защиты информации и предполагаемая оценка ее эффективности. Экономические проблемы информационных ресурсов; экономическая безопасность; информация как важнейший ресурс экономики; информация как товар, цена информации; основные подходы к определению затрат на защиту информации; система ресурсообеспечения защиты информации и эффективность ее использования; управление ресурсами в процессе защиты информации; виды ущерба, наносимые информации; степень наносимого ущерба информации; методы и способы страхования информации; формирование бюджета службы защиты информации; оценка эффективности защиты и страхования информации.

Тема 8. Технические средства защиты информации

Устройства и системы противоправного преднамеренного овладения конфиденциальной информацией. Технические средства защиты объектов. Инженерно-техническая защита. Системы охранной сигнализации на территории и в помещениях объекта обработки информации. Требования к системам охранной сигнализации. Наружные системы охраны. Традиционные системы. Ультразвуковые системы. Системы прерывания луча. Телевизионные системы. Радиолокационные системы. Микроволновые системы. Беспроводные системы. Система охранной (пожарной) сигнализации. Система хранения.

Интеграция систем контроля. Система контроля вскрытия аппаратуры. Требования, предъявляемые к системе контроля вскрытия аппаратуры. Защита информации от утечки за счет побочного электромагнитного излучения и наводок. Методы и средства защиты информации от случайных воздействий. Методы защиты информации от аварийных ситуаций. Биометрия, смарткарты.

Тема 9. Средства защиты информации в автоматизированных информационных системах

Классификация систем. Основные средства защиты информации: технические, программные, криптографические, организационные, законодательные. Средства контроля физического доступа. Автоматизированные средства защиты информации. Системы управления политикой безопасности. Автоматизированные системы как объекты защиты информации. Современное состояние классификации автоматизированных систем. Вычислительные сети. Сетевые модели доступа данных. Архитектура «файл-сервер». Архитектура «клиентсервер». Эталонная модель OSI. Масштабирование компьютерных сетей. Топология вычислительных сетей. Сегментация сложных локальных сетей. Персональные, локальные, корпративные, региональные и глобальные сети. Виртуальные сети. Автоматизированные системы управления. Классификация автоматизированных систем. Организация проектирования автоматизированных систем. Условия и режимы эксплуатации автоматизированных систем.

Тема 10. Основы защиты данных персонального компьютера

Организация рабочего места. Анализ возможных путей утечки информации. Программы контроля и разграничения доступа к информации. Задачи и общие принципы построения программ контроля и разграничения доступа к информации. Методы борьбы. Резервное копирование, контроль пользователей, защита файлов и папок. Схема защиты ПК. Защита BIOS. Системы защиты паролями Windows. Профили и пароли пользователей. Выбор значений паролей. Выбор носителей кодов паролей. Разграничение полномочий пользователей. Концепция построения систем контроля и разграничения доступа. Средства перекрытия путей обхода программ контроля и разграничения доступа. Оценка программ контроля и разграничения доступа как средства защиты. Контроль целостности программного обеспечения и информации. Дублирование информации. Средства защиты программного обеспечения и информации от несанкционированной загрузки. Защита информации на машинных носителях. Защита остатков информации. Защита информации в линиях связи. Защита информации при документировании. Удаленный доступ. Сетевая защита файлов и папок. Программы администрирования. Организационные мероприятия по защите информации в автоматизированных информационных системах.

Тема 11. Основы безопасности в Интернете

Угрозы. Классификация удаленных атак: по сценарию, по цели, по характеру взаимодействия с жертвой. Удаленный сбор информации. Выяснение адресов. Поиск уязвимостей. Наиболее распространенные классы удаленных атак. Вирусы и троянские программы. Отказ в обслуживании. Маскировка. Атаки на маршрутизацию. Атаки на серверы: CGI и HTTP. Атаки на клиентов: ActiveX, Java. Переполнение буфера. Пассивные атаки. Прослушивание сетей. Прослушивание в коммутируемых сетях Ethernet. Активные атаки. Атака повтором. Атака «злоумышленник-посредник». Атаки на основе сетевой маршрутизации. Перехват сессии. Инструменты злоумышленников. Классификация программ-шпионов и защита от них. Особенности защиты информации в базах данных. Обзор программных средств защиты. Обеспечение анонимности: службы анонимности, прокси-серверы. Сканеры уязвимости. Системы и технологии обнаружения атак. Топология

систем обнаружения атак. Автоматизированные средства управления политикой безопасности. Средства обеспечения безопасности работы в Интернете. Средства контроля и разграничения доступа. Программные шлюзы и проксисерверы. Межсетевые экраны. Функции межсетевого экранирования. Фильтрация трафика. Средства защиты трафика.

Тема 12. Методология построения защищенных автоматизированных информационных систем

Критерии защищенности. Анализ и оценка действующей концепции защиты. Выбор концептуальной модели построения защиты. Исходные данные для постановки задачи. Введение в проблему теории защиты информации. Общий методический подход. Основные принципы построения защитной оболочки. Модель элементарной защиты. Модель многозвенной защиты. Многоуровневая защита. Некоторые особенности точности расчета прочности защиты. Метод построения защиты информации в системах с сосредоточенной обработкой данных. Классификация возможных каналов НСД. Метод построения защиты информации в системах с распределенной обработкой данных.

4.3. Практические занятия / лабораторные занятия

Очно-заочная форма обучения

Занятие 1. Обеспечение информационной безопасности общества как основа государственной информационной политики

Занятие 2. Информационная война: сущность, разновидности, средства и методы ведения

Занятие 3. Информационная ответственность субъектов политических отношений

Занятие 4. Экономика информационной безопасности Идентификация рисков.

Занятие 5. Технические средства защиты информации

Занятие 6. Средства защиты информации в автоматизированных информационных систем

Занятие 7. Основы защиты данных персонального компьютера

Занятие 8. Основы безопасности в Интернете

Занятие 9. Методология построения защищенных автоматизированных информационных систем

5. Учебно-методическое и информационное обеспечение дисциплины

5.1. Основная литература

1. Капгер, И. В. Управление информационной безопасностью: учебное пособие / И. В. Капгер, А. С. Шабуров. — Пермь: ПНИПУ, 2023. — 91 с. — ISBN 978-5-398-02866-9. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/328889

2. Чекулаева, Е. Н. Управление информационной безопасностью: учебное пособие: [16+] / Е. Н. Чекулаева, Е. С. Кубашева; Поволжский государственный технологический университет. – Йошкар-Ола: Поволжский государственный технологический университет, 2020. – 156 с.: ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=612591

5.2. Дополнительная литература

1. Литвиненко, О. В. Правовые аспекты информационной безопасности: учебное пособие: [16+] / О. В. Литвиненко. – Новосибирск: Сибирский государственный университет телекоммуникаций и информатики, 2021. – 63 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=694774

2. Преступления в сфере высоких технологий и информационной безопасности: учебное пособие / В. Ф. Васюков, А. Г. Волеводз, М. М. Долгиева, В. Н. Чаплыгина. — Москва: Прометей, 2023. — 1086 с. — ISBN 978-5-00172-447-6. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/445748

5.3. Лицензионное программное обеспечение

1. Microsoft Windows 10 Pro
2. Microsoft Office 2007

5.4. Современные профессиональные базы данных и информационные справочные системы

1. ЭБС «Университетская библиотека онлайн» https://biblioclub.ru/index.php
2. Научная электронная библиотека http://www.elibrary.ru
3. Федеральный образовательный портал «Экономика. Социология. Менеджмент» http://ecsocman.hse.ru
4. Административно-управленческий портал http://www.aup.ru/
5. Официальный интернет-портал правовой информации http://pravo.gov.ru.
6. Компьютерные информационно-правовые системы «Консультант» http://www.consultant.ru, «Гарант» http://www.garant.ru.
7. Электронно-библиотечная система «Лань» https://e.lanbook.com/

6. Материально-техническое обеспечение дисциплины

1. Лекционная аудитория, аудитория для групповых и индивидуальных консультаций, оснащенная комплектом мебели для учебного процесса, учебной доской, персональным компьютером, плазменной панелью.
2. Аудитория информационных технологий, оснащенная комплектом мебели для учебного процесса, учебной доской, персональными компьютерами с возможностью подключения к сети «Интернет».
3. Аудитория для самостоятельной работы студентов, оснащенная комплектом мебели для учебного процесса, учебной доской, персональными компьютерами с возможностью подключения к сети «Интернет» и доступом к электронной информационно-образовательной среде Университета.

7. Методические рекомендации по организации изучения дисциплины

7.1. Методические рекомендации преподавателю

Данный раздел настоящей рабочей программы предназначен для начинающих преподавателей и специалистов-практиков, не имеющих опыта преподавательской работы.

Дисциплина «Основы управления информационной безопасностью» является дисциплиной, формирующей у обучающихся частично компетенцию ПК-3. В условиях конструирования образовательных систем на принципах компетентностного подхода произошло концептуальное изменение роли преподавателя, который, наряду с традиционной ролью носителя знаний, выполняет функцию организатора научно-поисковой работы обучающегося, консультанта в процедурах выбора, обработки и интерпретации информации, необходимой для практического действия и дальнейшего развития, что должно обязательно учитываться при проведении лекционных и практических занятий по дисциплине «Основы управления информационной безопасностью».

Преподавание теоретического (лекционного) материала по дисциплине «Основы управления информационной безопасностью» осуществляется на основе междисциплинарной интеграции и четких междисциплинарных связей в рамках образовательной программы и учебного плана по направлению 38.03.02 Менеджмент.

Подробное содержание отдельных разделов дисциплины «Основы управления информационной безопасностью» рассматривается в п.5 рабочей программы.

Методика определения итогового семестрового рейтинга обучающегося по дисциплине «Основы управления информационной безопасностью» представлена в составе ФОС по дисциплине в п 8 рабочей программы.

Примерные варианты тестовых заданий для текущего контроля и перечень вопросов к экзамену по дисциплине также представлены в п 8 рабочей программы.

Перечень основной и дополнительной литературы и нормативных документов, необходимых в ходе преподавания дисциплины «Основы управления информационной безопасностью», приведен в п.8 настоящей рабочей программы. Преподавателю следует ориентировать обучающихся на использование при подготовке к промежуточной аттестации оригинальной версии нормативных документов, действующих в настоящее время.

7.2. Методические указания обучающимся

Получение углубленных знаний по дисциплине достигается за счет активной самостоятельной работы обучающихся. Выделяемые часы целесообразно использовать для знакомства с учебной и научной литературой по проблемам дисциплины, анализа научных концепций.

В рамках дисциплины предусмотрены различные формы контроля уровня достижения обучающимися заявленных индикаторов освоения компетенций. Форма текущего контроля – активная работа на практических занятиях, подготовка и прохождение тестирования. Формой промежуточного контроля по данной дисциплине является экзамен, в ходе которого оценивается уровень достижения обучающимися заявленных индикаторов освоения компетенций.

Методические указания по освоению дисциплины.

Лекционные занятия проводятся в соответствии с содержанием настоящей рабочей программы и представляют собой изложение теоретических основ дисциплины.

Посещение лекционных занятий является обязательным.

Конспектирование лекционного материала допускается как письменным, так и компьютерным способом.

Регулярное повторение материала конспектов лекций по каждому разделу в рамках подготовки к текущим формам аттестации по дисциплине является одним из важнейших видов самостоятельной работы студента в течение семестра, необходимой для качественной подготовки к промежуточной аттестации по дисциплине.

Проведение практических занятий по дисциплине «Основы управления информационной безопасностью» осуществляется в следующих формах:

- анализ правовой базы, регламентирующей деятельность организаций различных организационно-правовых форм;
- опрос по материалам, рассмотренным на лекциях и изученным самостоятельно по рекомендованной литературе;
- решение типовых расчетных задач по темам;
- анализ и обсуждение практических ситуаций по темам.

Посещение практических занятий и активное участие в них является обязательным.

Подготовка к практическим занятиям обязательно включает в себя изучение конспектов лекционного материала и рекомендованной литературы для адекватного понимания условия и способа решения заданий, запланированных преподавателем на конкретное практическое занятие.

Методические указания по выполнению различных форм внеаудиторной самостоятельной работы

Изучение основной и дополнительной литературы, а также нормативно-правовых документов по дисциплине проводится на регулярной основе в разрезе каждого раздела в соответствии с приведенными в п.5 рабочей программы рекомендациями для подготовки к промежуточной аттестации по дисциплине «Основы управления информационной

безопасностью». Список основной и дополнительной литературы и обязательных к изучению нормативно-правовых документов по дисциплине приведен в п.7 настоящей рабочей программы. Следует отдавать предпочтение изучению нормативных документов по соответствующим разделам дисциплины по сравнению с их адаптированной интерпретацией в учебной литературе.

Решение задач в разрезе разделов дисциплины «Основы управления информационной безопасностью» является самостоятельной работой обучающегося в форме домашнего задания в случаях недостатка аудиторного времени на практических занятиях для решения всех задач, запланированных преподавателем, проводящим практические занятия по дисциплине.

Методические указания по подготовке к промежуточной аттестации

Промежуточная аттестация по дисциплине «Основы управления информационной безопасностью» проходит в форме экзамена. Примерный перечень вопросов к экзамену по дисциплине «Основы управления информационной безопасностью» и критерии оценки ответа обучающегося на экзамене для целей оценки достижения заявленных индикаторов сформированности компетенций приведены в составе ФОС по дисциплине в п 8 рабочей программы.

Обучающийся допускается к промежуточной аттестации по дисциплине независимо от результатов текущего контроля.

8. Фонд оценочных средств по дисциплине

8.1. Перечень компетенций с указанием этапов их формирования в процессе освоения дисциплины. Формы контроля формирования компетенций

Код и наименование компетенций	Индикаторы достижения компетенции	Форма контроля	Этапы формирования (разделы дисциплины)
ПК-3. Способен разрабатывать, реализовывать и оценивать эффективность мероприятий по воздействию на риск реализации цифровых решений.	ИПК-3.1. Способен описывать бизнес-процессы с учетом риска, проводить качественную и количественную оценку рисков. ИПК-3.2. Способен обосновывать мероприятия по воздействию на риски и управлять их реализацией. ИПК-3.3. Способен проводить мониторинг системы управления рисками, актуализировать карты рисков по бизнес-процессам и направлениям бизнеса.	Промежуточный контроль: экзамен Текущий контроль: опрос на практических занятиях; тестирование	Темы 1-9

8.2. Показатели и критерии оценивания компетенций при изучении дисциплины, описание шкал оценивания

8.2.1 Критерии оценки ответа на экзамене

(формирование компетенции ПК-3, индикаторы ИПК-3.1, ИПК-3.2., ИПК-3.3)

«5» (отлично): обучающийся демонстрирует системные теоретические знания, практические навыки, владеет терминами, делает аргументированные выводы и обобщения,

приводит примеры, показывает свободное владение монологической речью и способность быстро реагировать на уточняющие вопросы.

«4» (хорошо): обучающийся демонстрирует прочные теоретические знания, практические навыки, владеет терминами, делает аргументированные выводы и обобщения, приводит примеры, показывает свободное владение монологической речью, но при этом делает несущественные ошибки, которые быстро исправляет самостоятельно или при незначительной коррекции преподавателем.

«3» (удовлетворительно): обучающийся демонстрирует неглубокие теоретические знания, проявляет слабо сформированные навыки анализа явлений и процессов, недостаточное умение делать аргументированные выводы и приводить примеры, показывает не достаточно свободное владение монологической речью, терминами, логичностью и последовательностью изложения, делает ошибки, которые может исправить только при коррекции преподавателем.

«2» (неудовлетворительно): обучающийся демонстрирует незнание теоретических основ предмета, отсутствие практических навыков, не умеет делать аргументированные выводы и приводить примеры, показывает слабое владение монологической речью, не владеет терминами, проявляет отсутствие логичности и последовательности изложения, делает ошибки, которые не может исправить даже при коррекции преподавателем, отказывается отвечать на дополнительные вопросы.

8.2.2 Критерии оценки работы обучающегося на практических занятиях

(формирование компетенции ПК-3, индикаторы ИПК-3.1, ИПК-3.2., ИПК-3.3.)

«5» (отлично): выполнены все практические задания, предусмотренные практическими занятиями, обучающийся четко и без ошибок ответил на все контрольные вопросы, активно работал на практических занятиях.

«4» (хорошо): выполнены все практические задания, предусмотренные практическими занятиями, обучающийся с корректирующими замечаниями преподавателя ответил на все контрольные вопросы, достаточно активно работал на практических занятиях.

«3» (удовлетворительно): выполнены все практические задания, предусмотренные практическими занятиями с замечаниями преподавателя; обучающийся ответил на все контрольные вопросы с замечаниями.

«2» (неудовлетворительно): обучающийся не выполнил или выполнил неправильно практические задания, предусмотренные практическими занятиями; обучающийся ответил на контрольные вопросы с ошибками или не ответил на контрольные вопросы.

8.2.3 Критерии оценки тестирования

(формирование компетенции ПК-3, индикаторы ИПК-3.1, ИПК-3.2., ИПК-3.3.)

Тестирование оценивается в соответствии с процентом правильных ответов, данных обучающимся на вопросы теста.

Стандартная шкала соответствия результатов тестирования выставляемой балльной оценке:

- «отлично» - свыше 85% правильных ответов;
- «хорошо» - от 70,1% до 85% правильных ответов;
- «удовлетворительно» - от 55,1% до 70% правильных ответов;
- от 0 до 55% правильных ответов – «неудовлетворительно»

«5» (отлично): тестируемый демонстрирует системные теоретические знания, владеет терминами и обладает способностью быстро реагировать на вопросы теста.

«4» (хорошо): тестируемый в целом демонстрирует системные теоретические знания, владеет большинством терминов и обладает способностью быстро реагировать на вопросы теста.

«3» (удовлетворительно): системные теоретические знания у тестируемого отсутствуют, он владеет некоторыми терминами и на вопросы теста реагирует достаточно медленно.

«2» (неудовлетворительно): системные теоретические знания у тестируемого отсутствуют, терминологией он не владеет и на вопросы теста реагирует медленно.

8.2.4. Итоговое соответствие балльной шкалы оценок и уровней сформированности компетенций по дисциплине:

Уровень сформированности компетенции	Оценка	Пояснение
Высокий	«5» (отлично)	теоретическое содержание и практические навыки по дисциплине освоены полностью; все предусмотренные программой обучения учебные задания выполнены на высоком уровне; компетенции сформированы
Средний	«4» (хорошо)	теоретическое содержание и практические навыки по дисциплине освоены полностью; все предусмотренные программой обучения учебные задания выполнены с незначительными замечаниями; компетенции в целом сформированы
Удовлетворительный	«3» (удовлетворительно)	теоретическое содержание и практические навыки по дисциплине освоены частично, но пробелы не носят существенного характера; большинство предусмотренных программой обучения учебных задач выполнено, но в них имеются ошибки; компетенции сформированы частично
Неудовлетворительный	«2» (неудовлетворительно)	теоретическое содержание и практические навыки по дисциплине не освоены; большинство предусмотренных программой обучения учебных заданий либо не выполнено, либо содержит грубые ошибки; дополнительная самостоятельная работа над материалом не приводит к какому-либо значимому повышению качества выполнения учебных заданий; компетенции не сформированы

8.3. Методические материалы (типовые контрольные задания), определяющие результаты обучения по дисциплине, соотнесенные с индикаторами достижения

Контрольные задания, применяемые в рамках текущего контроля и промежуточной аттестации по дисциплине, носят универсальный характер и предусматривают возможность комплексной оценки всего набора заявленных по данной дисциплине индикаторов сформированности компетенций.

8.3.1. Текущий контроль (работа на практических занятиях)

(формирование компетенции ПК-3, индикаторы ИПК-3.1, ИПК-3.2., ИПК-3.3.)

Примерный перечень вопросов для обсуждения

Тема 1. Введение в информационную безопасность

Контрольные вопросы:

1. Данные и информация.

2. Свойства информации.

3. Виды и формы представления информации.

4. Информация как объект защиты.

5. Цели, механизмы, инструментарий, основные направления информационной безопасности.

Задание для самостоятельной работы:

Проведите дискуссию на предмет информации как объекта защиты.

Тема 2. Обеспечение информационной безопасности общества как основа государственной информационной политики

Контрольные вопросы:

1. Государственная информационная политика.

2. Особенности государственной информационной политики в современной России.

3. Информационная агрессия и способы ее нейтрализации.

4. Виды обеспечения защиты информации.

Задание для самостоятельной работы:

Проведите дискуссию на предмет особенностей государственной информационной политики в современной России.

Тема 3. Информационная безопасность как предмет философско-политологического осмысления

Контрольные вопросы:

1. Определения понятия «безопасность» представителей разных философских школ.

2. Динамика развития понятийного аппарата «безопасность».

3. Классификация информационных систем и объектов, модель классификации.

Задание для самостоятельной работы:

Проведите дискуссию на предмет развития понятийного аппарата «безопасность».

Тема 4. Информационная война: сущность, разновидности, средства и методы ведения

Контрольные вопросы:

1. Понятия «информационная война», «информационное оружие».

2. Разновидности информационной войны.

3. Технологии манипулятивного воздействия.

4. Источники угроз.

5. Виды угроз.

Задание для самостоятельной работы:

Проведите дискуссию на предмет источников и видов информационных угроз.

Тема 5. Информационная безопасность политического пространства

Контрольные вопросы:

1. Понятие политическое пространство.

2. Информационное пространство политики.

3. Субъекты информационного пространства политики.

4. Принципы и технологии обеспечения информационной безопасности.

Задание для самостоятельной работы:

Проведите дискуссию о технологиях обеспечения информационной безопасности.

Тема 6. Информационная ответственность субъектов политических отношений

Контрольные вопросы:

1. Субъекты политики с точки зрения традиционной политологии.

2. Особенности и значение СМИ как субъекта политики на современном этапе развития общества.

3. Трансформация роли традиционных политических институтов.

4. Информационное пространство, порождаемое субъектом политики.

Задание для самостоятельной работы:

Проведите дискуссию о информационном пространстве субъекта политики.

Тема 7. Экономика информационной безопасности

Контрольные вопросы:

1. Объективные и субъективные вероятности реализации угроз посредством уязвимостей и их оценка.

2. Измерение рисков, шкалы рисков.

3. Технологии оценки угроз, уязвимостей, рисков и потерь.

4. Методика выбора компонентов системы защиты информации и предполагаемая оценка ее эффективности.

5. Экономические проблемы информационных ресурсов.

6. Экономическая безопасность.

Задание для самостоятельной работы:

Проведите дискуссию о технологиях оценки угроз, уязвимостей, рисков и потерь.

Тема 8. Технические средства защиты информации

Контрольные вопросы:

1. Устройства и системы противоправного преднамеренного овладения конфиденциальной информацией.

2. Технические средства защиты объектов.

3. Инженерно-техническая защита.

4. Методы и средства защиты информации от случайных воздействий.

5. Методы защиты информации от аварийных ситуаций.

Задание для самостоятельной работы:

Проведите дискуссию о технических средствах защиты информационных объектов.

Тема 9. Средства защиты информации в автоматизированных информационных системах

Контрольные вопросы:

1. Средства защиты информации: технические, программные, криптографические, организационные, законодательные.

2. Автоматизированные средства защиты информации.

3. Системы управления политикой безопасности.

4. Вычислительные сети.

5. Сетевые модели доступа данных.

6. Архитектура «файл-сервер».

7. Архитектура «клиент-сервер».

8. Эталонная модель OSI.

9. Персональные, локальные, корпративные, региональные и глобальные сети.

10. Виртуальные сети.

Задание для самостоятельной работы:

Проведите дискуссию о системах управления политикой безопасности.

Тема 10. Основы защиты данных персонального компьютера

Контрольные вопросы:

1. Возможные пути утечки информации.

2. Программы контроля и разграничения доступа к информации.

3. Резервное копирование, контроль пользователей, защита файлов и папок.

4. Системы защиты паролями Windows. Профили и пароли пользователей.

5. Разграничение полномочий пользователей.

6. Контроль целостности программного обеспечения и информации.

7. Дублирование информации.

8. Сетевая защита файлов и папок.

9. Программы администрирования.

Задание для самостоятельной работы:

Проведите дискуссию о целостности программного обеспечения и информации.

Тема 11. Основы безопасности в Интернете

Контрольные вопросы:

1. Классификация удаленных атак: по сценарию, по цели, по характеру взаимодействия с жертвой.

2. Классы удаленных атак.

3. Вирусы и троянские программы.
4. Отказ в обслуживании.
5. Атаки на маршрутизацию.
6. Атаки на серверы: CGI и HTTP.
7. Атаки на клиентов: ActiveX, Java.
8. Переполнение буфера.
9. Пассивные атаки.
10. Активные атаки.
11. Программные средства защиты.
12. Средства защиты трафика.

Задание для самостоятельной работы:

Проведите дискуссию о удаленных информационных атаках.

Тема 12. Методология построения защищенных автоматизированных информационных систем

Контрольные вопросы:

1. Критерии защищенности.
2. Выбор концептуальной модели построения защиты.
3. Основные принципы построения защитной оболочки.
4. Модель элементарной защиты.
5. Модель многозвенной защиты.
6. Многоуровневая защита.
7. Метод построения защиты информации в системах с распределенной обработкой данных.

8.3.2. Текущий контроль (тестирование)

(формирование компетенции ПК-3, индикаторы ИПК-3.1, ИПК-3.2., ИПК-3.3.)

Примерные варианты тестовых заданий

Тест 1.

1. Меры защиты информационной безопасности направлены на защиту от:
1 нанесения неприемлемого ущерба;
2. нанесения любого ущерба;
3. вандализма.

2. Что из перечисленного не относится к числу основных аспектов информационной безопасности?
1. доступность;
2. целостность;
3. конфиденциальность;
4. правдивое отражение действительности.

3. Что такое защита информации?
1. защита от несанкционированного доступа к информации;
2. выпуск бронированных упаковок для дисков;
3.комплекс мероприятий, направленных на обеспечение информационной безопасности.

4 Что понимается под информационной безопасностью?
1.защита здоровья персонала;
2.защита от нанесения неприемлемого ущерба субъектам информационных отношений;
3.обеспечение информационной независимости России.

5. Самыми опасными угрозами являются:
1. непреднамеренные ошибки штатных сотрудников;
2. вирусные инфекции;
3. атаки хакеров.

6. Дублирование сообщений является угрозой:

1. доступности;
2.конфиденциальности;
3. целостности.
7. Агрессивное потребление ресурсов является угрозой:
1.доступности;
2.конфиденциальности;
3.целостности.
8. Согласно Закону «Об информации, информатизации и защите Информации»
персональные данные – это:
1.сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность;
2. данные, хранящиеся в персональном компьютере;
3. данные, находящиеся в чьей-либо персональной собственности.
9. Что нельзя отнести к функциям, выполняемым службой защиты информации:
1. финансовое обеспечение деятельности организации;
2. организация обучения персонала правилам соблюдения и поддержания
3.информационной безопасной деятельности предприятия;
4. материально-техническое и технологическое обеспечение информационной безопасности на предприятии.
10. Главная цель мер по защите информации, предпринимаемых на административном уровне:
1. сформировать программу безопасности и обеспечить еѐ выполнение;
2. выполнить положения действующего законодательства;
3 отчитаться перед вышестоящими инстанциями.
11. В число целей политики безопасности верхнего уровня входит:
1. решение сформировать или пересмотреть комплексную программу безопасности;
2.обеспечение базы для соблюдения законов и правил;
3. обеспечение конфиденциальности почтовых сообщений.
12. Какие виды страхования в рамках системы защиты информации возможны
1. страхование имущества и личное страхование;
2. страхование имущества, ответственности и личное страхование;
3. страхование имущества и ответственности.
13. В число этапов жизненного цикла информационного сервиса входят:
1.закупка;
2.продажа;
3.выведение из эксплуатации.
14.Ущерб от различных рисков потери информации включает
1. прямые и косвенные убытки;
2. упущенную выгоду предприятия от простоя атакованного узла;
3. прямые убытки от понесенного ущерба.
Тест 2
1. Политика безопасности:
1.фиксирует правила разграничения доступа;
2.отражает подход организации к защите своих информационных активов;
3. описывает способы защиты руководства организации.
2.В число этапов процесса планирования восстановительных работ после реализации угроз
входят:
1.выявление критически важных функций организации;
2.определения перечня возможных аварий;
3. проведение тестовых аварий.
3.В число принципов физической защиты входят:
1.беспощадный отпор;
2.непрерывность защиты в пространстве и времени;

3.минимизация защитных средств.

4. При оценке рисков информационной безопасности не по двум, а по трем факторам какой дополнительный фактор учитывается

1. цена потери;

2. вероятность происшествия;

3. вероятность угрозы.

5. К какому способу воздействия на риск относится способ страхование рисков

1. исключение риска

2. снижения вероятности возникновения риска

3. сохранение существующего уровня риска

6. Мониторинг, протоколирование и аудит могут использоваться для:

1. предупреждения нарушений ИБ;

2. обнаружение нарушений;

3. восстановление режима ИБ.

7. В число основных принципов архитектурной безопасности входят:

1.применение наиболее передовых технических решений;

2. применение простых апробированных решений;

3.сочетание простых и сложных защитных средств.

8. Контроль целостности может использоваться для:

1. предупреждения нарушений информационной безопасности;

2.обнаружения нарушений;

3.локализации последствий нарушений.

9.Обеспечение высокой доступности можно ограничить:

1.критически важными серверами;

2.сетевым оборудованием;

3. всей цепочкой от пользователей до серверов.

10 Предметная область «Защита информации» согласно ГОСТ Р 50922-96 – это:

1. деятельность (процесс), направленная на предотвращение утечки защищаемой информации;

2.специализаированная организация;

3.это самостоятельное структурное подразделение в рамках деятельности организации, тесно связана со службами охраны и объектового режима, составляет основу всей системы обеспечения информационной безопасности.

11. К организационным задачам и функциям службы защиты информации не относится:

1. разработка проектов защиты для каждого вида безопасности их реализация приемка и контроль их постоянной работоспособности;

2. организация проведения совместно с другими подразделениями мероприятий в отношении конкурентов,

3. взаимодействия с правоохранительными органами;

4. оказание управленческих воздействий на создание/поддержку своевременной реорганизации структуры управления безопасности предприятия.

12. Каковы требования к технологии управления безопасностью?

1.соответствие современному уровню развития информационных технологий;

2. выделение максимально возможных средств на защиту информации;

3. наличие обособленных субъектов в информационной системе.

13. На чем должно базироваться правовое обеспечение информационной безопасности:

1. соблюдение принципов законности;

2. комплексности и индивидуальности;

3. системности подходов;

4. балансе интересов в информационной сфере.

14. Действия Закона -О лицензировании отдельных видов деятельности‖ не распространяется на:

1.деятельность по технической защите конфиденциальной информации;
2.образовательную деятельность в области защиты информации;
3.предоставление услуг в области шифрования информации.

8.3.3. Промежуточный контроль (вопросы к экзамену)

(формирование компетенции ПК-3, индикаторы ИПК-3.1, ИПК-3.2., ИПК-3.3.)

Примерные вопросы к экзамену

1. Данные и информация.
2. Свойства информации.
3. Виды и формы представления информации.
4. Информация как объект защиты.
5. Цели, механизмы, инструментарий, основные направления информационной безопасности.
6. Государственная информационная политика.
7. Особенности государственной информационной политики в современной России.
8. Информационная агрессия и способы ее нейтрализации.
9. Виды обеспечения защиты информации.
10. Определения понятия «безопасность» представителей разных философских школ.
11. Динамика развития понятийного аппарата «безопасность».
12. Классификация информационных систем и объектов, модель классификации.
13. Понятия «информационная война», «информационное оружие».
14. Разновидности информационной войны.
15. Технологии манипулятивного воздействия.
16. Источники угроз.
17. Виды угроз.
18. Понятие политическое пространство.
19. Информационное пространство политики.
20. Субъекты информационного пространства политики.

15

21. Принципы и технологии обеспечения информационной безопасности.
22. Субъекты политики с точки зрения традиционной политологии.
23. Особенности и значение СМИ как субъекта политики на современном этапе развития общества.
24. Трансформация роли традиционных политических институтов.
25. Информационное пространство, порождаемое субъектом политики.
26. Объективные и субъективные вероятности реализации угроз посредством уязвимостей и их оценка.
27. Измерение рисков, шкалы рисков.
28. Технологии оценки угроз, уязвимостей, рисков и потерь.
29. Методика выбора компонентов системы защиты информации и предполагаемая оценка ее эффективности.
30. Экономические проблемы информационных ресурсов.
31. Экономическая безопасность.
32. Устройства и системы противоправного преднамеренного овладения конфиденциальной информацией.
33. Технические средства защиты объектов.
34. Инженерно-техническая защита.
35. Методы и средства защиты информации от случайных воздействий.
36. Методы защиты информации от аварийных ситуаций.
37. Средства защиты информации: технические, программные, криптографические, организационные, законодательные.
38. Автоматизированные средства защиты информации.

39. Системы управления политикой безопасности.
40. Вычислительные сети.
41. Сетевые модели доступа данных.
42. Архитектура «файл-сервер».
43. Архитектура «клиент-сервер».
44. Эталонная модель OSI.
45. Персональные, локальные, корпоративные, региональные и глобальные сети.
46. Виртуальные сети.
47. Возможные пути утечки информации.
48. Программы контроля и разграничения доступа к информации.
49. Резервное копирование, контроль пользователей, защита файлов и папок.
50. Системы защиты паролями Windows. Профили и пароли пользователей.
51. Разграничение полномочий пользователей.
52. Контроль целостности программного обеспечения и информации.
53. Дублирование информации.
54. Сетевая защита файлов и папок.
16
55. Программы администрирования.
56. Классификация удаленных атак: по сценарию, по цели, по характеру взаимодействия с жертвой.
57. Классы удаленных атак.
58. Вирусы и троянские программы.
59. Отказ в обслуживании.
60. Атаки на маршрутизацию.
61. Атаки на серверы: CGI и HTTP.
62. Атаки на клиентов: ActiveX, Java.
63. Переполнение буфера.
64. Пассивные атаки.
65. Активные атаки.
66. Программные средства защиты.
67. Средства защиты трафика.
68. Критерии защищенности.
69. Выбор концептуальной модели построения защиты.
70. Основные принципы построения защитной оболочки.
71. Модель элементарной защиты.
72. Модель многозвенной защиты.
73. Многоуровневая защита.
74. Метод построения защиты информации в системах с распределенной обработкой данных