МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Магнитогорский государственный технический университет им. Г.И. Носова»

УТВЕРЖДАЮ
Директор ИЭиАС
В.Р. Храмшин

26.01.2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Направленность (профиль/специализация) программы
.03.05 Педагогическое образование (с двумя профилями подготовки)

Направленность (профиль/специализация) программы
Информатика и экономика

Уровень высшего образования - бакалавриат

Форма обучения
очная

Институт/ факультет	Институт энергетики и автоматизированных систем
Кафедра	Бизнес-информатики и информационных технологий
Курс	4
Семестр	7

Магнитогорск
2022 год

Рабочая программа составлена на основе ФГОС ВО - бакалавриат по направлению подготовки 44.03.05 Педагогическое образование (с двумя профилями подготовки) (приказ Минобрнауки России от 22.02.2018 г. № 125)

Рабочая программа рассмотрена и одобрена на заседании кафедры Бизнес-информатики и информационных технологий 25.01.2022, протокол № 5

Зав. кафедрой _____ Г.Н. Чусавитина

Рабочая программа одобрена методической комиссией ИЭиАС 26.01.2022 г. протокол № 5

Председатель _____ В.Р. Храмшин

Рабочая программа составлена:
доцент кафедры БИиИТ, канд. пед. наук _____ Е.В. Чернова

Рецензент:
Генеральный директор ООО «Корпоративные системы Плюс», _____ Ю.А. Чудинова

Лист актуализации рабочей программы

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2023 - 2024 учебном году на заседании кафедры Бизнес-информатики и информационных

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ Г.Н. Чусавитина

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2024 - 2025 учебном году на заседании кафедры Бизнес-информатики и информационных

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ Г.Н. Чусавитина

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2025 - 2026 учебном году на заседании кафедры Бизнес-информатики и информационных

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ Г.Н. Чусавитина

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2026 - 2027 учебном году на заседании кафедры Бизнес-информатики и информационных

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ Г.Н. Чусавитина

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2027 - 2028 учебном году на заседании кафедры Бизнес-информатики и информационных

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ Г.Н. Чусавитина

1 Цели освоения дисциплины (модуля)

Цель дисциплины «Методы и средства защиты информации» - сформировать у бакалавров компетенции в области обеспечения охраны здоровья и жизни обучающихся при обращении с компьютерной техникой и программным обеспечением и, в особенности, в области применения различных сетевых технологий, а также практических навыков обеспечения защиты информации в системах обработки информации. Получить базовые знания, умения и навыки в области методов защиты информации для поддержки деятельности обучающихся в учебно-воспитательном процессе и внеурочной работе; для создания, формирования и администрирования электронных образовательных ресурсов с требуемым уровнем безопасности

2 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Методы и средства защиты информации входит в обязательную часть учебного плана образовательной программы.

Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:

Безопасность жизнедеятельности

Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:

Информационная безопасность в системе открытого образования

Подготовка к сдаче и сдача государственного экзамена

3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения

В результате освоения дисциплины (модуля) «Методы и средства защиты информации» обучающийся должен обладать следующими компетенциями:

Код индикатора	Индикатор достижения компетенции
УК-8 Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов	
УК-8.1	Анализирует и идентифицирует факторы опасного и вредного влияния элементов среды обитания (технических средств, технологических процессов, материалов, зданий и сооружений, природных и социальных явлений)
УК-8.2	Выявляет проблемы, связанные с нарушениями техники безопасности на рабочем месте; предлагает мероприятиях по предотвращению чрезвычайных ситуаций
УК-8.3	Разъясняет правила поведения при возникновении чрезвычайных ситуаций природного и техногенного происхождения; оказывает первую помощь, описывает способы участия в восстановительных мероприятиях

4. Структура, объём и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет 4 зачетных единиц 144 акад. часов, в том числе:

– контактная работа – 76,1 акад. часов:

– аудиторная – 72 акад. часов;

– внеаудиторная – 4,1 акад. часов;

– самостоятельная работа – 32,2 акад. часов;

– в форме практической подготовки – 0 акад. час;

– подготовка к экзамену – 35,7 акад. час

Форма аттестации - экзамен

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа студента	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код компетенции
		Лек.	лаб. зан.	практ. зан.				
1. Нормативно-правовые основы защиты информации								
1.1 Сущность и понятие информационной безопасности и защиты информации Основные понятия. Значение информационной безопасности для субъектов информационных отношений. Понятие и сущность защиты информации. Цели и концептуальные основы защиты информации. Критерии, условия и принципы отнесения информации к защищаемой. Носители защищаемой	7	4	2		2	Конспектирование учебных материалов Самостоятельное изучение учебной и научной литературы Подготовка к лабораторному занятию	Тестирование ЛР 1 «Надежность и достоверность информации»	УК-8.1
1.2 Правовое обеспечение информационной безопасности и защиты информации Назначение и структура правового обеспечения защиты информации. Правовые основы защиты информации в организации. Международные и национальные стандарты и спецификации в области ИБ. Современные стандарты в области управления рисками		4	4/4И		2	Конспектирование учебных материалов Самостоятельное изучение учебной и научной литературы Подготовка к семинарскому занятию по ЛР 2: проработка научно-методической литературы, доклад и презентация	Тестирование Выступление на семинаре по ЛР2 «Законодательная и нормативно-правовая база обеспечения информационной безопасности» Выступление на семинаре по ЛР3 «Стандарты и спецификации в области информационной безопасности»	УК-8.1

Итого по разделу		8	6/4И		4			
2. Классификация угроз и методов защиты информации								
2.1 Виды и источники угроз информационной безопасности Угрозы информационной безопасности и защиты информации. Дестабилизирующее воздействие на защищаемую информацию. Классификация видов угроз информационной безопасности по различным признакам. Несанкционированный	7	6	6/2И		4,2	Конспектирование учебных материалов Самостоятельное изучение учебной и научной литературы Подготовка к лабораторному занятию	Тестирование ЛР 4 «Классификация угроз предметной области»	УК-8.1, УК-8.2, УК-8.3
2.2 Классификация и характеристика основных методов и средств защиты Методы защиты информации. Способы защиты информации. Средства защиты информации		4			2	Конспектирование учебных материалов Самостоятельное изучение учебной и научной литературы Написание эссе-рассуждения	Тестирование Эссе «Методы защиты информации предметной области»	УК-8.1, УК-8.2
Итого по разделу		10	6/2И		6,2			
3. Уровни защиты информации: административный, программный, криптографический и технический								
3.1 Административный уровень обеспечения ИБ Политика безопасности. Программа безопасности. Оценка рисков и базовый уровень защиты. Управление персоналом. Физическая защита. Поддержание работоспособности. Реагирование на нарушения режима безопасности. Планирование восстановительных работ	7	4	8/6И		7	Конспектирование учебных материалов Самостоятельное изучение учебной и научной литературы Подготовка к семинарскому занятию по ЛР 4: проработка научно-методической литературы, доклад и презентация Подготовка к лабораторному занятию	Тестирование Выступление на семинаре по ЛР 5 «Политика информационной безопасности» ЛР 6 «Аудит защищенности сетей» ЛР 7 «Парольная защита и менеджеры паролей» ЛР 8 «Массовая рассылка писем»	УК-8.1, УК-8.2, УК-8.3

3.2 Программные средства защиты информации Защита программного обеспечения от несанкционированного доступа. Краткий обзор существующих на рынке средств защиты информации от несанкционированного доступа. Задача защиты от вмешательства посторонних лиц и аппаратные средства аутентификации. Стандарт CVSS «Общая		4	12		4	Конспектирование учебных материалов Самостоятельное изучение учебной и научной литературы Подготовка к лабораторному занятию	Тестирование ЛР 9 «Защита от несанкционированного доступа к информации» ЛР 10 «Защита информации в документах» ЛР 11 «Удаление информации» ЛР 12 «Восстановление данных» ЛР 13 «CVSS «Общая система оценки уязвимостей»»	УК-8.1, УК-8.2
3.3 Вирусы и антивирусные средства Определение компьютерных вирусов. Классификация компьютерных вирусов. Признаки заражения. Профилактика заражения. Программные антивирусные средства. Структура антивирусной программы. Принципы выбора сигнатуры		2			1	Конспектирование учебных материалов Самостоятельное изучение учебной и научной литературы	Тестирование	УК-8.1, УК-8.2
3.4 Криптографические методы защиты Методы криптографии. Средства криптографической защиты информации. Криптографические преобразования. Шифрование и дешифрование информации. Цифровая подпись		4	4/4И		10	Конспектирование учебных материалов Самостоятельное изучение учебной и научной литературы Подготовка к лабораторному занятию	Тестирование ЛР 13 «Защита информации с помощью криптографии» ЛР 14 «Защита информации с помощью стеганографии»	УК-8.1, УК-8.2
3.5 Технические средства защиты информации Инженерная защита объектов, защита информации от утечки по техническим каналам		4				Конспектирование учебных материалов Самостоятельное изучение учебной и научной литературы	Тестирование	УК-8.1, УК-8.2
Итого по разделу		18	24/10И		22			
Итого за семестр		36	36/16И		32,2		экзамен	
Итого по дисциплине		36	36/16И		32,2		экзамен	

5 Образовательные технологии

При проведении занятий и организации самостоятельной работы бакалавров ис-пользуются:

Традиционные технологии обучения, предполагающие передачу информации в го-товом виде, формирование учебных умений по образцу: лекция-изложение, лекция-объяснение, лабораторные работы, контрольная работа и др.

Использование традиционных технологий обеспечивает ориентирование студента в потоке информации, связанной с различными подходами к определению сущности, со-держания, методов, форм развития и саморазвития личности; самоопределение в выборе оптимального пути и способов личностно-профессионального развития; систематизацию знаний, полученных студентами в процессе аудиторной и самостоятельной работы. Лабораторные занятия обеспечивают развитие и закрепление умений и навыков определения целей и задач саморазвития, а также принятия наиболее эффективных решений по их реализации.

Интерактивные формы обучения, предполагающие организацию обучения как продуктивной творческой деятельности в режиме взаимодействия студентов друг с другом и с преподавателем

Использование интерактивных образовательных технологий способствует повышению интереса и мотивации учащихся, активизации мыслительной деятельности и творческого потенциала студентов, делает более эффективным усвоение материала, позволяет индивидуализировать обучение и ввести экстренную коррекцию знаний.

При проведении лабораторных занятий используются групповая работа, технология коллективной творческой деятельности, технология сотрудничества. Данные технологии обеспечивают высокий уровень усвоения студентами знаний, эффективное и успешное овладение умениями и навыками в предметной области, формируют познавательную потребность и необходимость дальнейшего самообразования, позволяют активизировать исследовательскую деятельность, обеспечивают эффективный контроль усвоения знаний

6 Учебно-методическое обеспечение самостоятельной работы обучающихся

Представлено в приложении 1.

7 Оценочные средства для проведения промежуточной аттестации

Представлены в приложении 2.

8 Учебно-методическое и информационное обеспечение дисциплины (модуля)

а) Основная литература:

1. Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. — 3-е изд. — Москва : РИОР : ИНФРА-М, 2021. — 400 с. — (Высшее образование). — DOI: https://doi.org/10.12737/1759-3. - ISBN 978-5-369-01759-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1210523 (дата обращения: 22.12.2021). – Режим доступа: по подписке

2. Сычев, Ю. Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2021. — 223 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/textbook_5cc15bb22f5345.11209330. - ISBN 978-5-16-014397-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/1189349 (дата обращения: 12.01.2022). – Режим доступа: по подписке.

б) Дополнительная литература:

1. Чернова, Е. В. Информационная безопасность человека : учебное пособие для вузов / Е. В. Чернова. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2022. — 243 с. — (Высшее образование). — ISBN 978-5-534-12774-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/495922 (дата обращения: 12.01.2022).

2. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2022. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/498844 (дата обращения: 12.01.2022).

3. Корабельников, С. М. Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. — Москва : Издательство Юрайт, 2022. — 111 с. — (Высшее образование). — ISBN 978-5-534-12769-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/496492 (дата обращения: 12.01.2022).

в) Методические указания:

1. Методические указания по выполнению лабораторных работ по дисциплине «Методы и средства защиты информации» для бакалавров направления 44.03.05 «Педагогическое образование (Информатика и экономика)». – Магнитогорск: Изд-во Магнитогорск. гос. техн. ун-та им. Г.И. Носова, 2020. – 30 с.

2. Методические указания по выполнению лабораторной работы «Надежность и достоверность информации» для бакалавров направления 38.03.05 Бизнес-информатика, 09.03.03 «Прикладная информатика», 44.03.05 «Педагогическое образование (Информатика и экономика)». – Магнитогорск: Изд-во Магнитогорск. гос. техн. ун-та им. Г.И. Носова, 2020. – 12 с.

3. Методические указания для оценки знаний студентов по дисциплине «Методы и средства защиты информации» для бакалавров направления 44.03.05 «Педагогическое образование (Информатика и экономика)» / Е.В. Чернова – Магнитогорск: Изд-во Магнитогорск. гос. техн. ун-та им. Г.И. Носова, 2022. – 35 с.

г) Программное обеспечение и Интернет-ресурсы:

Программное обеспечение

Наименование ПО	№ договора	Срок действия лицензии
MS Office 2007 Professional	№ 135 от 17.09.2007	бессрочно
7Zip	свободно распространяемое ПО	бессрочно
MS Office 2003 Professional	№ 135 от 17.09.2007	бессрочно
FAR Manager	свободно распространяемое ПО	бессрочно
Браузер Mozilla Firefox	свободно распространяемое ПО	бессрочно

Профессиональные базы данных и информационные справочные системы

Название курса	Ссылка
Национальная информационно-аналитическая система – Российский индекс научного цитирования (РИНЦ)	URL: https://elibrary.ru/project_risc.asp

Электронные ресурсы библиотеки МГТУ им. Г.И.	https://magtu.informsystema.ru/Marc.html?locale=ru
Университетская информационная система	https://uisrussia.msu.ru
Информационная система - Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические	https://fstec.ru/normotvorcheskaya/tekhnicheskaya-zashchita-informatsii
Информационная система - Банк данных угроз	https://bdu.fstec.ru/

9 Материально-техническое обеспечение дисциплины (модуля)

Материально-техническое обеспечение дисциплины включает:

Учебные аудитории для проведения занятий лекционного типа: специализированная (учебная) мебель (столы, стулья, доска аудиторная), мультимедийное оборудование (проектор, компьютер, экран) для презентации учебного материала по дисциплине;

Учебные аудитории для проведения лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации: специализированная (учебная) мебель (столы, стулья, доска аудиторная), персональные компьютеры объединенные в локальные сети с выходом в Internet и с доступом в электронную информационно-образовательную среду университета, оснащенные современными программно-методическими комплексами

Аудитории для самостоятельной работы (компьютерные классы; читальные залы библиотеки): специализированная (учебная) мебель (столы, стулья, доска аудиторная), персональные компьютеры объединенные в локальные сети с выходом в Интернет и с доступом в электронную информационно-образовательную среду университета, оснащенные современными программно-методическими комплексами

Помещение для хранения и профилактического обслуживания учебного оборудования: мебель (столы, стулья, стеллажи для хранения учебно-наглядных пособий и учебно-методической документации), персональные компьютеры.

Приложение 1

6 Учебно-методическое обеспечение самостоятельной работы обучающихся

По дисциплине «Методы и средства защиты информации» предусмотрена аудиторная и внеаудиторная самостоятельная работа бакалавров.

Аудиторная самостоятельная работа бакалавров предполагает решение и оформление согласно заданным требованиям заданий лабораторных работ. Требования к оформлению находятся в СМК-О-СМГТУ-42-09 Курсовой проект (работа): структура, содержание, общие правила выполнения и оформления.

Внеаудиторная самостоятельная работа студентов осуществляется в виде изучения учебной и научной литературы по соответствующему разделу с проработкой материала, участие в дистанционном курсе или изучении МООК, предложенном преподавателем и выполнения домашних заданий (подготовка к лабораторным работам) с консультациями преподавателя.

Вопросы для самостоятельного изучения:

1. Проведите сравнительный анализ доктрин и концепций государств США, Германии, Франции, Японии и других развитых стран в области обеспечения развития информационных технологий (концепции Клинтона-Гора, Банntемана в Европе, Окинавская хартия «Глобальное информационное общество» и т.д.)
2. Изучите совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации в «Доктрине информационной безопасности российской федерации», утвержденной 9 сентября 2000 г. № Пр-1895.
3. Познакомьтесь со статьями основного закона Российской Федерации — Конституцией (принятой 12 декабря 1993 года), затрагивающими вопросы информационной безопасности (статьи 23, 24, 29, 41, 42).
4. Рассмотрите определения всех важнейших компонентов информационной деятельности и направления развития законодательства в области информационной безопасности в законе «Об информации, информатизации и защите информации» от 20 февраля 1995 года номер 24-ФЗ (принят Государственной Думой 25 января 1995 года).
5. Изучите основные нормативные акты, регламентирующие охраны объектов с помощью норм авторского права в законах «О правовой охране программ для электронно-вычислительных машин и баз данных», «О правовой охране топологии интегральных микросхем» и «Об авторском праве и смежных правах».
6. Как определены понятия банковская, коммерческая и служебная тайна в Гражданском кодексе Российской Федерации.
7. Как отражены вопросы правового режима информации с ограниченным доступом в законах о государственной и коммерческой тайнах, в гражданском кодексе РФ в статье 139 «Служебная и коммерческая тайна».
8. Какие сведения **не** относятся к коммерческой тайне.
9. Как определяется понятие и содержание конфиденциальной информации в Указе Президента РФ «Об утверждении перечня сведений конфиденциального характера».
10. Дайте характеристику следующих форм защиты информации: патентование, авторское право, товарные знаки («Патентный закон РФ», «О товарных знаках, знаках обслуживания и наименовании мест происхождения товаров»).
11. Рассмотрите вопросы лицензирования в области защиты информации в законе «О лицензировании отдельных видов деятельности» от 8 августа 2001 года номер 128-ФЗ (Принят Государственной Думой 13 июля 2001 года).
12. Какими государственными правовыми документами определяются действия по защите информации от несанкционированного доступа.
13. Определите роль и место Федеральной службы по техническому и экспортному контролю (ФСТЭК, www.fstec.ru), являющейся правопреемником

Государственной технической комиссии при Президенте Российской Федерации (www.infotecs.ru/gtc/)

14. Каковы основные направления деятельности Федерального агентства правительственной связи и информации (ФАПСИ – www.fagci.ru) в государственной системе защиты информации.

15. Каковы основные направления деятельности «Совета Безопасности Российской Федерации».

16. Значение закона «Об участии в международном информационном обмене» от 4 июля 1996 года номер 85-ФЗ (принят Государственной Думой 5 июня 1996 года) в эпоху глобальных коммуникаций.

17. Рассмотрите законопроекты и существующую нормативно-правовую базу по вопросам электронного бизнеса и документооборота. Каким образом обеспечиваются правовые условия использования электронной цифровой подписи в электронных документах согласно закону «Об электронной цифровой подписи» № 1-ФЗ (принятому Государственной Думой 13 декабря 2001 года).

18. Познакомьтесь со статьями Кодекса об административных правонарушениях по проблемам правонарушений в области связи и информации (Глава 13).

19. Изучите статьи Уголовного кодекса Российской Федерации (редакция от 14 марта 2002 года) предусматривающие уголовную ответственность за компьютерные преступления.

20. Глава 28 «Преступления в сфере компьютерной информации», три статьи:

21. статья 272. Неправомерный доступ к компьютерной информации;

22. статья 273. Создание, использование и распространение вредоносных программ для ЭВМ;

23. статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

24. Познакомьтесь со статьями УК РФ под действие которых могут попадать противоправные деяния, совершенные с использованием компьютера и/или сети. Статьи – 129, 130, 137, 138, 146, 147, 158, 159, 163, 165, 167, 168, 171, 182, 183, 200, 242, 276, 280, 282, 283, 354.

25. Приведите примеры судебной практики в рассматриваемой сфере. Используйте материалы периодической печати, публикации в Интернет.

26. Сделайте обзор международного информационного законодательства (США, Германии, Великобритании, Франции, Японии) в области защиты информации.

27. Рассмотрите правовое регулирование сети Интернет в странах Европы, США, России.

28. Познакомьтесь с программой «Электронная Россия». Каковы результаты реализации данной программы?

29. Оценочные стандарты и технические спецификации. Основные понятия.

30. Стандарт Министерства обороны США «Критерии оценки доверенных компьютерных систем» (Department of Defense Trusted Computer System Evaliation Criteria, TCSEC, [TCSEC]) («Оранжевая книга») как оценочный стандарт. История создания и текущий статус. Политика безопасности согласно «Оранжевой книге». Классы безопасности информационных систем по степени доверия безопасности («Оранжевая книга»).

31. Красная книга. Интерпретация критериев оценки надежности систем для сетей. Trusted Network Interpretation. 1993. (NCSC-tg-005).

32. Розовая книга. Интерпретация системы управления надежной базой данных в критериях оценки надежных компьютерных систем Министерства обороны из числа критериев оценки надежных компьютерных систем. Trasted Database Management System Interpretation of the Trusted Computer System Evaluation Criteria. NCSC, 1991, (NCSC-TG-021).

33. Информационная безопасность распределенных систем. Рекомендации X.800 «Архитектура безопасности для взаимодействия открытых систем».

34. Спецификация Internet-сообщества RFC 1510 «Сетевой сервис аутентификации Kerberos (V5)» [Kerb].

35. Государственные стандарты. ГОСТ Р ИСО/МЭК 15408-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий (в русскоязычной литературе обычно, но не совсем верно, именуемый «Общие критерии» -ОК). Основные понятия и идеи. (Международный стандарт ISO/IEC 15408).

36. ГОСТ Р ИСО/МЭК 15408 – «Введение и общая модель». Общий подход к формированию требований и оценке безопасности (функциональные и доверия), основные конструкции (профиль защиты, задание по безопасности) представления требований безопасности в интересах потребителей, разработчиков и оценщиков продуктов и систем ИТ. Требования безопасности объекта оценки (ОО) по методологии Общих критериев определяются исходя из целей безопасности, которые, в свою очередь, основываются на анализе назначения ОО и условий среды его использования (угроз, предположений, политики безопасности).

37. ГОСТ Р ИСО/МЭК 15408-2 – «Функциональные требования безопасности». Классификация функциональных требований безопасности «Общих критериев». Классы функциональных требований, описывающие элементарные сервисы безопасности. Классы функциональных требований, описывающие производные сервисы безопасности.

38. Защита данных пользователя. Защита функций безопасности объекта оценки.

39. Классы функциональных требований, играющие инфраструктурную роль.

40. ГОСТ Р ИСО/МЭК 15408-3 – «Требования доверия к безопасности». Основные понятия и классификация требований доверия безопасности.

41. Оценка профилей защиты и заданий по безопасности. Требования доверия к этапу разработки. Требования к этапу получения, представления и анализа результатов разработки. Требования к поставке и эксплуатации, поддержка доверия

42. Оценочные уровни доверия безопасности в «Общих критериях».

43. Профили защиты, разработанные на основе «Общих критериев». Общие требования к сервисам безопасности. Биометрическая идентификация и аутентификация.

44. Британский стандарт BS 7799 «Управление информационной безопасностью. Практические правила» (Code of practice for information security management) [BS7799] и его вторая часть BS 7799-2:2002 «Системы управления информационной безопасностью - спецификация с руководством по использованию» (Information security management systems - Specification with guidance for use) [BS7799-2] для практического создания и поддержания режима информационной безопасности с помощью регуляторов административного и процедурного уровней. Регуляторы безопасности и реализуемые ими цели. Четырехфазная модель процесса управления информационной безопасностью.

45. Стандарт ISO/IEC 17799:2002 «Управление информационной безопасностью – Информационные технологии».

46. Федеральный стандарт США FIPS 140-2 "Требования безопасности для криптографических модулей" (Security Requirements for Cryptographic Modules) [FIPS140].

47. Требования к произвольному (дискреционному) управлению доступом. Руководящий документ Гостехкомиссии России «Безопасность информационных технологий. Контролируемый доступ. Профиль защиты» (ПЗ КД).

48. Требования к принудительному (мандатному) управлению доступом. Руководящий документ Гостехкомиссии России «Безопасность информационных технологий. Меточная защита. Профиль защиты» (ПЗ МЗ).

49. Ролевое управление доступом.

50. Межсетевое экранирование. Руководящие документы Гостехкомиссии России (Классификация автоматизированных систем (АС) по уровню защищенности от несанкционированного доступа (НСД), Классификация межсетевых экранов).

51. Системы активного аудита. Анонимизаторы. Выпуск и управление сертификатами. Анализ защищенности.

52. Профили защиты, разработанные на основе «Общих критериев». Частные требования к комбинациям и приложениям сервисов безопасности. Операционные системы.

53. Частные требования к комбинациям и приложениям сервисов безопасности. Системы управления базами данных.

54. Частные требования к комбинациям и приложениям сервисов безопасности. Виртуальные частные сети. Виртуальные локальные сети. Смарт-карты.

55. Гармонизированные критерии Европейских стран.

56. Техническая спецификация «Обобщенный прикладной программный интерфейс службы безопасности» (Generic Security Service Application Program Interface, GSS-API) [GSS-API].

57. Основные понятия и идеи рекомендаций семейства X.500. X.501 "Служба директорий: модели" [X501] и X.511 "Служба директорий: абстрактное определение сервиса" [X511].

58. Каркас сертификатов открытых ключей. X.509 "Служба директорий: каркасы сертификатов открытых ключей и атрибутов" (The Directory: Public-key and attribute certificate frameworks) [X509].

59. Каркас сертификатов атрибутов. Простая и сильная аутентификация.

60. Спецификации Internet-сообщества IPsec. Архитектура средств безопасности IP-уровня.

61. Спецификации Internet-сообщества IPsec Контексты безопасности и управление ключами.

62. Протокольные контексты и политика безопасности.

63. Обеспечение аутентичности IP-пакетов. Обеспечение конфиденциальности сетевого трафика.

64. Основные идеи и понятия протокола TLS. Протокол передачи записей. Протокол установления соединений и ассоциированные протоколы. Применение протокола HTTP над TLS.

65. Обобщенный прикладной программный интерфейс службы безопасности. Основные понятия.

66. Обобщенный прикладной программный интерфейс службы безопасности Функции для работы с удостоверениями. Создание и уничтожение контекстов безопасности. Защита сообщений. Логика работы пользователей интерфейса безопасности.

67. Структура и содержание документа «Политика информационной безопасности организации».

68. Служба информационной безопасности организации. Состав, цели и задачи службы информационной безопасности организации.

69. Роль стандартов и требований по информационной безопасности предприятия в формировании «Политики информационной безопасности организации».

70. Принципы распределения полномочий.

71. Процедуры и методы информационной безопасности организации как составляющие «Политики информационной безопасности организации».

72. Профили защиты.

73. Обязанности сотрудников по обеспечению информационной безопасности.

74. Порядок установления режима конфиденциальности информации. Перечень сведений, относимых к конфиденциальной информации и не подлежащих засекречиванию.

75. Требования, предъявляемые к претендентам на работу с конфиденциальной информацией и к претендентам на должность службу информационной безопасности.

76. Порядок обеспечения сохранности конфиденциальной информации при постоянном или временном прекращении пользователем доступа к конфиденциальному информационному ресурсу.

77. Организационные меры по обеспечению и поддержанию информационной безопасности в период чрезвычайных ситуаций.

78. Виды информации организации, подлежащие защите.

79. Регламентация действий всех категорий сотрудников, допущенных к работе с информационными системами.

80. Система организационно-распорядительных документов учреждения по вопросам обеспечения информационной безопасности.

81. Политика безопасности учреждения.

82. Программа безопасности учреждения.

Эссе «Методы защиты информации предметной области»

Опишите методы защиты информации, которые необходимо применить на вашей предметной области из лабораторной работы 3

Приложение 2

Оценочные средства для проведения промежуточной аттестации
а) Планируемые результаты обучения и оценочные средства для проведения промежуточной аттестации:

Код индикатора	Индикатор достижения компетенции	Оценочные средства
***УК-8* – Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов**		
УК-8.1	Анализирует и идентифицирует факторы опасного и вредного влияния элементов среды обитания (технических средств, технологических процессов, материалов, зданий и сооружений, природных и социальных явлений)	**Примерные варианты тестовых заданий.** 1. Что такое безопасность данных? a. это состояние хранимых, обрабатываемых и передаваемых данных, при котором невозможно их случайное или преднамеренное получение, изменение или уничтожение b. это состояние хранимых, обрабатываемых и передаваемых данных, при котором невозможно их случайное искажение c. это состояние хранимых, обрабатываемых и передаваемых данных, при котором невозможно их преднамеренное получение, изменение или уничтожение d. состояние защищенности национальных интересов РФ во всех сферах человеческой деятельности 2. Что является целью защиты информации? a. защита информации от утечки b. желаемый результат защиты информации c. защита информации от утраты d. предотвращение утраты и утечки конфиденциальной информации 3. Укажите некорректное определение нарушителя ИБ: a. физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности информации при ее обработке техническими средствами b. физическое или юридическое лицо, случайно совершающее действия, следствием которых является нарушение безопасности информации при ее обработке техническими средствами c. это лицо, предпринявшее попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, с целью самоутверждения и т.п.) и использующее для этого различные возможности, методы и средства 4. Что такое защищаемая информация?

Код индикатора	Индикатор достижения компетенции	Оценочные средства
		a. любая информация, которая появляется в СМИ b. информация, которая подлежит защите в соответствии с требованиями правовых документов и обязательно относится к государственной тайне c. информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации **Перечень вопросов для подготовки к экзамену** 1. Понятие информационной безопасности. 2. Основные составляющие информационной безопасности 3. Важность и сложность проблемы информационной безопасности 4. Законодательный уровень информационной безопасности 5. Обзор российского законодательства в области информационной безопасности 6. Правовые акты общего назначения, затрагивающие вопросы информационной безопасности 7. Понятие информационной безопасности. 8. Основные составляющие информационной безопасности 9. Основные определения и критерии классификации угроз 10. Наиболее распространенные угрозы доступности
		Практическое задание Разработать модель угроз и нарушителя предметной области
УК-8.2	Выявляет проблемы, связанные с нарушениями техники безопасности на рабочем месте; предлагает мероприятиях по предотвращению чрезвычайных ситуаций	**Примерные варианты тестовых заданий.** 1. Что такое безопасность данных? e. это состояние хранимых, обрабатываемых и передаваемых данных, при котором невозможно их случайное или преднамеренное получение, изменение или уничтожение f. это состояние хранимых, обрабатываемых и передаваемых данных, при котором невозможно их случайное искажение g. это состояние хранимых, обрабатываемых и передаваемых данных, при котором невозможно их преднамеренное получение, изменение или уничтожение h. состояние защищенности национальных интересов РФ во всех сферах человеческой

Код индикатора	Индикатор достижения компетенции	Оценочные средства
		деятельности 2. Укажите некорректное определение нарушителя ИБ: a. физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности информации при ее обработке техническими средствами b. физическое или юридическое лицо, случайно совершающее действия, следствием которых является нарушение безопасности информации при ее обработке техническими средствами c. это лицо, предпринявшее попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, с целью самоутверждения и т.п.) и использующее для этого различные возможности, методы и средства 4. Что такое защищаемая информация? a. любая информация, которая появляется в СМИ b. информация, которая подлежит защите в соответствии с требованиями правовых документов и обязательно относится к государственной тайне c. информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации **Перечень вопросов для подготовки к экзамену** 11. Понятие и сущность защиты информации. 12. Объекты защиты информации. 13. Средства защиты информации. 14. Методы защиты информации. 15. Основные понятия административного уровня информационной безопасности 16. Политика безопасности 17. Программа безопасности 18. Идентификация и аутентификация 19. Управление доступом 20. Ролевое управление доступом 21. Протоколирование и аудит 22. Шифрование 23. Экранирование 24. Классификация межсетевых экранов 25. Анализ защищенности

Код индикатора	Индикатор достижения компетенции	Оценочные средства
		26. Доступность 27. Отказоустойчивость и зона риска 28. Криптография 29. Вредоносные программы и способы защиты от них 30. Подразделения технической защиты информации. 31. Место и роль аппаратно-программных средств защиты. 32. Требования руководящих документов к средствам защиты информации от несанкционированного доступа. 33. Обнаружение сетевой атаки. 34. Способы обеспечения безопасной работы в Интернет. 35. Принципы функционирования брандмауэров. 36. Перечень информационных ресурсов, подлежащих защите. 37. Основы безопасности web-ресурсов. 38. Способы защиты файлов от постороннего доступа. 39. Эргономические и нормативные требования к организации рабочего места пользователя 40. Вредоносное программное обеспечение. 41. Пути проникновения вредоносного программного обеспечения. 42. Способы защиты от вредоносного программного обеспечения
		Практическое задание Провести аудит защищенности сети Восстановить удаленную информацию Удалить информацию с заданными параметрами Защитить информацию: пароль, криптография, стеганография Рассылка сообщений с сохранением конфиденциальности адресата Разработать модель нарушителя для заданной организации
		Комплексное задание Обеспечить защиту информации документов различного типа (доступность, целостность, конфиденциальность) от выявленных угроз предметной области
УК-8.3	Разъясняет правила поведения при возникновении чрезвычайных ситуаций природного и техногенного	**Примерные варианты тестовых заданий.** . Что является целью защиты информации? e. защита информации от утечки a. желаемый результат защиты информации b. защита информации от утраты c. предотвращение утраты и утечки конфиденциальной информации

Код индикатора	Индикатор достижения компетенции	Оценочные средства
	происхождения; оказывает первую помощь, описывает способы участия в восстановительных мероприятиях	**Перечень вопросов для подготовки к экзамену** 43. Вредоносное программное обеспечение 44. Основные угрозы целостности 45. Основные угрозы конфиденциальности 46. Управление рисками 47. Основные классы мер процедурного уровня 48. Управление персоналом 49. Физическая защита 50. Поддержание работоспособности 51. Реагирование на нарушения режима безопасности 52. Основные понятия программно-технического уровня информационной безопасности 53. Особенности современных информационных систем, существенные с точки зрения безопасности
		Практическое задание Сформировать пароль с заданными критериями устойчивости Рассчитать устойчивость пароля Применять специализированное программное обеспечение для сохранения статуса информации: хранение паролей, удаление информации, сокрытие информации
		Комплексное задание Найти нарушения нормативных правовых документов в предложенных заданиях: - репост записи, содержащей одобрение нарушение законодательства РФ; - скачивание «взломанных» программ; - рассылка спама; - покупка мини-видеокамеры; - установка программ прослушки на телефон супругу, ребенку; - использование доступа в чужую социальную сеть (подсмотрел пароль, не разлогинился пользователь и др.) - просмотр чужой почты. Подобрать требования существующего законодательства к ситуациям: - работодатель требует проходить детектор лжи сотрудников после инцидентов на предприятии; - работодатель требует сообщить сведения о доходах всех членов семьи работника; - пользователь вошел под учетной записью другого работника для выполнения профессиональных задач; - пользователь заразил рабочую станцию вредоносной программой, используя свой флеш-носитель (вариант 1 – умышленно, вариант 2

Код индикатора	Индикатор достижения компетенции	Оценочные средства
		– неумышленно)

б) Порядок проведения промежуточной аттестации, показатели и критерии оценивания:

Промежуточная аттестация по дисциплине «Методы и средства защиты информации» включает теоретические вопросы, позволяющие оценить уровень усвоения обучающимися знаний, и практические задания, выявляющие степень сформированности умений и владений, проводится в форме экзамена.

Экзамен по данной дисциплине проводится в устной форме по экзаменационным билетам, каждый из которых включает два теоретических вопроса и одно практическое задание.

Показатели и критерии оценивания экзамена:

«Отлично» – оценка знаний бакалавра, который свободно владеет:

1) понятийно-терминологической базой дисциплины и знает значение наиболее часто используемых аббревиатур;

2) четко увязывает теоретическое познание дисциплины с реальной практикой;

3) знаком с широким кругом литературных источников, знает, где их достать, хорошо разбирается в истории становления дисциплины, в оценке ее текущего состояния и перспектив ее развития;

4) полностью владеет материалом практического задания, четко и аргументировано защищает его положительные результаты, обосновано комментирует и объясняет допущенные недочеты.

«Хорошо» – оценка знаний бакалавра, который владеет понятийно-терминологической базой дисциплины, может увязать теоретическое познание дисциплины с реальной практикой. Владеет материалом практического задания, показал способность к объяснению смысла основных положений;

«Удовлетворительно» – оценка знаний бакалавра, который в большей части владеет, с небольшими изъянами, понятийно-терминологической базой дисциплины, имеет представление о внутренней логике дисциплины, представленной в виде учебной программы, Владеет, но неуверенно, материалом практического задания.

«Неудовлетворительно» – оценка знаний бакалавра, который не владеет понятийно-терминологической базой дисциплины и материалом практического задания.