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)

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Направление подготовки (специальность)
09.03.03 Прикладная информатика

Направленность (профиль/специализация) программы
Искусственный интеллект в цифровой экономике

Уровень высшего образования - бакалавриат

Форма обучения
очная

Институт/ факультет	Институт энергетики и автоматизированных систем
Кафедра	Бизнес-информатики и информационных технологий
Курс	3
Семестр	6

Магнитогорск
2022 год

Рабочая программа составлена на основе ФГОС ВО - бакалавриат по направлению подготовки 09.03.03 Прикладная информатика (приказ Минобрнауки России от 19.09.2017 г. № 922)

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

1 Цели освоения дисциплины (модуля)

Цель освоения дисциплины «Информационная безопасность» - сформировать у бакалавров компетенции в области методов и средств обеспечения информационной безопасности в организациях и на предприятиях различных сфер деятельности и форм собственности, основываясь на нормативно-правовых документах, международных и отечественных стандартах в области информационных систем и технологий, на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

2 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Информационная безопасность входит в обязательную часть учебного плана образовательной программы.

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

Безопасность жизнедеятельности

Информатика

Информационные системы и технологии

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

Производственная - технологическая (проектно-технологическая) практика

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) «Информационная безопасность» 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
ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;	
ОПК-3.1	Использует принципы, методы и средства информационной и библиографической культуры для решения стандартных задач профессиональной деятельности с использование информационно-коммуникационных технологий

ОПК-3.2	Решает стандартные задачи профессиональной деятельности с учетом основных требований информационной безопасности

4. Структура, объём и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет 3 зачетных единиц 108 акад. часов, в том числе:

– контактная работа – 51,95 акад. часов:

– аудиторная – 51 акад. часов;

– внеаудиторная – 0,95 акад. часов;

– самостоятельная работа – 56,05 акад. часов;

– в форме практической подготовки – 0 акад. час;

Форма аттестации - зачет с оценкой

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 информационной безопасности и защиты информации								
1.1 Сущность и понятие информационной безопасности	6	2	2		4	Конспектирование учебных материалов Самостоятельное изучение учебной и научной литературы Подготовка к лабораторному занятию	Тестирование ЛР 1 «Надежность и достоверность информации»	ОПК-3.1, ОПК-3.2
1.2 Угрозы информационной безопасности Угрозы информационной безопасности и защиты информации. Дестабилизирующее воздействие на защищаемую информацию. Классификация видов угроз информационной безопасности по различным признакам. Несанкционированный доступ к информации		2	2		4	Конспектирование учебных материалов Самостоятельное изучение учебной и научной литературы Подготовка к лабораторному занятию	Тестирование ЛР 2 «Классификация угроз предметной области»	УК-8.1, УК-8.2, ОПК-3.1, ОПК-3.2

1.3 Правовые основы обеспечения безопасности информационных технологий 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 информационной безопасности		2	4		6	Конспектирование учебных материалов Самостоятельное изучение учебной и научной литературы Подготовка к семинарскому занятию по ЛР 3 и 4: проработка научно-методической литературы, доклад и презентация	Тестирование Выступление на семинаре по ЛР 3 «Законодательная и нормативно-правовая база обеспечения информационной безопасности» Выступление на семинаре по ЛР 4 «Стандарты и спецификации в области информационной безопасности»	ОПК-3.1, ОПК-3.2
Итого по разделу		6	8		14			
2. Административный и процедурный уровни информационной безопасности								
2.1 Административный уровень обеспечения ИБ Политика безопасности. Программа безопасности. Оценка рисков и базовый уровень защиты	6	2	2		4	Конспектирование учебных материалов Самостоятельное изучение учебной и научной литературы Подготовка к семинарскому занятию по ЛР 5: проработка научно-методической литературы, доклад и презентация	Тестирование Выступление на семинаре по ЛР 5 «Политика информационной безопасности»	УК-8.3, ОПК-3.1, ОПК-3.2
2.2 Классы мер процедурного уровня Управление персоналом. Физическая защита. Поддержание работоспособности. Реагирование на нарушения режима безопасности. Планирование восстановительных работ		2	6/2И		8	Конспектирование учебных материалов Самостоятельное изучение учебной и научной литературы Подготовка к лабораторному занятию	Тестирование 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, ОПК-3.1, ОПК-3.2
Итого по разделу		4	8/2И		12			
3. Программно-технические меры обеспечения защиты информации								
3.1 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	6	2	8		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»	УК-8.1, УК-8.2, ОПК-3.1, ОПК-3.2

3.2 Вирусы и антивирусные средства Определение компьютерных вирусов. Классификация компьютерных вирусов. Признаки заражения. Профилактика заражения. Программные антивирусные средства. Структура антивирусной программы. Принципы выбора сигнатуры компьютерного вируса			2/4И		8	Самостоятельное изучение учебной и научной литературы Подготовка к семинарскому занятию по ЛР 13: проработка научно-методической литературы, доклад и	Тестирование Выступление на семинаре по ЛР 13 «Современные вредоносные программы для ПК и мобильных устройств»	УК-8.2, ОПК-3.1, ОПК-3.2
3.3 Криптографические методы защиты Методы криптографии. Средства криптографической защиты информации. Криптографические преобразования. Шифрование и дешифрование информации. Цифровая подпись.		2	4		8	Конспектирование учебных материалов Самостоятельное изучение учебной и научной литературы Подготовка к лабораторному занятию	Тестирование ЛР 14 «Защита информации с помощью криптографии» ЛР 15 «Защита информации с помощью стеганографии»	УК-8.2, ОПК-3.1, ОПК-3.2
3.4 Технические средства защиты информации Инженерная защита объектов, защита информации от утечки по техническим каналам. Стандарт CVSS «Общая система оценки уязвимостей»		1	2/4И		6	Конспектирование учебных материалов Самостоятельное изучение учебной и научной литературы Подготовка к лабораторному занятию	Тестирование ЛР 16 «CVSS «Общая система оценки уязвимостей»»	УК-8.2, УК-8.3, ОПК-3.1, ОПК-3.2
3.5 Информационно-психологическая безопасность Понятие информационно-психологической безопасности. Источники информационно-психологического воздействия на человека. Виды информационно-психологических воздействий. НЛП. Секты. Пирамиды. Рассылки. Защита личности от информационно-психологиче		2	2		4,05	Конспектирование учебных материалов Самостоятельное изучение учебной и научной литературы Подготовка к лабораторному занятию	Тестирование ЛР 17 «Информационно-психологические манипуляции»	УК-8.2, УК-8.3, ОПК-3.1, ОПК-3.2
Итого по разделу		7	18/8И		30,0			
Итого за семестр		17	34/10И		56,05		зао	
Итого по дисциплине		17	34/10И		56,05		зачет с оценкой	

5 Образовательные технологии

При проведении занятий и организации самостоятельной работы бакалавров используются:

Традиционные технологии обучения, предполагающие передачу информации в готовом 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, содержания, 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. Практикум по информационной безопасности для бакалавров Прикладной информатики / Е.В. Чернова. – Электрон. текстовые дан. (1,29 Мб). – Магнитогорск : ФГБОУ ВО «МГТУ им. Г.И. Носова», 2019. – 1 электрон. опт. диск (CD-R). – Систем. требования : IBMPC, любой, более lGHz ; 512 Мб RAM ; 10 Мб HDD ; M S WindowsXP и выше ; AdobeReader 8.0 и выше ; CD/ DVD-ROM дисковод ; мышь. – Загл. с титул. экрана

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.

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
Браузер Mozilla Firefox	свободно распространяемое ПО	бессрочно
FAR Manager	свободно распространяемое ПО	бессрочно
Браузер Yandex	свободно распространяемое ПО	бессрочно

Профессиональные базы данных и информационные справочные системы

Название курса	Ссылка

Национальная информационно-аналитическая система – Российский индекс	URL: https://elibrary.ru/project_risc.asp
Российская Государственная библиотека. Каталоги	https://www.rsl.ru/ru/4readers/catalogues/
Электронные ресурсы библиотеки МГТУ им. Г.И. Носова	https://magtu.informsystema.ru/Marc.html?locale=ru
Университетская информационная система РОССИЯ	https://uisrussia.msu.ru
Информационная система - Банк данных угроз безопасности	https://bdu.fstec.ru/
Информационная система - Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и	https://fstec.ru/normotvorcheskaya/tekhnicheskaya-zashchita-informatsii

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 Интернет 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

Учебно-методическое обеспечение самостоятельной работы обучающихся

По дисциплине «Информационная безопасность» 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, Баннтемана 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.

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. Требования «Общих критериев» группируются в: a.Классы b. Подклассы c. Группы d. Подгруппы **Перечень вопросов для подготовки к зачету с оценкой** 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. Обзор зарубежного законодательства в области информационной безопасности 8. Оценочные стандарты и технические спецификации.
		Практическое задание Провести аудит защищенности сети Настроить различные способы авторизации на веб-ресурсе с учетом поставленных задач
		Комплексное задание Обеспечить защиту информации документов различного типа (доступность, целостность, конфиденциальность) от выявленных угроз предметной области
УК-8.2	Выявляет проблемы, связанные с нарушениями техники безопасности на рабочем	**Примерные варианты тестовых заданий.** 1. Укажите некорректное определение нарушителя ИБ: a. физическое лицо, случайно или преднамеренно совершающее действия, следствием которых

Код индикатора	Индикатор достижения компетенции	Оценочные средства
	месте; предлагает мероприятиях по предотвращению чрезвычайных ситуаций	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 **Перечень вопросов для подготовки к зачету с оценкой** 9. Основные определения и критерии классификации угроз 10. Наиболее распространенные угрозы доступности 11. Вредоносное программное обеспечение 12. Основные угрозы целостности 13. Основные угрозы конфиденциальности 14. Идентификация и аутентификация 15. Управление доступом 16. Ролевое управление доступом 17. Протоколирование и аудит 18. Шифрование 19. Экранирование 20. Классификация межсетевых экранов 21. Анализ защищенности 22. Доступность 23. Отказоустойчивость и зона риска 24. Криптография 25. Вредоносное программное обеспечение. 26. Пути проникновения вредоносного программного обеспечения. 27. Способы защиты от вредоносного программного обеспечения
		Практическое задание Разработать модель угроз безопасности и нарушителя для предметной области
		Комплексное задание Разработать программу безопасности для предметной области
УК-8.3	Разъясняет правила поведения при возникновении	**Примерные варианты тестовых заданий.** 2. Что является целью защиты информации? a. защита информации от утечки

Код индикатора	Индикатор достижения компетенции	Оценочные средства
	чрезвычайных ситуаций природного и техногенного происхождения; оказывает первую помощь, описывает способы участия в восстановительных мероприятиях	b. желаемый результат защиты информации c. защита информации от утраты d. предотвращение утраты и утечки конфиденциальной информации **Перечень вопросов для подготовки к зачету с оценкой** 28. Основные понятия административного уровня информационной безопасности 29. Политика безопасности 30. Программа безопасности 31. Синхронизация программы безопасности с жизненным циклом систем
		Практическое задание Восстановить удаленную информацию Удалить информацию с заданными параметрами Противостоять распространенным способам информационного манипулирования
		Комплексное задание Применять специализированное программное обеспечение для сохранения конфиденциальности информации: хранение паролей, удаление информации, сокрытие информации
ОПК-3 – способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;		
ОПК-3.1: Использует принципы, методы и средства информационной и библиографической культуры для решения стандартных задач профессиональной деятельности с использование информационно-коммуникационных технологий		
Знать	не проверяется	
Уметь	не проверяется	
Владеть	не проверяется	
ОПК-3.2	Решает стандартные задачи профессиональной деятельности с учетом основных требований информационной безопасности	**Примерные варианты тестовых заданий.** 1. 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,

Код индикатора	Индикатор достижения компетенции	Оценочные средства
		устанавливаемыми собственником информации 2. 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 **Перечень вопросов для подготовки к зачету с оценкой** 32. Понятие информационной безопасности. 33. Основные составляющие информационной безопасности 34. Важность и сложность проблемы информационной безопасности 35. Подразделения технической защиты информации. 36. Место и роль аппаратно-программных средств защиты. 37. Требования руководящих документов к средствам защиты информации от несанкционированного доступа. 38. Обнаружение сетевой атаки. 39. Способы обеспечения безопасной работы в Интернет. 40. Принципы функционирования брандмауэров. 41. Перечень информационных ресурсов, подлежащих защите. 42. Основы безопасности web-ресурсов. 43. Способы защиты файлов от постороннего доступа. 44. Эргономические и нормативные требования к организации рабочего места пользователя
		Практическое задание Сформировать пароль с заданными критериями устойчивости Рассчитать устойчивость пароля Защитить информацию: пароль, криптография, стеганография Рассылка сообщений с сохранением конфиденциальности адресата
		Комплексное задание Найти нарушения нормативных правовых

Код индикатора	Индикатор достижения компетенции	Оценочные средства
		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 – неумышленно)

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

Промежуточная аттестация по дисциплине «**Информационная безопасность**» включает теоретические вопросы, позволяющие оценить уровень усвоения обучающимися знаний, и практические задания, выявляющие степень сформированности умений и владений, проводится в форме зачета с оценкой.

Зачет по данной дисциплине проводится в устной форме по зачетным билетам, каждый из которых включает один теоретический вопрос и одно практическое задание.

Показатели и критерии оценивания зачета с оценкой:

«Отлично» – оценка знаний студента, 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 ее положительные результаты, обосновано комментирует и объясняет допущенные недочеты.

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

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