Федеральное государственное бюджетное образовательное учреждение высшего образования
«ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ ДВАЖДЫ ГЕРОЯ СОВЕТСКОГО СОЮЗА, ЛЕТЧИКА-КОСМОНАВТА А.А. ЛЕОНОВА»

Троицкий Александр Витальевич
Подписано цифровой подписью: Троицкий Александр Витальевич

«УТВЕРЖДАЮ»
И.о. проректора
_____ А.В. Троицкий
«___»_____2023 г.

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАБОЧАЯ ПРОГРАММА
ДИСЦИПЛИНЫ (МОДУЛЯ)

Б.1.В.ДВ.05.01 «РАЗРАБОТКА ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНИЗАЦИЯХ»

Направление подготовки: 10.03.01 Информационная безопасность

Профиль: Организация и технологии защиты информации

Уровень высшего образования: бакалавриат

Форма обучения: очная, очно-заочная

Королев
2023

Рабочая программа является составной частью основной профессиональной образовательной программы и проходит рецензирование со стороны работодателей в составе основной профессиональной образовательной программы. Рабочая программа актуализируется и корректируется ежегодно.

Автор: Вихров А.П. Рабочая программа дисциплины: «Разработка политики информационной безопасности в организациях». – Королев МО: «Технологический университет», 2023.

Рецензент: **Соляной В.Н.**

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки бакалавров 10.03.01 «Информационная безопасность» и Учебного плана, утвержденного Ученым советом Университета. Протокол № 9 от 11.04.2023 года.

Рабочая программа рассмотрена и одобрена на заседании кафедры:

Заведующий кафедрой (ФИО, ученая степень, звание, подпись)	к.в.н., доцент Соляной В.Н.			
Год утверждения (переутверждения)	2023	2024	2025	2026
Номер и дата протокола заседания кафедры	№8 от 29.03.2023			

Рабочая программа согласована:

Руководитель ОПОП ВО Сухотерин А.И.

Рабочая программа рекомендована на заседании УМС:

Год утверждения (переутверждения)	2023	2024	2025	2026
Номер и дата протокола заседания УМС	№5 от 11.04.2023			

2

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОПОП ВО

Целями изучения дисциплины является:

1. Ускоренная адаптация студентов в предметную область информационная безопасность (выработка политики информационной безопасности), опираясь на весь спектр научных воззрений, на развитие и правовую защиту информационно - телекоммуникационной инфраструктуры и компьютерной информации;
2. Повысить уровень правовых знаний, которые необходимы обучающимся для высоко профессиональной деятельности во всех сферах информационной безопасности с учетом требований высшей школы, для активизации их учебной и исследовательской деятельности;
3. Изучение правовых основ информационной безопасности и информирование студентов о законодательных источниках, подзаконных и ведомственных правовых актах обеспечивающих информационную безопасность личности, общества и государства;
4. Формирование у студентов специализированной базы знаний по основным понятиям в области правовой защиты информации и разработки политики информационной безопасности;
5. Приобретение студентами первичных навыков по практическому формированию комплекса документов, составляющих правовую базу защиты информации и разработки политики информационной безопасности на предприятиях и в организациях.

В процессе обучения студент приобретает и совершенствует следующие компетенции:

Профессиональные компетенции:

ПК-3. Способность осуществлять управление с разработкой организационно-распорядительных документов и реализацию организационных мер по ЗИ в АС

ПК-4. Способен осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций;

Основными **задачами** дисциплины являются:

1. Теоретические основы разработки политики информационной безопасности на основе действующего российского законодательства с помощью современных принципов, методов, сил и средств в различных организационных структурах;
2. Практические аспекты разработки политики информационной безопасности по базовым направлениям защиты государственной, профессиональной, коммерческой тайны и конфиденциальной информации и формированием у обучающихся системы знаний.

Показатель освоения компетенции отражают следующие индикаторы:

Необходимые знания:

- основные нормативно-правовые акты, методы управления деятельностью, угрозы ИБ и нарушители систем безопасности информации;
- знать нормативно-методические, руководящие и методические документы, организационные меры, критерии оценки защищенности и регламенты обеспечения работоспособности систем ЗИ;

Необходимые умения:

- оценивать информационные риски разрабатывать предложения по совершенствованию СУ (ИБ) и применять средства контроля эффективности ЗИ;
- определять и оценивать источники, причины и последствия возникающих инцидентов выявлять и устранять нарушения в области ИБ (ЗИ);

Трудовые действия:

- анализировать воздействие на защищаемую систему информации, оценивать последствия и вырабатывать предложения по ее совершенствованию;
- принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации;

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Разработка политики информационной безопасности в организациях» относится к дисциплинам по выбору вариативной части основной профессиональной образовательной программы подготовки бакалавров по направлению 10.03.01 «Информационная безопасность».

Изучение данной дисциплины базируется на ранее изученных дисциплинах: «Основы информационной безопасности», «Информатика», «Основы права», «Основы управленческой деятельности» и компетенциях: ОПК-1,6,7,8,9,13; УК-5,6,9.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Организация защиты персональных данных на предприятии», «Правовая охрана результатов интеллектуальной деятельности», «Организация системы обеспечения информационной безопасности (служба ИБ)», «Лицензирование и сертификация в области защиты информации», «Аттестация в области защиты информации», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

3. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины для студентов очной и очно-заочной формы составляет 2 зачетных единиц 72 часов.

Таблица1

Виды занятий	Всего часов	Семестр 6	Семестр 8	Семестр …	Семестр …
Общая трудоемкость	72	72	72		
ОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	32	32			
Лекции (Л)	16	16			
Практические занятия (ПЗ)	16	16			
Лабораторные работы (ЛР)	-	-			
Самостоятельная работа	30	30			
Другие виды контактной работы	6	6			
Практическая подготовка	12	12			
Курсовые работы (проекты)	-	-			
Расчетно-графические работы	-	-			
Контрольная работа, домашнее задание	+ -	+ -			
Текущий контроль знаний (7 - 8, 15 - 16 недели)- 2ч.	Т1; Т2	Т1; Т2			
Вид итогового контроля	Зачет	Зачет			
ОЧНО-ЗАОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	20		20		
Лекции (Л)	8		8		
Практические занятия (ПЗ)	12		12		
Лабораторные работы (ЛР)	-		-		
Другие виды контактной работы	6		6		
Практическая подготовка	нет		нет		
Самостоятельная работа	52		52		
Курсовые работы (проекты)	-		-		
Расчетно-графические работы	-		-		
Контрольная работа, домашнее задание	+ -		+ -		
Вид итогового контроля	Зачет		Зачет		

Под другими видами контактной работы понимается: групповые и индивидуальные консультации, тестирование

4. Содержание дисциплины

4.1. Темы дисциплины и виды занятий

Таблица 2

Наименование тем	Лекции, час. очное	Практические занятия, час. очное	Занятия в интерактивной форме, час. очное	Практическая подготовка, час	Код компетенций
1	2	3	4		5
Раздел 1. Актуальность политик информационной безопасности.					
Тема 1. Введение. Современные проблемы информационной безопасности	1/0.5	1/0.5	0.5/0.5	1/нет	ПК-3
Тема 2. Служба информационной безопасности организаций. Модель информационных потоков. Типовая модель нападения.	1/0.5	1/0.5	0.5/0.5	1/нет	ПК-3
Тема 3. Адекватность механизмов защиты. Управление и методики оценки рисков.	1/0.5	1/0.5	1/0.5	1/нет	ПК-3
Тема 4. Криптография и её основные принципы. Общетехнические средства защиты. Протоколы сетевой безопасности. Разработка приложений.	1/0.5	1/0.5	1/0.5	1/нет	ПК-3
Тема 5. Концепция создания политики информационной безопасности организации	1/0.5	1/0.5	1/0.5	1/нет	ПК-3
Тема 6. Работа с пользователями, администраторами и разработчиками. Тестирование процедур и	1/0.5	1/0.5	1/0.5	1/нет	ПК-3

механизмов безопасности.					
Тема 7. Действия в условиях нарушения безопасности.	1/0.5	1/0.5	1/1	1/0.5	ПК-,4
Раздел 2. Административный уровень обеспечения разработки политики информационной безопасности					
Тема 8. Административный уровень обеспечения разработки политики информационной безопасности	1/0.5	1/0.5	1/2	1/нет	
Тема 9. Основные причины и принципы создания ПИБ.	1/0.5	1/0.5	1/0.5	1/нет	ПК-4
Тема 10. Стандарты и спецификации в области информационной безопасности и разработки политики информационной безопасности	1/0.5	1/0.5	1/0.5	1/нет	ПК-4
Тема 11. Процесс разработки политики информационной безопасности.	2/1	2/1	1/0.5	1/нет	ПК-4
Тема 12. Российская специфика разработки политики информационной безопасности	2/1	2/1	1/0.5	0.5/нет	ПК-4
Тема 13. Лучшие практики создания и реализации политик информационной безопасности зарубежных компаний	2/1	2/1	1/2	0.5/нет	ПК-4
	16/8	16/12	12/10	**12/нет**	

4.2. Содержание тем дисциплины

Раздел 1.

Тема 1. Введение. Современные проблемы информационной безопасности

Предмет и задачи курса. Значение и место курса в подготовке магистров по информационной безопасности. Взаимосвязь курса с другими дисциплинами.

Разделы и темы, их распределение по видам аудиторных занятий. Формы проведения контрольных мероприятий. Формы проверки знаний. Состав и методика самостоятельной работы студентов по изучению дисциплины.

Знания и умения студентов, которые должны быть получены в результате изучения курса. Рекомендованная научная и учебная литература.

Характеристика существующих проблем по информационной безопасности в ходе становления современного информационного общества.

Анализ исторического развития подходов к обеспечению информационной безопасности в мире и в Российской Федерации. Современная постановка задачи по обеспечению информационной безопасности. Переход к интенсивным мерам по обеспечению информационной безопасности.

Тема 2. Служба информационной безопасности организаций. Модель информационных потоков. Типовая модель нападения.

Общие понятия информационной безопасности. Определение и цели информационной безопасности. Механизмы информационной безопасности. Инструментарий информационной безопасности. Основное направления информационной безопасности. Задачи и принципы организации службы информационной безопасности. Создание службы информационной безопасности. Инвентаризация и классификация информационных систем. Модель информационных потоков. Типовая модель нападения. Локальные и удалённые атаки. Атаки на поток данных.

Тема 3. Адекватность механизмов защиты. Управление и методики оценки рисков.

Управление рисками. Методика оценки рисков. Модели качественной и количественной оценки рисков. Модель обобщённого стоимостного результата Миоры (GCC). Высоко вероятные атаки.

Тема 4. Криптография и её основные принципы. Общетехнические средства защиты. Протоколы сетевой безопасности. Разработка приложений.

Основные принципы криптографии. Симметричная криптография. Асимметричная криптография и цифровая подпись. Прочие криптографические алгоритмы. Сложные криптографические протоколы.

Тема 5. Концепция создания политики информационной безопасности организации

Структура документа. Примеры: выдержки из концепции предприятия. Стандарты. Процедуры. Методы. Аварийный план. Политики по отдельным направлениям.

Тема 6. Работа с пользователями, администраторами и разработчиками. Тестирование процедур и механизмов безопасности.

Рекомендации по взаимодействию с персоналом. Работа с пользователями. Работа с администраторами. Работа с разработчиками. Вопросы подчинения и взаимодействия служб. Создание заявки на выполнение работ. Право подписи заявки. Формы приложения к заявке 06. Тестирование процедур и механизмов безопасности.

Тема 7. Действия в условиях нарушения безопасности.

Право подписи заявки. Формы приложения к заявке 06. Тестирование процедур и механизмов безопасности. Аварийный план и принципы его создания. Структура аварийного плана. Методология работы с аварийным планом. Пример аварийного плана. Классификация технологий RAID. Реагирование на нарушение информационной безопасности. Проведение расследования.

Раздел 2. Административный уровень обеспечения разработки политики информационной безопасности

Тема 8. Административный уровень обеспечения разработки политики информационной безопасности

Политики информационной безопасности, рекомендуемые ведущими компаниями.

Политика безопасности, программа безопасности, анализ рисков, уровень детализации, карта информационной системы, классификация ресурсов, физическая защита, правила разграничения доступа, порядок разработки политики безопасности, непрерывная работа, оценка рисков, координация, стратегическое планирование, контроль, жизненный цикл, инициация, закупка, установка, эксплуатация, выведение из эксплуатации.

Тема 9. Основные причины и принципы создания ПИБ.

Анализ отечественного рынка средств защиты информации. Основные причины и принципы создания ПИБ. Кому и что доверять. Трудности внедрения ПИБ. Заинтересованность в политиках безопасности. Состав группы по разработке политик безопасности. Тенденции развития стандартов и политик информационной безопасности. Общая методология оценки безопасности информационных технологий. Основные понятия и идеи. Реализация политики информационной безопасности.

Тема 10. Стандарты и спецификации в области информационной безопасности и разработки политики информационной безопасности

Обзор наиболее важных стандартов и спецификаций в области информационной безопасности. Общие критерии оценки безопасности информационных технологий (Общие критерии). Основные понятия и идеи. Функциональные требования безопасности. Требования доверия безопасности. Профили защиты, разработанные на основе «Общих критериев».

Практическое применение международного стандарта безопасности информационных систем ISO 17799. Типовые документы, основанные на стандарте безопасности. Задание общих правил информационной безопасности.

Тема 11. Процесс разработки политики информационной безопасности.

Основные требования к политике информационной безопасности. Уровень средств безопасности. Процесс разработки политики информационной безопасности. Системы оценки текущей ситуации в области информационной безопасности на предприятии. Алгоритм метода: "исследование сверху вниз".

Тема 12. Российская специфика разработки политики информационной безопасности

Разработка и внедрение эффективных политик информационной безопасности. Факторы, определяющие эффективность политики безопасности. Оценка риска. Рекомендации по разработке и внедрению эффективных политик. Создание благоприятной среды. Жизненный цикл политики безопасности. Пример неудачной политики. Пример управленческой политики организации.

Тема 13. Лучшие практики создания и реализации политик информационной безопасности зарубежных компаний

Подходы зарубежных компаний к разработке политик информационной безопасности. Примеры политик информационной безопасности зарубежных компаний.

Практика компании IBM в области защиты информации. Структура документов безопасности Пример особенностей подхода к построению системы безопасности в компании IBM

Подход компании Sun Microsystems. Структура политики

безопасности. .Пример политики безопасности.

Подход компании Cisco Systems. Описание политики безопасности.

Практика компании Cisco Systems в разработке сетевой политики безопасности. Порядок разработки сетевой политики безопасности. Проведение анализа рисков информационной безопасности. Определение состава и структуры группы сетевой безопасности. Предупреждение нарушений политики безопасности компании.

Практика компании Microsoft в области информационной безопасности

Пример политики сетевой безопасности.

Подход компании Symantec. Описание политики безопасности.

Подход SANS. Описание политики безопасности. Пример политики

аудита безопасности.

5. Перечень учебно-методического обеспечения для самостоятельной работы по дисциплине

«Методические указания для самостоятельной работы обучающихся по освоению дисциплины» представлены в Приложении 2.

6. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

Структура фонда оценочных средств, для проведения промежуточной аттестации обучающихся по дисциплине «Выработка политики информационной безопасности», приведена в Приложении 1.

7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная литература:

1.Барлаков, С. А. Модели и методы в управлении и экономике с применением информационных технологий : учебное пособие / С. А. Барлаков, С. И. Моисеев, В. Л. Порядина. — Санкт-Петербург : Интермедия, 2016. — 264 с. — ISBN 978-5-4383-0135-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/103198 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

2.Гришаева, С. А. Информационная безопасность в системах менеджмента качества : учебное пособие / С. А. Гришаева. — Москва : МАИ, 2021. — 63 с. — ISBN 978-5-4316-0804-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/256274 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

3.Черемухина, Ю. Ю. Системы менеджмента качества : учебное пособие / Ю. Ю. Черемухина. — Москва : РТУ МИРЭА, 2019. — 95 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/171525 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

4.Киреева, Н. В. Аудит информационной безопасности : методические указания / Н. В. Киреева, И. С. Поздняк, О. А. Караулова. — Самара : ПГУТИ, 2019. — 21 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/223223 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

Дополнительная литература:

5.Поздняк, И. С. Экспертные системы оценки информационной безопасности : методические указания / И. С. Поздняк, Н. В. Киреева, О. А. Караулова. — Самара : ПГУТИ, 2019. — 23 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/223304 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

Интернет-ресурсы:

1. **http://eup.ru/catalog/all-all.asp** – научно-образовательный портал.
2. **www.wikIsec.ru** - Энциклопедия информационной безопасности. – Публикации, статьи.
3. **http://www.fsb.ru/** - Официальный сайт Федеральной Службы Безопасности
4. **http://www.fstec.ru/** - Официальный сайт Федеральной Службы по Техническому Экспортному Контролю
5. **http://www.AuditNet.ru** (все об аудите ИТ и ИБ).
6. **http://www.ISO27000.ru** (портал по ИБ, аналитика, информация по законодательству и стандартам, блоги, каталоги ресурсов и ПО).
7. **http://www.SecurityManagement.ru** (форум по ИБ).
8. **http://www.WinSecurity.ru** (статьи, документация, новости по безопасности Windows).

9. Методические указания для обучающихся, по освоению дисциплины

Методические указания для обучающихся, по освоению дисциплины приведены в Приложении 2 к настоящей рабочей программе.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

- **Перечень программного обеспечения:** MSOffice, PowerPoint.

- **Информационные справочные системы:**

1. Учебный портал с электронно-методическими комплексами (do.kimes).
2. Универсальная библиотека онлайн (www.biblioclub.ru).
3. Polpred.com www.polpred.com.
4. Единое окно доступа (www.window.edu.ru)/
5. Издательский дом «Гребенников» (http://grebennikon.ru/)..

Ресурсы информационно-образовательной среды МГОТУ:

Рабочая программа и методическое обеспечение по курсу «Разработка политики информационной безопасности в организациях»

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Лекционные занятия:

- аудитория, оснащенная презентационной техникой (проектор, экран);
- комплект электронных презентаций / слайдов на темы:

- **Практические занятия:**
- компьютерный класс с проектором для интерактивного обучения и проведения лекций в форме слайд-презентаций, оборудованный современными лицензионными программно-техническими средствами: операционная система не ниже WindowsXP; офисные программы MSOffice 7;
- рабочее место преподавателя, оснащенное компьютером с доступом в Интернет;
- рабочие места студентов, оснащенные компьютерами с доступом в Интернет.

Приложение 1

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю)

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

«РАЗРАБОТКА ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНИЗАЦИЯХ»

Направление подготовки: 10.03.01 «Информационная безопасность»

Профиль: Организация и технологии защиты информации

Уровень высшего образования: бакалавриат

Форма обучения: очная, очно-заочная

Королев
2023

1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

№ п/п	Индекс компе-тенции	Содержание компетенции	Раздел дисциплины, обеспечивающий формирование компетенции	В результате изучения раздела дисциплины, обеспечивающего формирование компетенции, обучающийся приобретает:		
				Трудовые действия	Необходимые умения	Необходимые знания
1.	ПК-3	Способность осуществлять управление с разработкой организационно-распорядительных документов и реализацию организационных мер по ЗИ в АС	Тема:1-6	- анализировать воздействие на защищаемую систему информации, оценивать последствия и вырабатывать предложения по ее совершенствованию	- оценивать информационные риски разрабатывать предложения по совершенствованию СУ (ИБ) и применять средства контроля эффективности ЗИ;	- основные нормативно-правовые акты, методы управления деятельностью, угрозы ИБ и нарушители систем безопасности информации;
2.	**ПК-4**	Способность осуществлять диагностику и оценку обеспечения работоспособности системы ЗИ при возникновении внештатных ситуаций	Тема 7-13	- принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации;	- определять и оценивать источники, причины и последствия возникающих инцидентов выявлять и устранять нарушения в области ИБ (ЗИ);	- знать нормативно-методические, руководящие и методические документы, организационные меры, критерии оценки защищенности и регламенты обеспечения работоспособности систем ЗИ;

2.Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Код компетенции	*Инструмент, оценивающий сформированность компетенции*	*Этапы и показатель оценивания компетенции*	*Критерии оценивания компетенции на различных этапах формирования и шкалы оценивания*
ПК-3,4	*Доклад*	*А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 5 баллов* *Б) частично сформирована:* • *компетенция освоена на <u>продвинутом</u> уровне – 4 балла;* • *компетенция освоена на <u>базовом</u> уровне – 3 балла;* *В) не сформирована (<u>компетенция не сформирована</u>) – 2 и менее баллов*	*Например:* *Проводится в письменной и/или устной форме.* *Критерии оценки:* *1. Соответствие содержания доклада заявленной тематике (1 балл).* *2. Качество источников и их количество при подготовке работы (1 балл).* *3. Владение информацией и способность отвечать на вопросы аудитории (1 балл).* *4. Качество самой представленной работы (1 балл).* *5. Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл).* *Максимальная сумма баллов - 5 баллов.*
ПК-3,4	*Выполнение контрольной работы*	*А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 5 баллов* *Б) частично сформирована:* • *компетенция освоена на <u>продвинутом</u> уровне – 4 балла;* • *компетенция освоена на <u>базовом</u> уровне – 3 балла;* *В) не сформирована (<u>компетенция не сформирована</u>) – 2 и менее баллов*	*При определении сформированности компетенций критериями оценивания выступают методические рекомендации, разработанные по дисциплине для данного вида*

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Примерная тематика докладов в презентационной форме:

1. Политика безопасности.
2. Избирательное управление доступом: модель Харрисона-Руззо-Ульмана.
3. Полномочное управление доступом: модели Белла-ЛаПадула, Биба.
4. Структура политики безопасности организации.
5. Управленческие меры политики безопасности организации.
6. Структура и назначение процедуры аудита безопасности.
7. Типовые модели нападения.
8. Локальные и удаленные атаки.
9. Атаки на поток данных.
10. Сложные криптографические протоколы.

Примерная тематика заданий на контрольную работу:

1. Методологические основы разработки политики информационной безопасности.
2. Теоретико-прикладные основы разработки политики информационной безопасности.
3. Основные принципы криптографии.
4. Задачи и принципы организации службы информационной безопасности.
5. Методология работы с аварийным планом.
6. Проведение расследований.
7. Реагирование на нарушение информационной безопасности.
8. Тестирование процедур и механизмов безопасности.
9. Карта информационной системы.
10. Общая методология оценки безопасности информационных технологий.
11. Реализация политики информационной безопасности.
12. Общие критерии оценки безопасности информационных технологий
13. Функциональные требования безопасности.
14. Требования доверия безопасности.
15. Профили защиты, разработанные на основе «Общих критериев».
16. Практическое применение международного стандарта безопасности информационных систем ISO 17799.
17. Основные требования к политике информационной безопасности.
18. Уровень средств безопасности.
19. Процесс разработки политики информационной безопасности.
20. Системы оценки текущей ситуации в области информационной безопасности на предприятии.

4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Формой контроля знаний по дисциплине «Разработка политики информационной безопасности в организациях» являются две текущие аттестации в виде тестов в каждом семестре, а также итоговая аттестация в виде зачета и зачета.

Неделя текущего контроля	Вид оценочного средства	Код компетенций, оценивающий знания, умения, навыки	Содержание оценочного средства	Требования к выполнению	Срок сдачи (неделя семестра)	Критерии оценки по содержанию и качеству с указанием баллов
Проводится в сроки, установленные графиком образовательного процесса	тестирование	ПК-3,4	20 вопросов	Компьютерное тестирование; время отведенное на процедуру - 30 минут	Результаты тестирования предоставляются в день проведения процедуры	***Преподаватель указывает критерии оценки данного вида контроля. Например, критерии оценки определяются процентным соотношением. Неявка – 0. Неудовлетворительно – менее 50% правильных ответов Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%.***
Проводится в сроки, установленные графиком образовательного процесса	тестирование	ПК-3,4	20 вопросов	Компьютерное тестирование; время отведенное на процедуру – 30 минут	Результаты тестирования предоставляются в день проведения процедуры	***Преподаватель указывает критерии оценки данного вида контроля. Например, критерии оценки определяются процентным соотношением. Неявка – 0. Неудовлетворительно – менее 50% правильных ответов Удовлетворительно - от 51%***

						правильных ответов. Хорошо - от 70%. Отлично – от 90%.
Проводится в сроки, установленные графиком образовательного процесса	Зачет	ПК-3,4	2 теоретических вопроса + практическое задание	Зачет проводится в письменной форме, путем ответа на вопросы. Время, отведенное на процедуру – 15 минут.	Результаты предоставляются в день проведения зачета	***Например, критерии оценки: «Зачтено»:*** • ***знание основных понятий предмета;*** • ***умение использовать и применять полученные знания на практике;*** • ***работа на семинарских занятиях;*** • ***знание основных научных теорий изучаемых предметов;*** • ***ответ на вопросы билета.*** ***«Не зачтено»:*** • ***демонстрирует частичные знания по темам дисциплин;*** • ***незнание основных понятий предмета;*** • ***неумение использовать и применять полученные знания на практике;*** • ***не работал на семинарских занятиях;*** ***не отвечает на вопросы.***

Примерное содержание тестов для текущей аттестации:

ЗАДАНИЕ НА ВЫБОР ОДНОГО ПРАВИЛЬНОГО ВАРИАНТА ОТВЕТА

1. Предмет, цель и задачи разработки политики информационной безопасности.
2. Система защиты TETRA.
3. Корпоративная компьютерная сеть.
4. Классы защищенности
5. Принципы работы с пользователями, администраторами и разработчиками.
6. Стандарты, используемые при разработке политики информационной безопасности предприятия и объектов региона.
7. Концепция политики безопасности.
8. Проблемы обеспечения нормативно-правового пространства.
9. Разработка приложений при проектировании политики безопасности предприятия.
10. Теоретико-прикладные основы страхования информационных рисков в объектах.
11. Классификация атак и построение политики информационной безопасности с учётов различных видов атак.
12. Адекватность механизмов защиты. Управление рисками. Методика оценки рисков.
13. Политика системного администрирования.
14. Протоколы TCP/IP.
15. Классы сетей.
16. Контроль физического доступа и протоколы сетевой безопасности.
17. Автоматизированные средства безопасности.
18. Проблема информационной войны в современных условиях.
19. Информационное оружие в современной системе обеспечения информационной безопасности.
20. Криптография и её место в политике информационной безопасности предприятия и объектов региона .
21. Проведение расследования и анализ его результатов.
22. Реагирование на нарушение безопасности.
23. Методологические основы организационного обеспечения информационной безопасности региона на уровне крупных поставщиков защищенных информационных систем.
24. Методологические основы развития государственно-регионального управления информационной безопасностью).
25. Тестирование процедур и механизмов безопасности при разработке политики безопасности.
26. Теоретико-прикладные основы развития менеджмента информационной безопасности на уровне региональных предприятий.

27. Методологические основы построения унифицированной Концепции (политики) информационной безопасности предприятия и объектов региона.
28. Основные требования к политике информационной безопасности.
29. Уровень средств безопасности.
30. Алгоритм метода: "исследование сверху вниз".

Типовые вопросы, выносимые на зачет

1. Предмет, цель и задачи политики информационной безопасности.
2. Проблема информационной войны в современных условиях.
3. Информационное оружие в современной системе обеспечения информационной безопасности
4. Развитие подходов к организации информационной безопасности в мире (исторический аспект).
5. Развитие и становление обеспечения информационной безопасности в Российской Федерации.
6. Современная постановка целей и задач по обеспечению информационной безопасности и разработка политики безопасности.
7. Определение, принципы и методологический базис формирования основ теории информационной безопасности.
8. Развитие неформальных теоретико-прикладных подходов анализа процессов по информационной безопасности в современных условиях.
9. Теоретические основы моделирования современных процессов информационной безопасности при разработки политики информационной безопасности.
10. Базовое содержание основ теории информационной безопасности.
11. Понятие и системная классификация современных информационных угроз.
12. Основные теоретико-прикладные показатели уязвимости защищаемого информационного ресурса.
13. Методологические основы достоверности прогнозирования уязвимости информационных объектов при разработке политики информационной безопасности.
14. Теоретико-прикладные модели оценки ущерба от реализации информационных угроз.
15. Постановка задачи и основы методологии определения требований к обеспечению информационной безопасности.
16. Основные параметры безопасности информации (информационного ресурса).
17. Основы методологии оценки основных факторов, влияющих на требуемый уровень обеспечения информационной безопасности.
18. Методологические основы определения весов и классификации возможных условий обеспечения информационной безопасности.

19. Системный подход как основа построения современных комплексов обеспечения информационной безопасности.
20. Определение, типизация и стандартизация современных систем обеспечения информационной безопасности.
21. Современные методологические основы проектирования комплексных систем обеспечения информационной безопасности.
22. Методологические основы совокупной оценки функционирования комплексных систем информационной безопасности.
23. Основные научные принципы и общая задача управления современными системами информационной безопасности.
24. Типовая модель и виды управления информационной безопасностью (краткосрочное; среднесрочное и долгосрочное).
25. Методологические основы выработки и оптимизации управленческих решений по информационной безопасности (характеристика основных этапов принятия и реализации решений).
26. Методологические основы организации и проведения контрольных мероприятий по информационной безопасности.
27. Основы организации обеспечения информационной безопасности предприятия и объектов региона.
28. Функции, задачи, структура и организация работы службы информационной безопасности предприятия и объектов, региональных центров информационной безопасности.
29. Анализ состояния и прогноз развития теории информационной безопасности.
30. Перспективы развития межведомственной системы подготовки и переподготовки кадров в области обеспечения информационной безопасности.

**Итоговое начисление баллов по дисциплине осуществляется в соответствии с разработанной и внедренной балльно-рейтинговой системой контроля и оценивания уровня знаний и внеучебной созидательной активности обучающихся.*

Приложение 2

Методические указания для обучающихся по освоению дисциплины (модуля)

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

«РАЗРАБОТКА ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНИЗАЦИЯХ»

Направление подготовки: 10.03.01 «Информационная безопасность»

Профиль: Организация и технологии защиты информации

Уровень высшего образования: бакалавриат

Форма обучения: очная, очно-заочная

Королев
2023

1. Общие положения

Целями изучения дисциплины является:

– формирование у студентов базовых знаний и практических навыков в области разработки политики информационной безопасности.

– Формирование у студентов специализированной базы знаний по основным понятиям в области выработки политики информационной безопасности.

Задачами дисциплины является:

1. Теоретические основы разработки политики информационной безопасности на основе действующего российского законодательства с помощью современных принципов, методов, сил и средств в различных организационных структурах;
2. Практические аспекты разработки политики информационной безопасности по базовым направлениям защиты государственной, профессиональной, коммерческой тайны и конфиденциальной информации и формированием у обучающихся системы знаний.

2. Указания по проведению практических занятий

Практическое занятие 1-4.

Вид практического занятия**:** ***подготовка доклада.***

Образовательные технологии: ***групповая дискуссия.***

Тема и содержание практического занятия:

Тема: Современные проблемы информационной безопасности

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Ознакомление студентов с современными проблемами информационной безопасности.

Основные положения темы занятия:

1. Исторический аспект развития и становление обеспечения информационной безопасности в мире.
2. Развитие и становление обеспечения информационной безопасности в России.

Вопросы для обсуждения:

1. Предмет и задачи курса.
2. Значение и место в подготовке студентов.
3. Характеристика существующих проблем по информационной безопасности.
4. Анализ исторического развития подходов к обеспечению информационной безопасности в мире.
5. Анализ исторического развития подходов к обеспечению информационной безопасности в Российской Федерации.

6. Современная постановка задачи по обеспечению информационной безопасности.

Продолжительность занятия: 4/4ч.

Практическое занятие 5-7.

Вид практического занятия**:** ***подготовка доклада.***

Образовательные технологии: ***групповая дискуссия.***

Тема и содержание практического занятия:

Тема: Служба информационной безопасности организаций.

.

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить теоритические основы, задачи и принципы организации службы информационной безопасности.

Основные положения темы занятия:

1. Механизмы информационной безопасности.
2. Создание службы информационной безопасности.

Вопросы для обсуждения:

1. Общие понятия информационной безопасности.
2. Определение и цели информационной безопасности.
3. Типовая модель нападения.
4. Инвентаризация и классификация информационных систем.
5. Модель информационных потоков.
6. Локальные и удалённые атаки.
7. Атаки на поток данных.

Продолжительность занятия: 3/3 ч.

Практическое занятие 8-11

Вид практического занятия**:** ***подготовка доклада.***

Образовательные технологии: ***групповая дискуссия.***

Тема и содержание практического занятия:

Тема: Адекватность механизмов защиты.

Вид практического занятия**:** *смешанная форма практического занятия.*

Тема и содержание практического занятия:

Цель работы: Получить практические навыки анализа и использования механизмов защиты.

Основные положения темы занятия:

1. Управление и методики оценки рисков.
2. Обоснование целесообразных механизмов защиты.

Вопросы для обсуждения:

1. Управление рисками.

2. Методика оценки рисков.
3. Модели качественной оценки рисков.
4. Модели количественной оценки рисков.
5. Модель обобщённого стоимостного результата Миоры (GCC).
6. Высоко вероятные атаки.

Продолжительность занятия: 3/3 ч.

Практическое занятие 12

Вид практического занятия**: *подготовка доклада.***
Образовательные технологии: ***групповая дискуссия.***
Тема и содержание практического занятия:

Тема: Основные причины и принципы создания ПИБ.

Вид практического занятия: *смешанная форма практического занятия.*
Тема и содержание практического занятия:
Цель работы: Получить практические навыки выбора и реализации выработки политики информационной безопасности.

Основные положения темы занятия:

1. Основные причины создания ПИБ.
2. Основные принципы создания ПИБ.

Вопросы для обсуждения:

1. Анализ отечественного рынка средств защиты информации.
2. Трудности внедрения ПИБ.
3. Заинтересованность в политиках безопасности.
4. Состав группы по разработке политик безопасности.
5. Тенденции развития стандартов и политик информационной безопасности.
6. Общая методология оценки безопасности информационных технологий.
7. Реализация политики информационной безопасности.

Продолжительность занятия: 6/2 ч.

3. Указания по проведению самостоятельной работы студентов

№ п/п	Наименование блока (раздела) дисциплины	Виды СРС
1.	**Тема 10. Стандарты и спецификации в области информационной безопасности и разработки политики информационной безопасности**	***Подготовка докладов по темам:*** 1. Подходы зарубежных компаний к разработке политик информационной безопасности. 2. Примеры политик информационной безопасности зарубежных компаний.

		3. Практика компании IBM в области защиты информации. 4. Структура документов безопасности 5. Структура политики безопасности.
2.	**Тема 11. Процесс разработки политики информационной безопасности.**	***Подготовка докладов по темам:*** 1. Пример политики безопасности. 2. Описание политики безопасности. 3. Порядок разработки сетевой политики безопасности. 4. Проведение анализа рисков информационной безопасности. 5. Определение состава и структуры группы сетевой безопасности. 6. Предупреждение нарушений политики безопасности компании.
3	**Тема 12. Российская специфика разработки политики информационной безопасности**	***Подготовка докладов по темам:*** 1. Практика компании Cisco Systems в разработке сетевой политики безопасности. 2. Подход компании Cisco Systems. 3. Подход компании Sun Microsystems. 4. Пример особенностей подхода к построению системы безопасности в компании IBM
4	**Тема 13. Лучшие практики создания и реализации политик информационной безопасности зарубежных компаний**	***Подготовка докладов по темам:*** 1. Практика компании Microsoft в области информационной безопасности 2. Пример политики сетевой безопасности. 3. Подход компании Symantec. Описание политики безопасности. 4. Подход SANS. Описание политики безопасности. Пример политики аудита безопасности.

4. Указания по проведению контрольных работ

4.1.Требование к структуре

Структура контрольной работы должна способствовать раскрытию темы: иметь титульный лист, содержание, введение, основную часть, заключение, список литературы.

4.2. Требования к содержанию (основной части)

1. Во введении обосновывается актуальность темы, определяется цель работы, задачи и методы исследования.

2. При определении целей и задач исследования необходимо правильно их формулировать. Так, в качестве цели не следует употреблять глагол «сделать». Правильно будет использовать глаголы «раскрыть», «определить», «установить», «показать», «выявить» и т.д.

3. Основная часть работы включает 2-4 вопроса, каждый из которых посвящается решению задач, сформированных во введении, и заканчивается констатацией итогов.

4. Приветствуется иллюстрация содержания работы таблицами, графическим материалом (рисунками, схемами и т.п.).

5. Необходимо давать ссылки на используемую литературу.

6. Заключение должно содержать сделанные автором работы выводы, итоги исследования.

7. Вслед за заключением идет список литературы, который должен быть составлен и оформлен с установленными требованиями. Если в работе имеются приложения, они оформляются на отдельных листах, и должны быть соответственно пронумерованы.

4.3. Требования к оформлению

Объем контрольной работы – 10-15 страниц формата А 4, напечатанного с одной стороны текста (1,5 интервал, шрифт Times New Roman).

4.4. Примерная тематика контрольных работ:

21. Методологические основы разработки политики информационной безопасности.
22. Теоретико-прикладные основы разработки политики информационной безопасности.
23. Основные принципы криптографии.
24. Задачи и принципы организации службы информационной безопасности.
25. Методология работы с аварийным планом.
26. Проведение расследований.
27. Реагирование на нарушение информационной безопасности.
28. Тестирование процедур и механизмов безопасности.
29. Карта информационной системы.
30. Общая методология оценки безопасности информационных технологий.
31. Реализация политики информационной безопасности.
32. Общие критерии оценки безопасности информационных технологий
33. Функциональные требования безопасности.
34. Требования доверия безопасности.
35. Профили защиты, разработанные на основе «Общих критериев».
36. Практическое применение международного стандарта безопасности информационных систем ISO 17799.
37. Основные требования к политике информационной безопасности.
38. Уровень средств безопасности.
39. Процесс разработки политики информационной безопасности.

40. Системы оценки текущей ситуации в области информационной безопасности на предприятии.

5. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная литература:

1.Барлаков, С. А. Модели и методы в управлении и экономике с применением информационных технологий : учебное пособие / С. А. Барлаков, С. И. Моисеев, В. Л. Порядина. — Санкт-Петербург : Интермедия, 2016. — 264 с. — ISBN 978-5-4383-0135-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/103198 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

2.Гришаева, С. А. Информационная безопасность в системах менеджмента качества : учебное пособие / С. А. Гришаева. — Москва : МАИ, 2021. — 63 с. — ISBN 978-5-4316-0804-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/256274 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

3.Черемухина, Ю. Ю. Системы менеджмента качества : учебное пособие / Ю. Ю. Черемухина. — Москва : РТУ МИРЭА, 2019. — 95 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/171525 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

4.Киреева, Н. В. Аудит информационной безопасности : методические указания / Н. В. Киреева, И. С. Поздняк, О. А. Караулова. — Самара : ПГУТИ, 2019. — 21 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/223223 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

Дополнительная литература:

5.Поздняк, И. С. Экспертные системы оценки информационной безопасности : методические указания / И. С. Поздняк, Н. В. Киреева, О. А. Караулова. — Самара : ПГУТИ, 2019. — 23 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/223304 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

8. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

Интернет-ресурсы:

2. www.fstec.ru – Официальный сайт ФСТЭК России.
3. www.securityforum.org - (лучшие практики, исследования, отчеты,

методологии).

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)

Перечень программного обеспечения: *MSOffice, PowerPoint.*
Информационные справочные системы:

1. Электронные ресурсы образовательной среды Университета
2. Рабочая программа и методическое обеспечение по дисциплине «Разработка политики информационной безопасности в организациях».
3. Учебный портал с электронно-методическими комплексами (do.kimes).
4. Универсальная библиотека онлайн (www.biblioclub.ru).
5. Polpred.com www.polpred.com.
6. Единое окно доступа (www.window.edu.ru)

Ресурсы информационно-образовательной среды Университета:
Рабочая программа и методическое обеспечение по курсу «Разработка политики информационной безопасности в организациях»