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)

Б1.ДВ.02.01 «ОСНОВЫ ТЕОРИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Направление подготовки: 10.04.01 - Информационная безопасность
Направленность (профиль): Менеджмент информационной безопасности
Уровень высшего образования: магистратура
Форма обучения: очная

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: Соляной В.Н. Рабочая программа дисциплины (модуля): Основы теории информационной безопасности. – Королев МО: «Технологический Университет», 2023

Рецензент: Сухотерин А.И.

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки магистров 10.04.01 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)	Соляной В.Н., к.в.н., доцент			
Год утверждения (переутверждения)	2023	2024		
Номер и дата протокола заседания кафедры	№8 от 29.03.2023г.			

Рабочая программа согласована:
Руководитель ОПОП ВО Сухотерин А.И.

Рабочая программа рекомендована на заседании УМС:

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

2

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

Целью изучения дисциплины являются:

1. Формирование у обучаемых концептуальных основ обеспечения информационной безопасности в процессе развития современного информационного общества на всех уровнях функционирования Российской Федерации: межгосударственном, государственном, ведомственном и отдельных граждан;

2. Дать обучаемым методологические аспекты решения основных прикладных задач по информационной безопасности на основе процесса поиска наиболее рациональных решений в различных информационных ситуациях на региональном и объектовом уровнях управления.

В процессе обучения по направлению подготовки 10.04.01 «Информационная безопасность», студент приобретает и совершенствует следующие компетенции:

Профессиональные компетенции:

- ПК-1: Способен организовывать выполнение работ, управлять коллективом автоматизированных ИАС в защищенном исполнении.
- ПК-3: Способен осуществлять анализ и систематизацию научно-технической информации, вырабатывать и внедрять научно-обоснованные решения в области защищенных технологий АИАД (автоматизированной информационно-аналитической деятельности.

Основными задачами дисциплины являются:

- раскрытие сущности, целей и содержание основ теории информационной безопасности и методологии защиты информации;
- определение общих методологических подходов построения систем защиты информации в современных условиях;
- освоение методических подходов установления состава защищаемой информации и выявления ключевых объектов защиты;
- выявление целесообразных методов определения актуальных информационных угроз и опасных нарушителей (злоумышленников);
- овладение современными методами оценки уязвимости защищаемой информации;
- определение методов выявления целесообразных параметров и структур потребных систем информационной безопасности;
- освоение методов установления целесообразного состава мероприятий по обеспечению функционирования систем информационной безопасности;
- раскрытие методов управления современными системами информационной безопасности;

- определение методологических подходов оценки эффективности мер по информационной безопасности.

Показатель освоения компетенции отражают следующие индикаторы:

Трудовые действия:

- ПК-1.3. Управлять работой коллектива профессионалов ИБ, разрабатывать нормативно-методические документы по функционированию автоматизированной ИАС, формировать комплекс мер по информационной защите автоматизированной ИАС с разработкой частных политик безопасности компьютерных систем.

- ПК-3.3. Организует научно-исследовательскую деятельность на основе тенденций развития, области научного знания и рынка труда.

Необходимые умения:

- ПК-1.2. Работать в коллективе, разрабатывать организационно-управленческие документы, принимать управленческие решения, реализовывать целесообразные меры противодействия информационным угрозам с применением национальных и международных стандартов в области ЗИ, оценивать их эффективность.

- ПК-3.2. Определять актуальность тематики исследовательской деятельности, формулировать темы НИР и оказывать методическую помощь в их выполнении.

Необходимые знания:

- ПК-1.1. Знать научные основы, методы и технологии управленческой деятельности, нормативную базу по созданию и эксплуатацию защищенных автоматизированных ИАС, принципы и методы организации работ по ЗИ в ИАС, основные средства и способы организационного обеспечения ИБ, источники и классификацию угроз ИБ.

- ПК-3.1. Знать проблемы и тенденции развития научной области и профессиональной деятельности, а также теоретические основы и технологии организации научно-исследовательской работы и требования к оформлению исследовательских разработок.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина относится к дисциплинам по выбору части, формируемой участниками образовательных отношений, основной образовательной программы подготовки магистров по направлению подготовки 10.04.01 Информационная безопасность, профиль подготовки – Менеджмент информационной безопасности региона.

Дисциплина базируется на ранее изученных в бакалавриате дисциплинах “Основы исследований информационной безопасности”, “Основы информационной безопасности”, на одновременно изучаемых дисциплинах: «Защищенные информационные системы» и компетенциях: УК-1; ОПК-1.

Знания и компетенции, полученные при освоении дисциплины «Основы теории информационной безопасности», являются базовыми при дальнейшем изучении дисциплин профессионального цикла «Концептуальное проектирование технологий обеспечения информационной безопасности», «Организационно-правовые механизмы обеспечения информационной безопасности», «Информационно-аналитические системы безопасности» прохождения практики (НИР), государственной итоговой аттестации и выполнения выпускной квалификационной работы (магистерской диссертации).

3. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 6 зачетных единиц, 216 часов.

Таблица 1

Виды занятий	Всего часов	Семестр 1	Семестр …	Семестр …	Семестр …
Общая трудоемкость	**216**	**216**			
ОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	**70**	**70**			
Лекции (Л)	**32**	**32**			
Практические занятия (ПЗ)	**32**	**32**			
Лабораторные работы (ЛР)					
Другие виды контактной работы*	**6**	**6**			
Практическая подготовка	**нет**	**нет**			
Самостоятельная работа	**144**	**144**			
Курсовые, расчетно-графические работы					
Контроль самостоятельной работы студентов	+	+			
Контрольная работа, домашнее задание	+	+			
Текущий контроль знаний (7 - 8, 15 - 16 недели)	**Тест**	**Тест**			
Вид итогового контроля	**Экзамен**	**Экзамен**			

* 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.	Практ. занят., час.	Занят. в интер акт. форме, час.	Код компетенций
Раздел 1. Концептуально-теоретические аспекты информационной безопасности				
Тема 1. Современные проблемы информационной безопасности	5	5	2	ПК-1,3
Тема 2. Научно-методологические основы интенсификации процессов информационной безопасности	5	5	2	ПК-3
Тема 3. Теоретико-методологические основы оценки угроз и уязвимостей информационных объектов	5	5	2	ПК-1,3
Тема 4. Методологические основы определения требований к информационной безопасности	5	5	2	ПК-1,3
Раздел 2. Прикладные основы теории информационной безопасности				
Тема 5. Методология формирования комплексных систем информационной безопасности	5	5	4	ПК-1
Тема 6. Особенности управления информационной безопасностью	5	5	2	ПК-1,3
Тема 7. Перспективы развития теории и практики информационной безопасности	2	2	2	ПК-1,3
Итого	**32**	**32**	**16**	

4.2. Содержание тем дисциплины

Тема 1. 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.

Тема 2. Научно-методологические основы интенсификации процессов информационной безопасности

Переход к интенсивным мерам по обеспечению информационной безопасности: сущность, необходимость, пути и условия перехода. Определение и принципы формирования основ теории информационной безопасности. Методологический базис основ теории информационной безопасности. Развитие неформальных подходов анализа процессов по информационной безопасности. Основы моделирования процессов информационной безопасности. Основное содержание теории информационной безопасности.

Тема 3. Теоретико-методологические основы оценки угроз и уязвимостей информационных объектов

Понятие и системная классификация современных информационных угроз. Основные теоретико-прикладные показатели уязвимости защищаемого информационного ресурса. Методологические основы достоверности прогнозирования уязвимости информационных объектов. Теоретико-прикладные модели оценки ущерба от реализации информационных угроз.

Тема 4. Методологические основы определения требований к информационной безопасности

Постановка задачи и методология определения основных требований к обеспечению информационной безопасности. Параметры безопасности информации и информационных объектов. Методология оценки

основных факторов, влияющих на требуемый уровень обеспечения информационной безопасности. Методологические основы определения весов и классификации возможных условий обеспечения информационной безопасности.

Тема 5. Методология формирования комплексных систем информационной безопасности

Системный подход как основа построения современных комплексов обеспечения информационной безопасности. Определение, типизация и стандартизация систем обеспечения информационной безопасности. Комплексные системы информационной безопасности как многокритериальные развивающие объекты. Современные методологии проектирования комплексных систем обеспечения информационной безопасности. Методологические основы оценки эффективности функционирования комплексных систем информационной безопасности.

Тема 6. Особенности управления информационной безопасностью

Основные научные принципы управления современными системами информационной безопасности. Общая задача по управлению информационной безопасностью. Типовая модель управления информационной безопасностью. Общие положения Концепции управления информационной безопасностью. Виды управления информационной безопасностью: краткосрочное; среднесрочное и долгосрочное. Методологические основы выработки управленческих решений по информационной безопасности и характеристика основных этапов принятия и реализации решений. Основы оптимизации управленческих решений по информационной безопасности. Виды и характеристика контрольных мероприятий по информационной безопасности. Основы организации обеспечения информационной безопасности государства и региона. Функции, задачи, структура и организация работы региональных центров информационной безопасности.

Тема 7. Перспективы развития теории и практики информационной безопасности

Анализ состояния и прогноз развития теории информационной безопасности. Развития Концепции специализированных центров информационной безопасности. Перспективы развития межведомственной системы подготовки и переподготовки кадров в области обеспечения информационной безопасности.

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

Методические указания для самостоятельной работы обучающихся по освоению дисциплины (модуля) «Теоретические основы информационной безопасности» представлены в Приложении 2 к настоящей программе.

6. Фонд оценочных средств проведения промежуточной аттестации обучающихся по дисциплине

Структура фонда оценочных средств проведения промежуточной аттестации обучающихся по дисциплине (модуля) «Теоретические основы информационной безопасности» приведена в Прил. 1 к настоящей РП.

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

Основная литература:

1. Гришина Н. В. Информационная безопасность предприятия: Учебное пособие / Гришина Наталия Васильевна. - 2; доп. - Москва; Москва: Издательство "ФОРУМ": ООО "Научно-издательский центр ИНФРА-М", 2015. - 240 с. - ДЛЯ СТУДЕНТОВ ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЙ. - ISBN 978-5-00091-007-8. URL: http://znanium.com/go.php?id=491597.

2.Малюк А. А. Теория защиты информации [Текст] / А. А. Малюк. - М.: Горячая линия - Телеком, 2013. - 184 с.: ил. - (Научное издание). - ISBN 978-5-9912-0246-6.

Дополнительная литература:

3.Бирюков А. Информационная безопасность: защита и нападение [Текст] / А. Бирюков. - М.: ДМК Пресс, 2012. - 474 с.: ил.; 60х90 /16. - ISBN 978-5-94074-647-8.

В-2

Основная литература:

1.Кауфман В.Ш. Человеко-машинный интерфейс систем управления. Концепции и принципы. – М.: Лань. - 2011. – 464 с. - [электронный ресурс] // http://znanium.com/catalog.php?bookinfo=409077

2. Терещенко П. В. Интерфейсы информационных систем / П.В. Терещенко; В.А. Астапчук. - Новосибирск: НГТУ, 2012. - 67 с. - ISBN 978-5-7782-2036-2. URL: http://biblioclub.ru/index.php?page=book&id=228775

Дополнительная литература:

3.Шишов О. В. Технические средства автоматизации и управления: учебное пособие / О.В. Шишов. — Москва: ИНФРА-М, 2021. — 396 с. + Доп. материалы [Электронный ресурс]. — (высшее образование: Бакалавриат). -

ISBN 978-5-16-010325-9. - Текст: электронный. - URL: https://znanium.com/catalog/product/1157118

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

Интернет-ресурсы:

1. http://www.biblioclub.ru
2. http://znanium.com

9. Методические указания для обучающихся по освоению дисциплины

Методические указания для обучающихся, по освоению дисциплины (модуля) «Теоретические основы информационной безопасности», приведены в Приложении 2 к настоящей РП.

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

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

- **Информационные справочные системы:**

1. Электронные ресурсы образовательной среды Университета..
2. Информационно-справочные системы (Консультант+; Гарант)

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

Лекционные занятия:

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

Практические занятия:

- Аудитория, оснащенная мультимедийными средствами (проектор, ноутбук), демонстрационными материалами (наглядными пособиями).
- рабочее место преподавателя, оснащенное ПК с доступом в глобальную сеть Интернет ;
- рабочие места студентов, оснащенные компьютерами с доступом в глобальную сеть Интернет.

Приложение 1

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ
ОСНОВЫ ТЕОРИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Направление подготовки: 10.04.01 - Информационная безопасность

Профиль: Менеджмент информационной безопасности

Уровень образования: магистратура

Форма обучения: очная

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 должен:		
				Трудовые действия	Необходимые умения	Необходимые знания
1.	ПК-1	Способен организовывать выполнение работ, управлять коллективом автоматизированных ИАС в защищенном исполнении.	Тема:1, 2, 4, 7	ПК-1.3. Управлять работой коллектива профессионалов ИБ, разрабатывать нормативно-методические документы по функционированию автоматизированной ИАС, формировать комплекс мер по информационной защите автоматизированной ИАС с разработкой частных политик безопасности компьютерных систем.	ПК-1.2 Работать в коллективе, разрабатывать организационно-управленческие документы, принимать управленческие решения, реализовывать целесообразные меры противодействия информационным угрозам с применением национальных и международных стандартов в области ЗИ, оценивать их эффективность	ПК-1.1. Знать научные основы, методы и технологии управленческой деятельности, нормативную базу по созданию и эксплуатацию защищенных автоматизированных ИАС, принципы и методы организации работ по ЗИ в ИАС, основные средства и способы организационного обеспечения ИБ, источники и классификацию угроз ИБ.
2.	ПК-3	,Способен осуществлять анализ и систематизацию научно-технической информации, вырабатывать и внедрять научно-обоснованные решения в области защищенных технологий АИАД (автоматизированной информационно-аналитической деятельности	Тема: 1-7	ПК-3.3. Организует научно-исследовательскую деятельность на основе тенденций развития, области научного знания и рынка труда.	ПК-3.2. Определять актуальность тематики исследовательской деятельности, формулировать темы НИР и оказывать методическую помощь в их выполнении.	ПК-3.1. Знать проблемы и тенденции развития научной области и профессиональной деятельности, а также теоретические основы и технологии организации научно-исследовательской работы и требования к оформлению исследовательских разработок.

Код компетенции	Инструменты, оценивающие сформированность компетенции	Показатель оценивания компетенции	Критерии оценки
ПК-1 ПК-3	***Тест***	***А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 90% правильных ответов*** ***Б) частично сформирована:*** • ***компетенция освоена на <u>продвинутом</u> уровне – 70% правильных ответов;*** • ***компетенция освоена на <u>базовом</u> уровне – от 51% правильных ответов;*** ***В) не сформирована (<u>компетенция не сформирована</u>) – менее 50% правильных ответов***	***Например:*** ***Проводится письменно. Время, отведенное на процедуру - 30 минут.*** ***Неявка – 0 баллов.*** ***Критерии оценки определяются процентным соотношением.*** ***Неудовлетворительно – менее 50% правильных ответов.*** ***Удовлетворительно - от 51% правильных ответов.*** ***Хорошо - от 70%.*** ***Отлично – от 90%.*** ***Максимальная оценка – 5 баллов.***
ПК-1 ПК-3	Доклад в форме презентации	***А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 90% правильных ответов*** ***Б) частично сформирована:*** • ***компетенция освоена на <u>продвинутом</u> уровне – 70% правильных ответов;*** • ***компетенция освоена на <u>базовом</u> уровне – от 51% правильных ответов;*** ***В) не сформирована (<u>компетенция не сформирована</u>) – менее 50% правильных ответов***	Проводится устно с использованием мультимедийных систем, а также с использованием технических средств Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие представленной презентации заявленной тематике (1 балл). 2.Качество источников и их количество при подготовке доклада и разработке презентации (1 балл). 3.Владение информацией и способность отвечать на вопросы аудитории (1 балл). 4.Качество самой представленной презентации (1 балл). 5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл). Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся непосредственно в день проведения презентации – для текущего контроля. Оценка проставляется в электронный журнал.
ПК-1,3	Контрольная	***А) полностью сформирована***	1. Проводится устно в форме защиты

	работа	***(компетенция освоена на <u>высоком</u> уровне) – 90% правильных ответов*** ***Б) частично сформирована:*** • ***компетенция освоена на <u>продвинутом</u> уровне – 70% правильных ответов;*** • ***компетенция освоена на <u>базовом</u> уровне – от 51% правильных ответов;*** ***В) не сформирована (<u>компетенция не сформирована</u>) – менее 50% правильных ответов***	отчета 2.Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие оформления требованиям (1 балл). 2. Соответствие разработанного устройства техническому заданию (1 балл) 3. Моделирование работы разработанного устройства (1 балл) 4. Качество и количество используемых источников (1 балл) 5. Правильность и полнота ответов на контрольные вопросы (1 балл) Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся непосредственно после защиты – для текущего контроля. Оценка проставляется в электронный журнал.

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

3.1 Примерная тематика докладов в форме презентаций:

1. Проблема информационной войны в современных условиях.
2. Информационное оружие и обеспечение информационной безопасности.
3. Методологические основы анализа состояния и развития менеджмента информационной безопасности региона.
4. Теоретико-прикладные основы деятельности международных независимых организаций в сфере информационной безопасности и их влияние на развитие защиты информации в регионе.
5. Теоретико-прикладные основы деятельности международных специализируемых организаций в сфере информационной безопасности и их влияние на развитие защиты информации в регионе.
6. Методологические основы организационного обеспечения информационной безопасности региона на уровне крупных поставщиков защищенных информационных систем.
7. Методологические основы развития государственно-регионального управления информационной безопасностью (российская практика).
8. Теоретико-прикладные основы организационного обеспечения информационной безопасности на государственно-региональном уровне

(практика США).

9. Теоретико-прикладные основы развития менеджмента информационной безопасности на уровне региональных предприятий.
10. Методологические основы построения унифицированной Концепции (политики) информационной безопасности региона.
11. Методологические основы построения и функционирования департамента информационной безопасности региона.
12. Теоретико-прикладные основы организации реагирования на чрезвычайные ситуации (инциденты) в области информационной безопасности региона.
13. Теоретико-прикладные основы организации и проведения аудита информационной безопасности региона.
14. Методологические основы применения программных средств, поддерживающих управление информационной безопасностью в регионе.
15. Методологические основы представления специализированных услуг по информационной безопасности в регионе.
16. Теоретико-прикладные основы страхования информационных рисков в регионе.
17. Теоретико-прикладные основы экономического анализа целесообразности мероприятий по информационной безопасности региона.
18. Методологические основы организационного обеспечения информационно-психологической безопасности региона.
19. Методологические основы организационного обеспечения энергоинформационной безопасности региона.
20. Теоретико-прикладные основы обеспечения информационной безопасности «облачных» информационных технологий региона.

3.2 Примерная тематика контрольных работ:

1. Вредоносные программы и антивирусные программные средства.
2. Методы программно-аппаратной защиты информации.
3. Аттестация объектов информатизации. Виды защиты информации.
4. Системы защиты информации.
5. Модели разграничения доступа.
6. Криптографические стандарты и их использование в информационных системах.
7. Способы и средства защиты информации от утечки по техническим каналам.
8. Принципы организации информационных систем в соответствии с требованиями по защите информации.
9. Основные нормативные правовые акты в области информационной безопасности и защиты информации.

10. Отечественные и зарубежные стандарты в области компьютерной безопасности.
11. Принципы и методы организационной защиты информации.
12. Методы и средства обнаружения уязвимостей в корпоративных компьютерных сетях.
13. Лицензирование и сертификация в области защиты информации.
14. Комплексные системы защиты информации.

3.3 Требования к контрольным работам

Требования к структуре контрольных работ

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

Требования к содержанию (основной части) контрольных работ

1. Во введении обосновывается актуальность темы, определяется цель работы, задачи и методы исследования.
2. Основная часть работы раскрывает процесс проектирования заданного аппаратного устройства и должна содержать соответствующие таблицы или временные диаграммы, которые должны формироваться разрабатываемым устройством, принципиальную схему устройства и описание его работы.
3. В процессе изложения материала необходимо давать ссылки на используемую литературу.
4. Заключение должно содержать сделанные автором работы выводы, итоги исследования.
5. Вслед за заключением идет список литературы, который должен быть составлен в соответствии с установленными требованиями.

Требования к оформлению

Объём контрольной работы – 5-6 страниц формата А 4, напечатанного с одной стороны текста (1,5 интервал, шрифт Times New Roman).

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

Формой контроля знаний по дисциплине «Основы теории информационной безопасности» являются две текущие аттестации в виде тестов и итоговая аттестация в виде экзамена.

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-1 ПК-3	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***
Проводится в сроки, установленные графиком образовательного процесса	тестирование	ПК-1 ПК-3	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***
Проводится в сроки, установленные графиком образовательного	Экзамен	ПК-1 ПК-3	3 вопроса	Экзамен проводится в устной форме, путем ответа на вопросы. Время, отведенное на процедуру – 30 минут.	Результаты предоставляются в день проведения	Критерии оценки: «**Отлично**»: 1. знание основных понятий предмета; 2. умение использовать и применять полученные знания на

процесса						практике; 3. работа на практических занятиях; 4. знание основных научных теорий, изучаемых предметов; 5. ответ на вопросы билета. «**Хорошо**»: • знание основных понятий предмета; • умение использовать и применять полученные знания на практике; • работа на практических занятиях; • знание основных научных теорий, изучаемых предметов; • ответы на вопросы билета • неправильно решено практическое задание «У**довлетвори-тельно**»: • демонстрирует частичные знания по темам дисциплин; • незнание неумение использовать и применять полученные знания на практике; • не работал на практических занятиях; «**Неудовлетвори-тельно**»: • демонстрирует частичные знания по темам дисциплин; • незнание основных понятий

						предмета; • неумение использовать и применять полученные знания на практике; • не работал на практических занятиях; • не отвечает на вопросы.

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.

4.1. Типовые вопросы, выносимые на тестирование

Тесты используются в режиме промежуточного контроля. По форме заданий выбраны закрытые тесты (с выборочным ответом). Каждому вопросу соответствует один вариант ответа.

1. Требование безопасности повторного использования объектов противоречит:
   инкапсуляции
   наследованию
   полиморфизму

2. Предположим, что при разграничении доступа учитывается семантика программ. В таком случае на игровую программу могут быть наложены следующие ограничения:
   запрет на чтение каких-либо файлов, кроме конфигурационных
   запрет на изменение каких-либо файлов, кроме конфигурационных
   запрет на установление сетевых соединений

3. В число граней, позволяющих структурировать средства достижения информационной безопасности, входят:
   меры обеспечения целостности
   административные меры
   меры административного воздействия

4. Дублирование сообщений является угрозой:
   доступности
   конфиденциальности
   целостности +

5. Самыми опасными источниками внутренних угроз являются:
   некомпетентные руководители
   обиженные сотрудники
   любопытные администраторы

6. Для внедрения бомб чаще всего используются ошибки типа:
   отсутствие проверок кодов возврата
   переполнение буфера
   нарушение целостности транзакций

7. В число целей политики безопасности верхнего уровня входят:
   решение сформировать или пересмотреть комплексную программу безопасности
   обеспечение базы для соблюдения законов и правил
   обеспечение конфиденциальности почтовых сообщений

8. В число целей программы безопасности верхнего уровня входят:
   управление рисками
   определение ответственных за информационные сервисы
   определение мер наказания за нарушения политики безопасности

9. В рамках программы безопасности нижнего уровня осуществляются:
   стратегическое планирование
   повседневное администрирование
   отслеживание слабых мест защиты

10. Политика безопасности строится на основе:
    общих представлений об ИС организации
    изучения политик родственных организаций
    анализа рисков

11. В число целей политики безопасности верхнего уровня входят:
    формулировка административных решений по важнейшим аспектам реализации программы безопасности
    выбор методов аутентификации пользователей
    обеспечение базы для соблюдения законов и правил +

4.2 Типовые вопросы, выносимые на экзамен

1.Существующие проблемы по информационной безопасности в современном информационном обществе.

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 (исторический аспект).

6. Современная постановка целей и задач по обеспечению информационной безопасности (переход к интенсивным мерам).

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.

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.

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 государства и региона.

28. Функции, задачи, структура и организация работы 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.

31. Проблема информационной войны в современных условиях.

32. Информационное оружие в современной системе обеспечения информационной безопасности.

33. Методологические основы анализа состояния и развития менеджмента информационной безопасности региона.

34. Теоретико-прикладные основы деятельности международных независимых организаций в сфере информационной безопасности и их влияние на развитие защиты информации в регионе.

35. Теоретико-прикладные основы деятельности международных специализируемых организаций в сфере информационной безопасности и их влияние на развитие защиты информации в регионе.

36. Методологические основы организационного обеспечения информационной безопасности региона на уровне крупных поставщиков защищенных информационных систем.

37. Методологические основы развития государственно-регионального управления информационной безопасностью (российская практика).

38. Теоретико-прикладные основы организационного обеспечения информационной безопасности на государственно-региональном уровне (практика США).

39. Теоретико-прикладные основы развития менеджмента информационной безопасности на уровне региональных предприятий.

40. Методологические основы построения унифицированной Концепции 43. (политики) информационной безопасности региона.

41. Методологические основы построения и функционирования департамента информационной безопасности региона.

42. Теоретико-прикладные основы организации реагирования на чрезвычайные ситуации (инциденты) в области информационной безопасности региона.

43. Теоретико-прикладные основы организации и проведения аудита информационной безопасности региона.

44. Методологические основы применения программных средств, поддерживающих управление информационной безопасностью в регионе.

45. Методологические основы представления специализированных услуг по информационной безопасности в регионе.

46. Теоретико-прикладные основы страхования информационных рисков в регионе.

47. Теоретико-прикладные основы экономического анализа целесообразности мероприятий по информационной безопасности региона.

48. Методологические основы организационного обеспечения информационно-психологической безопасности региона.

49. Методологические основы организационного обеспечения энергоинформационной безопасности региона.

50. Теоретико-прикладные основы обеспечения информационной безопасности «облачных» информационных технологий региона.

Приложение 2

Методические указания для обучающихся по освоению дисциплины

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ) ОСНОВЫ ТЕОРИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Направление подготовки: 10.04.01 - Информационная безопасность

Направленность (профиль): Менеджмент информационной безопасности

Уровень высшего образования: магистратура

Форма обучения: очная

Королев
2023

1. Общие положения

Цели дисциплины:

1. Формирование у обучаемых концептуальных основ обеспечения информационной безопасности в процессе развития современного информационного общества на всех уровнях функционирования Российской Федерации: межгосударственном, государственном, ведомственном и отдельных граждан;

2. Дать обучаемым методологические аспекты решения основных прикладных задач по информационной безопасности на основе процесса поиска наиболее рациональных решений в различных информационных ситуациях на региональном и объектовом уровнях управления.

Задачи дисциплины:

- раскрытие сущности, целей и содержание основ теории информационной безопасности и методологии защиты информации;
- определение общих методологических подходов построения систем защиты информации в современных условиях;
- освоение методических подходов установления состава защищаемой информации и выявления ключевых объектов защиты;
- выявление целесообразных методов определения актуальных информационных угроз и опасных нарушителей (злоумышленников);
- овладение современными методами оценки уязвимости защищаемой информации;
- определение методов выявления целесообразных параметров и структур потребных систем информационной безопасности;
- освоение методов установления целесообразного состава мероприятий по обеспечению функционирования систем информационной безопасности;
- раскрытие методов управления современными системами информационной безопасности;
- определение методологических подходов оценки эффективности мер по информационной безопасности.

2. Указания по проведению практических занятий

Практическое занятие 1.

Вид практического занятия**:**
смешанная форма практического занятия.
Образовательные технологии: *групповая дискуссия.*
Тема: **Современные проблемы информационной безопасности**

Учебные вопросы (содержание занятия):

1. Исторический аспект развития и становление обеспечения информационной безопасности в мире. Развитие и становление обеспечения информационной безопасности в России.
2. Место информационной безопасности в системе национальной безопасности России. Информационная безопасность как составляющая общей безопасности объектов государства.
3. Современная Доктрина информационной безопасности Российской Федерации. Проблема измерения характеристик информационной безопасности.

Продолжительность занятия – ***4 ч.***

Практическое занятие 2.

Вид практического занятия**:**
смешанная форма практического занятия.
Образовательные технологии: *беседа.*

Тема: **Научно-методологические основы интенсификации процессов информационной безопасности**

Учебные вопросы (содержание занятия):

1. Понятийный аппарат и классификация существующих теорий (с ракурса обеспечения информационной безопасности). Определение и классификация существующих современных теорий безопасности.
2. Определение и характеристика теории информационной безопасности. Понятие и общая характеристика методологии обеспечения информационной безопасности.
3. Современная Доктрина информационной безопасности Российской Федерации. Проблема измерения характеристик информационной безопасности.

Продолжительность занятия – 4 ***ч.***

Практическое занятие 3.

Вид практического занятия**:**
смешанная форма практического занятия.
Образовательные технологии: *практическая работа в группах.*

Тема: **Теоретико-методологические основы оценки уязвимости информационных объектов**

Учебные вопросы (содержание занятия):

1. Понятие и системная классификация современных информационных угроз. Основные показатели уязвимости защищаемого информационного ресурса.
2.Эмпирическая база методологии обеспечения информационной безопасности: - учет статистических данных реквизитов нарушений (угроз) и объектов информационной защиты. Методологические подходы оценки и анализа показателей информационной безопасности: оценка стоимости защищаемых информационных ресурсов.
3.Методологические подходы оценки и анализа показателей информационной безопасности: оценка интенсивности воздействия информационных угроз; оценка экономического ущерба от последствий реализации информационных угроз.

Продолжительность занятия – 4 ***ч.***

Практическое занятие 4.

Вид практического занятия**:**
смешанная форма практического занятия.
Образовательные технологии: *групповая дискуссия.*

Тема: **Методологические основы определения требований к информационной безопасности**

Учебные вопросы (содержание занятия):

1. Концептуальные принципы обеспечения информационной безопасности. Много рубежный и многозвенный подход обеспечения информационной безопасности.
2. Методы категорирования объектов и источников угроз информационной безопасности.
3.Методы категорирование уровней обеспечения информационной безопасности объектов.

Продолжительность занятия – 4 ***ч.***

Практическое занятие 5.

Вид практического занятия**:**
смешанная форма практического занятия.
Образовательные технологии: *беседа.*

Тема: **Методологические основы формирования комплексных систем информационной безопасности**

Учебные вопросы (содержание занятия):

1.Типизация и стандартизация систем обеспечения информационной безопасности.
2.Современные методологии проектирования комплексных систем обеспечения информационной безопасности.
3.Экономическая модель комплексной системы обеспечения информационной безопасности.
4.Вероятностная модель физической безопасности информационных объектов.
5.Экспертная модель комплексной системы обеспечения информационной безопасности.

Продолжительность занятия – ***4 ч.***

Практическое занятие 6.

Вид практического занятия**:**
смешанная форма практического занятия.
Образовательные технологии: *групповая дискуссия.*

Тема: **Особенности управления информационной безопасностью**

Учебные вопросы (содержание занятия):

1. Основные принципы управления современными системами информационной безопасности. Модель управления информационной безопасностью.
2. Концепции управления информационной безопасностью. Виды управления информационной безопасностью: краткосрочное; среднесрочное и долгосрочное.

3. Методологические основы выработки управленческих решений по информационной безопасности и характеристика основных этапов принятия и реализации решений.
4. Основы оптимизации управленческих решений по информационной безопасности.
5. Функции, задачи, структура и организация работы региональных центров информационной безопасности.

Продолжительность занятия – ***6 ч.***

Практическое занятие 7.

Вид практического занятия**:**
смешанная форма практического занятия.
Образовательные технологии: *практическая работа в группах.*

Тема: **Перспективы развития теории и практики информационной безопасности**

Учебные вопросы (содержание занятия):

1. Состояние и прогноз развития теории информационной безопасности.
2. Развитие Концепции специализированных региональных центров информационной безопасности.
3. Становление межведомственной системы подготовки и переподготовки кадров в области обеспечения информационной безопасности.
4. Методологические основы оценки рисков и эффективности систем информационной безопасности.
5. Эффективность систем страхования информационных рисков.

Продолжительность занятия – ***6 ч.***

3. Указания по проведению лабораторного практикума

Не предусмотрено учебным планом

4.Указания по проведению самостоятельной работы студентов

№ п/п	Наименование блока (раздела) дисциплины	Виды СРС
1.	Современные проблемы информационной безопасности	*Подготовка докладов по темам:* Проблема информационной войны в современных условиях. Информационное оружие и обеспечение информационной безопасности. Методологические основы анализа состояния и развития менеджмента информационной безопасности региона
2.	Научно-методологические основы интенсификации процессов информационной безопасности	*Подготовка докладов по темам:* Теоретико-прикладные основы деятельности международных независимых организаций в сфере информационной безопасности и их влияние на развитие защиты информации в регионе. Теоретико-прикладные основы деятельности международных специализируемых организаций в сфере информационной безопасности и их влияние на развитие защиты информации в регионе. Методологические основы организационного обеспечения информационной безопасности региона на уровне крупных поставщиков защищенных информационных систем.
3	Теоретико-методологические основы оценки угроз и уязвимостей информационных объектов	*Подготовка докладов по темам:* Методологические основы развития государственно-регионального управления информационной безопасностью (российская практика). Теоретико-прикладные основы организационного обеспечения информационной безопасности на государственно-региональном уровне (практика США). Теоретико-прикладные основы развития менеджмента информационной безопасности на

		уровне региональных предприятий.
4	Методологические основы определения требований к информационной безопасности	*Подготовка докладов по темам:* Методологические основы построения унифицированной Концепции (политики) информационной безопасности региона. Методологические основы построения и функционирования департамента информационной безопасности региона. Теоретико-прикладные основы организации реагирования на чрезвычайные ситуации (инциденты) в области информационной безопасности региона.
5	Методология формирования комплексных систем информационной безопасности	*Подготовка докладов по темам:* Теоретико-прикладные основы организации и проведения аудита информационной безопасности региона. Методологические основы применения программных средств, поддерживающих управление информационной безопасностью в регионе. Методологические основы представления специализированных услуг по информационной безопасности в регионе.
6	Особенности управления информационной безопасностью	*Подготовка докладов по темам:* Теоретико-прикладные основы экономического анализа целесообразности мероприятий по информационной безопасности региона. Методологические основы организационного обеспечения информационно-психологической безопасности региона.
7	Перспективы развития теории и практики информационной безопасности	*Подготовка докладов по темам:* Методологические основы организационного обеспечения энергоинформационной безопасности региона. Теоретико-прикладные основы обеспечения информационной безопасности «облачных» информационных технологий региона.

5.Указания по проведению контрольных работ для обучающихся очной формы обучения

5.1. Требования к структуре.

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

5.2. 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, сформулированных 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 в соответствии с установленными требованиями. Если в работе имеются приложения, они оформляются на отдельных листах, и должны быть соответственно пронумерованы.

5.3. Требования к оформлению.

Объём контрольной работы – … страниц формата А4, напечатанного с одной стороны текста (1,5 интервал, шрифт Times New Roman).

6. Перечень основной и дополнительной учебной литературы

Основная литература:

1. Гришина Н. В. Информационная безопасность предприятия: Учебное пособие / Гришина Наталия Васильевна. - 2; доп. - Москва; Москва: Издательство "ФОРУМ": ООО "Научно-издательский центр ИНФРА-М", 2015. - 240 с. - ДЛЯ СТУДЕНТОВ ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЙ. - ISBN 978-5-00091-007-8. URL: http://znanium.com/go.php?id=491597.
2.Малюк А. А. Теория защиты информации [Текст] / А. А. Малюк. - М.: Горячая линия - Телеком, 2013. - 184 с.: ил. - (Научное издание). - ISBN 978-5-9912-0246-6.

Дополнительная литература:

3.Бирюков А. Информационная безопасность: защита и нападение [Текст] / А. Бирюков. - М.: ДМК Пресс, 2012. - 474 с.: ил.; 60х90 /16. - ISBN 978-5-94074-647-8.
В-2

Основная литература:

1.Кауфман В.Ш. Человеко-машинный интерфейс систем управления. Концепции и принципы. – М.: Лань. - 2011. – 464 с. - [электронный ресурс] // http://znanium.com/catalog.php?bookinfo=409077
2. Терещенко П. В. Интерфейсы информационных систем / П.В. Терещенко; В.А. Астапчук. - Новосибирск: НГТУ, 2012. - 67 с. - ISBN 978-5-7782-2036-2. URL: http://biblioclub.ru/index.php?page=book&id=228775

Дополнительная литература:

3.Шишов О. В. Технические средства автоматизации и управления: учебное пособие / О.В. Шишов. — Москва: ИНФРА-М, 2021. — 396 с. + Доп. материалы [Электронный ресурс]. — (высшее образование: Бакалавриат). - ISBN 978-5-16-010325-9. - Текст: электронный. - URL: https://znanium.com/catalog/product/1157118

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

Интернет-ресурсы:

3. http://www.biblioclub.ru
4. http://znanium.com

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

Перечень программного обеспечения: *MSOffice, Multisim.*

Информационные справочные системы:

1. Электронные ресурсы образовательной среды Университета.
2. Информационно-справочные системы (Консультант+; Гарант).