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.О.15.05 «ОРГАНИЗАЦИЯ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (СЛУЖБА ИБ)»

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: Пономаренко Г.В. Рабочая программа дисциплины: Организация системы обеспечения информационной безопасности (служба ИБ). – 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

Целью изучения дисциплины является:

1. Подготовить специалиста, обладающего знаниями о порядке организации работы с персоналом допущенным к конфиденциальной информации;
2. Повысить уровень специальных 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. Формирование у студентов специализированной базы знаний по основным понятиям в области работы с персоналом допущенным к конфиденциальной информации;
4. Приобретение студентами первичных навыков по практическому формированию комплекса документов, составляющих нормативно - правовую базу защиты конфиденциальной информации.

В процессе обучения студент приобретает и совершенствует следующие компетенции.

ДОПК-1. Способен проводить анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба;

ДОПК-2. Способен формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы.

Основными **задачами** дисциплины являются:

1. Научить студентов самостоятельно решать поставленные задачи в области безопасности банковской деятельности на основе действующего российского законодательства с помощью с помощью современных принципов, методов, сил и средств в различных организационных структурах;
2. Научить студентов самостоятельно решать поставленные задачи в области защиты информации в банках по базовым направлениям защиты банковской тайны и конфиденциальной информации и формированием у обучающихся системы знаний;
3. Постоянно формировать систему знаний у обучающихся в области защиты информации в кредитно финансовой сфере деятельности.
4. Изучение особенностей современной организации противодействия угрозам информационной безопасности в кредитно – финансовой сфере;

5. Ознакомление с методами и средствами защиты информации банковских инструментов и технологий функциональных и контролирующих подразделений финансово – кредитных организаций.

Показатель освоения компетенции отражают следующие индикаторы:

Необходимые знания:

- знает технологии обеспечения информационной безопасности, способы их организации и оптимизации
- знает технологии проектирования и построения информационных систем
- знает стратегии обеспечения информационной безопасности, способы их организации и оптимизации
- знает определения рисков информационной безопасности применительно к объекту информатизации с заданными характеристиками
- знает методы и подходы к реализации системы управления безопасностью автоматизированных информационных систем
- знает методы анализа процессов для определения актуальных угроз
- знает особенности работы решений по защите информации в информационных процессах и системах

знает принципы обеспечения информационной безопасности объекта информатизаци;

- знает основные категории требований к программным и программно-аппаратным средствам защиты информации
- знает требования по защите автоматизированных систем от НСД
- знает методы хранения, обработки и передачи и получения информации из открытых информационных систем
- знает подходы к построению подсистем фиксации и реагирования на инциденты информационной безопасности
- знает принципы разработки организационных и технических мер по сбору, анализу и мониторингу событий безопасности
- знает как проводится анализ журналов событий средств защиты информации
- знает основные этапы расследования компьютерных преступлений в соответствии с нормативными требованиями
- знает руководящие документы в области классификации современных информационных систем и средств вычислительной и техники
- знает основы нормативно-правовых актов в области защиты информации конфиденциального характера
- знает как формируется организационно-распорядительная и эксплуатационная документация по обеспечению безопасности информационных систем

Необходимые умения:

- умеет обосновывать решения по обеспечению информационной безопасности объектов в профессиональной сфере деятельности
- умеет представлять процессы в формализованном виде на языках моделирования

- умеет делать выводы по результатам проведённого анализа, выявляя потенциальные угрозы ИБ
- умеет делать обоснованный выбор существующих средств защиты информации для нейтрализации определенного вида угроз
- владеет навыками выбора и применения современных аппаратных и программных средств технической защиты информации
- умеет анализировать эффективность применения мер по обеспечению ЗИ и разрабатывать предложения по совершенствованию структуры мер и повышению эффективности.
- умеет реагировать на инциденты информационной безопасности
- умеет сопоставлять основные структурно-функциональные характеристики информационных систем с требованиями руководящих документов
- умеет классифицировать информацию и автоматизированные системы, определять основные требования к ее защите

Трудовые действия:

- владеет навыками выявления и устранения угроз информационной безопасности
- владеет навыками реализации политики информационной безопасности
- владеет навыками применения современных программно-аппаратных средств моделирования информационных процессов и систем ЗИ
- владеет навыками оценки адекватности моделей и анализа результатов моделирования
- владеет навыками применения автоматизированных средств сбора и анализа информации, основанных на технологиях OSINT и data mining
- владеет навыками анализа надежности защиты информационных систем
- владеет навыками эффективного использования средств автоматического контроля и обнаружения возможных каналов утечки сведений, представляющих государственную, военную, служебную и коммерческую тайну
- владеет навыками классификации информационных систем и средств вычислительной техники по требованиям регуляторов ИБ
- владеет навыками сравнения и анализа существующих средств защиты информации
- владеет навыками нахождения наиболее подходящего решения применительно к заданным характеристикам информационной системы
- владеет навыками работы с нормативно-правовыми актами, навыками ориентации в них и поиска необходимой информации

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Организация системы обеспечения информационной безопасности (служба ИБ)» относится к обязательной 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», «Организационное и правовое обеспечение информационной безопасности», «Математическая логика и теория алгоритмов» и компетенциях: ОПК-1,3,5,6,8.

Знания и компетенции, полученные при освоении дисциплины, являются базовыми для изучения последующих дисциплин: «Экономика информационной безопасности», «Информационно-аналитическая деятельность по обеспечению комплексной безопасности», «Комплексное обеспечение защиты информации объекта информатизации (предприятия)», прохождения практики, государственной итоговой аттестации и выполнения выпускной квалификационной работы бакалавра.

3. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины для студентов очной формы составляет 4 зачетных единицы, 144 часов; для студентов очно - заочной формы составляет 4 зачетных единицы, 144 часов.

Таблица1

Виды занятий	**Всего часов**	**Семестр** 7	**Семестр 9**	**Семестр …**	**Семестр …**
Общая трудоемкость	144	144	**144**		
ОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	64	64			
Лекции (Л)	32	32			
Практические занятия (ПЗ)	32	32			
Лабораторные работы (ЛР)					
Самостоятельная работа	70	70			
Другие виды контактной работы	10	10			
Практическая подготовка	-нет	-нет			
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 с оценкой	Зачет с оценкой			
ОЧНО - ЗАОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	28		28		
Лекции (Л)	12		12		
Практические занятия (ПЗ)	16		16		
Лабораторные работы (ЛР)					
Самостоятельная работа	116		116		
Курсовые работы (проекты)	-		-		
Расчетно-графические работы	-		-		
Контрольная работа, домашнее задание	+		+		
Практическая подготовка	8		8		
Другие виды контактной работы	10		10		
Вид итогового контроля	Зачет с оценкой		Зачет с оценкой		

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/очно-заочное	Практические занятия, час Очное/очно-заочное	Занятия в интерактивной форме, час. Очное/очно-заочное	Код компетенций
Тема 1. Основные направления и методы работы с персоналом предприятия, допущенным к конфиденциальной информации	1/1	1/1	1/1	ДОПК-1
Тема 2. Сущность защиты конфиденциальной информации	1/1	1/1	1/1	ДОПК-1
Тема 3. Методы и формы защиты конфиденциальной информации	1/1	1/1	2/1	ДОПК-1
Тема 4. Подбор персонала и оформление допуска для работы с конфиденциальной информацией	1/1	1/1	2/1	ДОПК-1
Тема 5. Обучение сотрудников правилам и приемам работы с конфиденциальной информацией	1/1	1/1	2/1	ДОПК-1
Тема 6. Лицензирование деятельности организаций для проведения работ, связанных с конфиденциальной информацией	1/1	1/1	2/1	ДОПК-2
Тема 7. Режим хранения носителей конфиденциальной информации	2/1	2/1	1/1	ДОПК-2
Тема 8. Организация физической охраны предприятия, пропускного и внутриобъектового режимов	2/1	2/1	1/1	ДОПК-2
Тема 9. Организация защиты конфиденциальной информации при проведении закрытых мероприятий. Организация защиты конфиденциальной информации при осуществлении международного сотрудничества	2/1	2/4	2/1	ДОПК-2
Тема 10. Организация защиты конфиденциальной продукции в процессе транспортировки	2/1	2/2	2/1	ДОПК-2
Тема 11. Организация служебного расследования по	2/2	2/2	2/2	ДОПК-2

фактам утраты конфиденциальной информации				
Итого:	32/12	32/16	18/12	

4.2. Содержание тем дисциплины

Тема 1. Основные направления и методы работы с персоналом предприятия, допущенным к конфиденциальной информации

Основы работы с персоналом предприятия. Основные этапы работы с персоналом. Методы работы с персоналом и их характеристика. Мотивация деятельности персонала.

Тема 2. Сущность защиты конфиденциальной информации

Информационные ресурсы в условиях рыночной экономики. Способы, источники и методы промышленно-экономического шпионажа. Требования, предъявляемые к защите конфиденциальной информации. Условия, которым должна удовлетворять система защиты конфиденциальной информации. Угрозы конфиденциальной информации.

Тема 3. Методы и формы защиты конфиденциальной информации

Каналы утечки конфиденциальной информации. Методы защиты конфиденциальной информации. Система мер направленных на обеспечение конфиденциальной информации. Этапы процесса защиты конфиденциальной информации. Комиссия по защите конфиденциальной информации. Перечень сведений конфиденциальной информации. Распорядительные документы по защите конфиденциальной информации.

Тема 4. Подбор персонала и оформление допуска для работы с конфиденциальной информацией

Трехступенчатое анкетирование при приеме на работу. Трудовой договор (контракт) и договор (обязательство) о неразглашении конфиденциальной информации. требования к персоналу по международному стандарту ISO/TEC 17799/2000. Положения статьи 139 ГК РФ. Мероприятия, проводимые при подборе персонала для работы с конфиденциальной информацией. Технологическая цепочка при отборе персонала. Цели, определяемые при подборе специалистов при проведении бесед и собеседований. Порядок оформления допуска к конфиденциальным документам.

Тема 5. Обучение сотрудников правилам и приемам работы с конфиденциальной информацией

Работа с персоналом при устройстве на работу. Текущая работа с персоналом. Процесс обучения сотрудников. Задачи и методика обучения сотрудников. Основные формы контроля качества работы персонала.

Тема 6. Лицензирование деятельности организаций для проведения работ, связанных с конфиденциальной информацией

Нормы и требования российского законодательства в области лицензирования и сертификации. Случаи отказа в выдачи лицензии. Случаи

приостановления и аннулирования лицензии. Принципы лицензирования в области защиты конфиденциальной информации.

Тема 7. Режим хранения носителей конфиденциальной информации

Защищаемые помещения. Классификация помещений в зависимости от условий доступа. Инструкция о порядке сдачи под охрану и приема из-под охраны защищаемых и иных служебных помещений. Инструкция о порядке действий должностных лиц при пожаре, аварии или стихийном бедствии в защищаемых помещениях.

Тема 8. Организация физической охраны предприятия, пропускного и внутриобъектового режимов

Физическая охрана предприятия. Оперативный дежурный на предприятии. Руководитель подразделения (старший смены) личной охраны. Старший смены суточного наряда (дежурный по объекту). Сотрудник подразделения личной охраны. Сотрудник охраны. Система охраны частного предприятия. Меры, обеспечивающие нормальное функционирование предприятия. Меры активной защиты (обороны) предприятия. Пропускной и внутиобъектовый режимы предприятия. Организация пропускного режима. Инструкция о пропускном режиме.

Тема 9. Организация защиты конфиденциальной информации при проведении закрытых мероприятий. Организация защиты конфиденциальной информации при осуществлении международного сотрудничества

Этапы проведения закрытых совещаний и переговоров. Подготовка закрытого совещания. Защита информации в рекламно – выставочной деятельности. Обязанности руководителя организации, участвующей в международном сотрудничестве. Содержание плана проведения мероприятий.

Тема 10. Организация защиты конфиденциальной продукции в процессе транспортировки

Ответственность транспортников за сохранность грузов. Вопросы, требующие проработки при охране грузов. Особенности охраны грузов при использовании отдельных видов транспорта. Охрана груза перевозимого в купе пассажирского поезда. Охрана груза перевозимого в автомобиле. Использование воздушного транспорта.

Тема 11. Организация служебного расследования по фактам утраты конфиденциальной информации

Организация служебного расследования. Обязанности комиссии проводящей служебное расследование. Документы, предоставляемые руководителю организации для принятия решения.

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 «Организация работы с персоналом допущенным к конфиденциальной информации» приведена в Приложении 1.

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.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://eup.ru/catalog/all-all.asp** – научно-образовательный портал
2. **http://informika.ru/** – образовательный портал
3. **www.wikIsec.ru** - Энциклопедия информационной безопасности. – Публикации, статьи
4. **www.biblioclub.ru** - Универсальная библиотека онлайн
5. **www.rucont.ru** - ЭБС «Руконт»
6. **http://www.academy.it.ru/** – академия АЙТИ
7. **http://www.minfin.ru** - Официальный сайт Министерства финансов Российской Федерации
8. **http://www.gov.ru/** - Официальный сервер органов государственной власти Российской Федерации

9. **http://www.fsb.ru/ -** Официальный сайт Федеральной Службы Безопасности

10. **http://www.fstec.ru/ -** Официальный сайт Федеральной Службы по Техническому Экспортному контролю

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:**

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

Ресурсы информационно-образовательной среды МГОТУ:
Рабочая программа и методическое обеспечение по курсу «Организация системы обеспечения информационной безопасности (служба ИБ).

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

«ОРГАНИЗАЦИЯ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (СЛУЖБА ИБ)»

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.	ДОПК-1	Способен проводить анализ функционального процесса объекта защиты и его информационных составляющих с целью выявления возможных источников информационных угроз, их возможных целей, путей реализации и предполагаемого ущерба	Темы 1 -5	- владеет навыками выявления и устранения угроз информационной безопасности - владеет навыками реализации политики информационной безопасности - владеет навыками применения современных программно-аппаратных средств моделирования информационных процессов и систем ЗИ - владеет навыками оценки адекватности моделей и анализа результатов моделирования - владеет навыками применения автоматизир	- умеет обосновывать решения по обеспечению информационной безопасности объектов в профессиональной сфере деятельности - умеет представлять процессы в формализованном виде на языках моделирования - умеет делать выводы по результатам проведённого анализа, выявляя потенциальные угрозы ИБ - умеет делать обоснованный выбор существующих средств защиты информации для нейтрализации	- знает технологии обеспечения информационной безопасности, способы их организации и оптимизации - знает технологии проектирования и построения информационных систем - знает стратегии обеспечения информационной безопасности, способы их организации и оптимизации - знает определения рисков информационной безопасности применительно к объекту информатизации с заданными характеристикам и - знает методы и подходы к реализации системы управления безопасностью автоматизированных информационных систем - знает методы

				ованных средств сбора и анализа информации, основанных на технологиях OSINT и data mining - владеет навыками анализа надежности защиты информационных систем - владеет навыками эффективного использования средств автоматического контроля и обнаружения возможных каналов утечки сведений, представляющих государственную, военную, служебную и коммерческую тайну	определенного вида угроз - владеет навыками выбора и применения современных аппаратных и программных средств технической защиты информации	анализа процессов для определения актуальных угроз - знает особенности работы решений по защите информации в информационных процессах и системах - знает принципы обеспечения информационной безопасности объекта информатизаци - знает основные категории требований к программным и программно-аппаратным средствам защиты информации - знает требования по защите автоматизированных систем от НСД - знает методы хранения, обработки и передачи и получения информации из открытых информационных систем
2.	ДОПК-2	Способен формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих	Темы 6-11	- владеет навыками классификации информационных систем и средств вычислительной	- умеет анализировать эффективность применения мер по обеспечению ЗИ и	- знает подходы к построению подсистем фиксации и реагирования на инциденты информационной безопасности - знает

		с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы;		техники по требованиям регуляторов ИБ - владеет навыками сравнения и анализа существующих средств защиты информации - владеет навыками нахождения наиболее подходящего решения применительно к заданным характеристикам информационной системы - владеет навыками работы с нормативно-правовыми актами, навыками ориентации в них и поиска необходимой информации	разрабатывать предложения по совершенствованию структуры мер и повышению эффективности. - умеет реагировать на инциденты информационной безопасности - умеет сопоставлять основные структурно-функциональные характеристики информационных систем с требованиями руководящих документов - умеет классифицировать информацию и автоматизированные системы, определять основные требования к ее защите	принципы разработки организационных и технических мер по сбору, анализу и мониторингу событий безопасности - знает как проводится анализ журналов событий средств защиты информации - знает основные этапы расследования компьютерных преступлений в соответствии с нормативными требованиями - знает руководящие документы в области классификации современных информационных систем и средств вычислительной и техники - знает основы нормативно-правовых актов в области защиты информации конфиденциального характера - знает как формируется организационно-распорядительная и эксплуатационная документация по обеспечению безопасности информационных систем

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*
ДОПК-1,2	*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.***
ДОПК-1,2	*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. Правовые основы защиты тайны предварительного расследования.

2. Правовые основы защиты тайны предварительного расследования. Уголовная ответственность за ее разглашение.
3. Правовые основы защиты тайны судебного производства. Соотношения терминов « уголовное судопроизводство» и «судебное заседание».
4. Содержание принципа гласности судебного разбирательства. Специфика тайны судебного разбирательства.
5. Использование в ходе предварительного расследования и судебного разбирательства информации ограниченного доступа.
6. Роль и место информации ограниченного доступа в уголовном процессе. Специфика защиты государственной тайны в уголовном процессе.
7. Право на неприкосновенность частной жизни. Понятие права на неприкосновенность частной жизни.
8. Правовая охрана и защита права на неприкосновенность частной жизни.
9. Уголовно – правовая ответственность за нарушение права на неприкосновенность частной жизни.
10. Законодательные основания для ограничений прав граждан на неприкосновенность тайны частной жизни.
11. Основные положения российского законодательства, связанные с защитой персональных данных.
12. Европейская конвенция о защите личности в связи с автоматической обработкой персональных данных.
13. Правовая основа защиты персональных данных в Конституции РФ и других нормативно – правовых актах.
14. Основные положения Федерального закона «О персональных данных» и других подзаконных нормативно – правовых актах.
15. Принципы и условия обработки персональных данных. Права субъекта персональных данных.
16. Контроль и надзор за обработкой персональных данных. Ответственность за нарушение требований ФЗ «О персональных данных».
17. Объекты нарушения права на профессиональную тайну.
18. Права доверителя в отношении сведений, ставших на законном основании известными держателю профессиональной тайны. Защита доверителем своих прав.
19. Правовая защита профессиональной тайны.
20. Права доверителя в отношении сведений, ставших на законном основании известными держателю профессиональной тайны. Защита доверителем своих прав.

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

Формой контроля знаний по дисциплине «Организация системы обеспечения информационной безопасности (служба ИБ)» являются две текущие аттестации в виде тестов и итоговая аттестация в виде зачета с оценкой.

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	ДОПК-1,2	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	ДОПК-1,2	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	Зачет с оценкой	ДОПК-1,2	2 теоретических вопроса + практическое задание	зкзамен проводится в письменной форме, путем ответа на вопросы.	Результаты предоставляются в день проведения экзамена	Критерии оценки: «**Отлично**»: 1. знание основных понятий

графиком образовательного процесса				Время, отведенное на процедуру – 15 минут.		предмета; 2. умение использовать и применять полученные знания на 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.

Примерное содержание тестов для текущей аттестации:

ЗАДАНИЕ НА ВЫБОР ОДНОГО ПРАВИЛЬНОГО ВАРИАНТА ОТВЕТА

1. С какой тайной связывают банковскую тайну?

(!) Коммерческая тайна
(?) Государственная тайна
(?) Служебная тайна
(?) Тайна следствия и судопроизводства

2. Какие операции не могут осуществляться при банковских отношениях?

(?) Привлечение во вклады денежных средств физических и юридических лиц
(?) Открытие и ведение счетов физических и юридических лиц
(?) Размещение указанных средств от своего имени и за свой счет на условиях возврата
(!) Размещение указанных средств от своего имени и за свой счет

3. Какова величина суммы застрахованного банковского вклада?

(!) 1 млн. 400 тыс. руб.
(?) 800 тыс. руб.
(?) 100 тыс. руб.
(?) 150 тыс. руб.

4. Основной законодательный акт, в котором определена Банковская Тайна?

(?) Конституция РФ
(?) ФЗ. № 149 «Об информации, информационных технологиях и защите информации»
(!)ФЗ. № 395-1 «О Банках и Банковской деятельности»
(?) Доктрина ИБ

5. Кредитная организация не вправе осуществлять…?

(!) Лизинговые операции
(!) Оказание консультаций и информационных услуг
(!) Осуществление операций с драгоценными металлами и камнями в соответствии с законами
(?) Осуществление операций с драгоценными металлами и камнями

6. В соответствии, с каким законом сотрудник подписывает документ о неразглашении?

(?) Конституция РФ
(!) ФЗ. №86 «О ЦБ РФ»

(?) УК РФ
(?) ФЗ «О коммерческой тайне»

7. В соответствии, с каким законом обеспечивается сохранность ПД при аудиторских проверках?

(?) ФЗ. № 149 «Об информации, информационных технологиях и защите информации»
(?) ФЗ. №86 «О ЦБ РФ»
(?) ФЗ. № 395-1 «О Банках и Банковской деятельности»
(!) ФЗ. №107 «Об аудиторской деятельности»

8. Кто занимается созданием центральной базы кредитных историй?

(?) Вкладчик
(!) Бюро кредитных историй
(?) Специалист по ИБ
(?) Банк

9. Кому не может быть предоставлен кредитный отчет?

(?) Пользователь кредитной истории
(?) Субъекту кредитных историй
(?) В суд
(!) Родственникам

10. Обязательно ли попадет кредитная история в центральное бюро кредитных историй?

(!) Обязательно
(?) По желанию
(?) Не попадет
(?) Попадет через 5 лет

11. В соответствии, с каким законом осуществляется страхование счетов?

(?) ФЗ. №86 «О ЦБ РФ»
(?) ФЗ. № 395-1 «О Банках и Банковской деятельности»
(?) Конституцией РФ
(!) ФЗ. №177 «О страховых вкладах физических лиц в банковских организациях»

12. Чем регламентируется работа бюро кредитных историй?

(!) Законом о кредитных историях
(?) Конституцией РФ
(?) Уголовным кодексом
(?) Банком

13. Кредитная история хранится в течении?

(!) 15 лет с последнего изменения
(?) 16 лет с последнего изменения
(?) 10 лет с последнего изменения
(?) 5 лет с последнего изменения

14. Что не входит в кредитную историю?

(!) Сведения о месте работы
(?) ФИО
(?) Данные паспорта
(?) Индивидуальный номер налогоплательщика

15. Правом на сохранение БТ не обладает?

(!) Государство
(?) Доверитель
(?) Клиент
(?) Корреспондент

16.Согласно закону РФ «Об авторском праве» автор это:

(!) физическое лицо, творческим трудом которого создано произведение;
(?) юридическое лицо, творческим трудом которого создано произведение;
(?) физическое лицо, физическим трудом которого создано произведение;
(?) юридическое лицо, умственным трудом которого создано произведение.

17. Авторское право это:

(!) институт гражданского права, регулирующий отношения, связанные с созданием и использованием (изданием, исполнением, показом и т. д.) результатов творческой деятельности людей;

(?) институт гражданского права, регулирующий отношения, связанные с созданием и использованием (изданием, исполнением, показом и т. д.) периодических произведений;

(?) институт гражданского права, регулирующий отношения, связанные с разработкой нормативно правовой базы предприятий;

(?) институт уголовного права, регулирующий отношения, связанные с совершением преступных деяний.

18. Что из перечисленного относится к смежным правам:

(!) гражданские правоотношения тесно связанные с авторским правом, возникающие в ходе реализации исполнительных прав и прочих прав;

(?) гражданские правоотношения тесно связанные с авторским правом, возникающие в случае утери автором оригинала произведения;

(?) гражданские правоотношения тесно связанные с авторским правом, возникающие в ходе продажи авторских прав;

(?) юридические правоотношения не связанные с авторским правом.

19. Что не является объектом авторского права:

(?) фольклор;

(!) литературные произведения;

(!) музыкальные произведения;

(!) скульптуры.

20. После смерти автора, авторское право защищается в течении:

(!) 70 лет;

(?) 25 лет;

(?) 10 лет;

(?) 100 лет.

21. К неделимому соавторству относится:

(!) случаи, когда произведение образует неразрывное целое;

(?) случаи, когда созданное в соавторстве произведение состоит из частей, имеющих самостоятельное значение;

(?) случаи, когда произведение состоит из взаимозаменяемых частей;

(?) случаи, когда деление произведения не рассмотрено в договоре соавторов.

22. Право на произведение, обнародованное под псевдонимом, действует в течении:

(!) 70 лет;

(?) 100 лет;

(?) 25 лет;

(?) 10 лет.

23. Правовому регулированию смежных прав посвящается:

(!) часть 4 гражданского кодекса РФ;

(?) ФЗ №101 «Об авторском праве и смежных правах»;

(?) Постановление правительства РФ №93 «О смежных правах»;

(?) Указ президента РФ №60 «Перечень смежных прав».

24. Право на отзыв это:

(!) право позволяющее автору отказаться от ранее принятого решения об обнародовании произведения;

(?) право позволяющее другому лицу делать отзыв на произведение;

(?) право на составление отзыва на собственное произведение;

(?) право позволяющее автору отказаться от ранее принятого решения о составлении отзыва.

25. Произведение считается обнародованным если:

(!) в течении 30 дней после опубликования за пределами РФ оно было опубликовано на территории РФ;

(?) в течении 40 дней после опубликования за пределами РФ оно было опубликовано на территории РФ;

(?) после 10 дней поле опубликования в РФ;

(?) сразу после опубликования в РФ.

26. К авторским правам не относятся:

(!) специальное право;

(?) исключительное право;

(?) личные не имущественные права;

(?) иные права.

27. К личным не имущественным правам не относится:

(!) право на продажу произведения;

(?) право на обнародование произведения;

(?) право на имя;

(?) право авторства.

28. К исключительному праву относятся:

(!) право распространения;

(!) право публичного показа;

(?) право на отзыв;

(?) право на имя.

29. К иным правам не относится:

(!) право на издание;

(?) право на отзыв;

(?) право следования;

(?) право доступа.

30. Авторское право действует на:

(!) обнародованное произведение;

(!) необнародованное произведение;

(?) чужое произведение;

(?) федеральный закон.

31. Определение коммерческой тайны в соответствии с ФЗ «О коммерческой тайне»:

(!) Информация, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду;

(?) Информация, имеющая реальную или потенциальную ценность, в силу её неизвестности третьим лицам;

(?) Информация, которая может нанести ущерб, в случае её разглашения;

(?) Информация о деятельности коммерческой организации, которая может нанести непоправимый ущерб, в случае утечки.

32. Конфиденциальная составляющая коммерческой тайны:

(!) Конфиденциальная информация, отражающая следующие аспекты коммерческой деятельности: технические, экономические, организационные;

(?) Информация о коммерческой деятельности фирмы внутреннем и внешнем рынках;

(?) Информация об организационном порядке по работе с информацией конфиденциального характера;

(?) Персональные данные руководящего состава предприятия.

33. Интеллектуальная составляющая коммерческой тайны:

(!) Не обнародованные в официальном порядке результаты интеллектуальной деятельности: изобретения, полезные модели, промышленные образцы, оригинальные технологии, оригинальный набор информационных подходов;

(?) Обнародованные в официальном порядке результаты интеллектуальной деятельности: изобретения, полезные модели, промышленные образцы, оригинальные технологии, оригинальный набор информационных подходов;

(?) Документально зафиксированная информация об использовании и применении оригинальных технологий и подходов на предприятии;

(?) Часть коммерческой тайны, которая в явном виде не присутствует в перечне сведений, подразумевается.

34. Кем и когда утверждён, перечень сведений конфиденциального характера:

(!) Указ президента от 6 марта 1997 года №188;

(?) Постановление правительства от 5 декабря 2003 года № 89;

(?) Федеральный закон от 27 декабря 2002 года № 184-ФЗ;

(?) Федеральный закон от 28 декабря 2010 года № 390-ФЗ

35. Назовите документ, связанный с защитой информации, составляющей коммерческую тайну, посвящённый требованиям и рекомендациям по технической защите конфиденциальной информации

(!) «Специальные требования и рекомендации по защите конфиденциальной информации» решение президиума гостехкомиссии России № 7.2 от 2 марта 2001 года.

(?) Федеральный закон № 149 «Об информации, информационных технологиях и о защите информации»;

(?) Федеральный закон № 98 «О коммерческой тайне»;

(?) Гражданский кодекс РФ часть 4.

36. Какой нормативно - правовой акт регламентирует включение в договор с работодателем, условий о неразглашении охраняемой законом коммерческой тайны:

(!) Трудовой кодекс РФ;

(?) Федеральный закон «О коммерческой тайне»;

(?) Гражданский кодекс РФ;

(?) Уголовный кодекс РФ.

37. Каким документом определяются условия отнесения информации к сведениям, составляющим коммерческую тайну, обязанность соблюдения конфиденциальности такой информации, а так же ответственность за её разглашение:

(!) Федеральный закон № 149 «Об информации, информационных технологиях и о защите информации»;

(?) Гражданский кодекс РФ;

(?) Уголовный кодекс РФ;

(?) Федеральный закон № 98 «О коммерческой тайне».

38. Каким нормативно-правовым актом определяется защита элементов коммерческой тайны, которые рассматриваются как объекты интеллектуальной деятельности:

(!) Гражданский кодекс РФ от 18 декабря 2006 г. № 230-ФЗ часть 4. Глава 75 (право на секрет производства (ноу-хау));

(?) Федеральный закон «О коммерческой тайне»;

(?) Руководящий документ ФСТЭК «Специальные требования и рекомендации по защите конфиденциальной информации» (СТР-К)

(?) Уголовно-процессуальный кодекс РФ.

39. Какие требования предъявляются к лицу-обладателю информацией, составляющей коммерческую тайну:

(!) Оно владеет на законном основании; оно ограничивает доступ к информации, и установило режим коммерческой тайны в отношении этой информации;

(?) Оно является гражданином РФ; оно является законным держателем информации; оно обеспечивает защиту закрытой информации;

(?) Оно является юридическим лицом; оно установило режим конфиденциальной информации в отношении этой информации,

(?) Оно владеет информацией на законном основании; оно является гражданином РФ, проживающим на территории РФ не менее пяти лет; оно ограничило доступ к информации.

40. Признаки информации, обретённой незаконно:

(!) Получатель умышленно преодолевал меры по её охране; получатель знал, что получает информацию от лица, не имеющего право на её передачу получателю;

(?) Информация, так или иначе, имеет отношение к деловой активности конкретной фирмы;

(?) Информация, полученная из открытых источников;

(?) Плагиат.

41. Каким законом определяется порядок предоставление информации, составляющей коммерческую тайну:

(!) Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне»

(?) Руководящий документ ФСТЭК «Специальные требования и рекомендации по защите конфиденциальной информации» (СТР-К)

(?) Федеральный закон № 149 « Об информации, информационных технологиях и о защите информации»;

(?) Федеральный закон № 98 «О коммерческой тайне».

42. Дать определение контрагента в соответствии с ФЗ № 98 «О коммерческой тайне»:

(!) Сторона гражданско-правового договора, которой обладатель информации, составляющей коммерческую тайну, передал эту информацию;

(?) Сторона соглашения, которой обладатель информации, составляющей коммерческую тайну, передал эту информацию;

(?) Обладатель информации;

(?) Лицо, которому стала известна информация, в силу исполнения им служебных обязанностей.

43. Общие меры обеспечения соблюдения конфиденциальности информации:

(!) Разработка перечня информации, ограничение и регламентирование доступа, разработка и регулирование правил по регулированию отношений, нанесение на документы грифа коммерческой тайны;

(?) Разработка и регулирование правил организации обращения с конфиденциальной информацией;

(?) Организация конфиденциального документооборота на предприятии;

(?) Заключение соглашения с сотрудниками по обработке конфиденциальной информации.

44. Каких правил должен придерживаться работник при обработке информации конфиденциального характера:

(!) Выполнять установленный режим защиты, не разглашать сведения, составляющие коммерческую тайну; после прекращения трудовых отношений, вернуть работодателю все документы, составляющие коммерческую тайну;

(?) Не разглашать сведения, составляющие коммерческую тайну; выполнять установленный режим защиты;

(?) Выполнять обязанности, согласно ФЗ № 149 «Об информации, информационных технологиях и о защите информации»;

(?) Выполнять требования инструкции по организации обработки конфиденциальной информации в организации.

45. Срок действия права на секрет производства, с грифом коммерческая тайна:

(!) Действует до тех пор, пока сохраняется конфиденциальность сведений, составляющих коммерческую тайну в соответствии с гражданским кодексом РФ «Исключительное право на секрет производства» ст. 1467;

(?) Право на секрет производства с грифом коммерческая тайна не имеет срока давности;

(?) Право на секрет производства с грифом коммерческая тайна составляет тридцать календарных дней, с момента присвоения грифа;

(?) Действует до тех пор, пока сохраняется конфиденциальность сведений, составляющих коммерческую тайну, согласно федеральному закону № 98;

Кто утвердил перечень сведений конфиденциального характера № 188:

(!)Президент.

(?)Премьер министр.

(?)ФСТЭК.

(?)ФСБ.

46. Что понимается под мошенничеством, согласно статьи №159 УК РФ

(!)Хищение имущества или приобретение права на чужое имущество путем злоупотребления доверием.

(?)Хищение имущества.

(?)Приобретение права на чужое имущество с помощью злоупотребления доверием.

(?)Получение имущества с помощью применения силы.

47. К правовым методам защиты информации доктрина относит:

(!)Разработка нормативно правовых актов, регламентирующих отношение в информационной сфере.

(?)Составление списка ответственных лиц.

(?)Указание по использованию физических средств ЗИ.

(?)Указание по использованию технических средств ЗИ.

48. Сколько видов конфиденциальной информации существует в соответствии с указом президента №188 1997 года?

(?)5.

(?)4.

(!)6.

(?)8.

49. Врачебная тайна, адвокатская тайна, нотариальная тайна, тайна переписки. К какому виду конфиденциальной информации относятся перечисленные тайны?

(?)Служебная тайна.

(?)Коммерческая тайна.

(?)Персональные данные.

(!)Профессиональная тайна.

50. Субъектами банковской тайны являются:

(!)Держатели.

(!)Кредитные организации.

(?)Вкладчики.

(?)Государство.

51. Определение организационно-розыскной деятельности

(!)Вид деятельности, осуществляющий по средствам ОРМ в целях защиты конституционных прав гражданина.

(?)Вид деятельности, направленный на безопасность общества, государства, личности.

(?)Вид деятельности, осуществляющийся по средства ОРМ в целях раскрытия инцидентов нарушения ИБ.

52. Какие сведения относятся к информации конфиденциального характера

(!)Сведения о возможных природных бедствиях.

(?)Информация, составляющая тайну следствия.

(?)Сведения, связь с профессиональной деятельностью.

(?)Сведения, связь с коммерческой деятельностью.

53. Информация, составляющая коммерческую тайну:

(?)Товарные знаки.

(?)Авторское право.

(?)Государственная тайна.

(!)Банковская тайна.

54. Чем охраняется информация, ограниченного доступа?

(!)Федеральными законами.

(?)Ведомственными приказами.

(?)Силовыми структурами (ведомствами).

55. За разглашение сведений конфиденциального характера наступает ответственность:

(?)Уголовная.

(?)Административная.

(?)Дисциплинарная.

(!)Все вышеперечисленные.

56. С правовой точки зрения защите подлежит:

(?)Любая закрытая информация.
(!)Информация, зафиксированная на материальном носителе.
(?)Любая коммерческая тайна.
(?)Всё вышеперечисленное.

Типовые вопросы, выносимые зачет с оценкой

1. Основные угрозы информационной безопасности РФ.
2. Правовые режимы распространения информации в исключительных ситуациях, представляющих угрозу безопасности РФ.
3. Совершенствование правого регулирования информационной безопасности.
4. Законодательная основа защиты государственной тайны.
5. Уголовно – правовая защита сведений, составляющих государственную тайну.
6. Правовая защита служебной информации ограниченного распространения.
7. Правовая защита служебной тайны, основу которой составляет конфиденциальная.
8. Правовая защита служебной информации ограниченного распространения.
9. Правовая охрана и защита прав на информационно – телекоммуникационные системы.
10. Основные положения общеевропейской Конвенции о киберпреступности.
11. Криминалистическая характеристика компьютерных преступлений.
12. Понятие и история правовой охраны программ для ЭВМ и баз данных.
13. Правовое регулирование деятельности в области обеспечения связи. Понятие тайны связи и ее правовая защита.
14. Обеспечение безопасности ведомственной информации, информационных ресурсов, средств и систем информации.
15. Основные цели и задачи правовой защиты информации.
16. Методы правовой защиты информации.
17. Подзаконные, ведомственные и локальные правовые акты, действующие в сфере защиты основных видов конфиденциальной информации.
18. Сущность государственной защиты участников уголовного судопроизводства.
19. Правовые основы защиты тайны предварительного расследования.
20. Использование в ходе предварительного расследования и судебного разбирательства информации ограниченного доступа.
21. Право на неприкосновенность частной жизни.
22. Основные положения Федерального закона «О персональных данных» и некоторых подзаконных нормативно – правовых актов.
23. Субъекты и объекты правоотношений в области защиты профессиональной тайны.
24. Ответственность, связанная с нарушением законодательства о коммерческой тайне.
25. Современное правовое регулирование авторских прав.
26. Интеллектуальные права авторов произведений литературы, науки и искусства. Правовая защита смежных прав.
27. Патент как форма охраны объектов патентного права.
28. Передача исключительного права на изобретения, полезные модели и промышленные образцы.
29. Соотношение понятий «защита информации» и «информационная безопасность». Цель и задачи защиты информации.
30. Организационно – правовые принципы защиты информации.
31. Методы правовой защиты информации.
32. Понятие правовой защиты информации, ее методов и способов.
33. Закрепление права предприятия на защиту информации в нормативных документах (коллективном договоре, трудовом договоре, иных локальных правовых актах организаций).
34. Права и обязанности органов, обеспечивающих государственную защиту.
35. Соотношения терминов « уголовное судопроизводство» и «судебное заседание».
36. Содержание принципа гласности судебного разбирательства.

37. Роль и место информации ограниченного доступа в уголовном процессе. Право на неприкосновенность частной жизни.
38. Правовая охрана и защита права на неприкосновенность частной жизни.
39. Уголовно – правовая ответственность за нарушение права на неприкосновенность частной жизни.
40. Основные положения российского законодательства, связанные с защитой персональных данных.
41. Европейская конвенция о защите личности в связи с автоматической обработкой персональных данных.
42. Правовая основа защиты персональных данных в Конституции РФ и других нормативно – правовых актах.
43. Основные положения Федерального закона «О персональных данных» и некоторых подзаконных нормативно – правовых актах.
44. Ответственность за нарушение требований ФЗ «О персональных данных».
45. Субъекты и объекты правоотношений в области защиты профессиональной тайны.
46. Права доверителя в отношении сведений, ставших на законном основании известными держателю профессиональной тайны.
47. Основные понятия, связанные с банковской тайной, и правовая основа ее защиты.
48. Объекты и субъекты банковской тайны.
49. Действующие нормативно – правовые акты, устанавливающие требования по защите коммерческой тайны.
50. Понятие результатов интеллектуальной деятельности, средств индивидуализации и иных объектов, созданных в результате деятельности, приравненной к интеллектуальной деятельности.
51. Понятие объектов интеллектуальной собственности и их законодательный перечень.
52. Правовая защита авторских и смежных прав.
53. Лицензирование в области материализации отдельных результатов интеллектуальной деятельности.
54. Понятие патентного права.
55. Патент как форма охраны объектов патентного права.
56. Административная и уголовная ответственность, связанная с нарушением изобретательских и патентных прав.
57. Контроль со стороны Роспатента за некоторыми направлениями реализации патентного законодательства.
58. Международное и межгосударственное сотрудничество России в области защиты патентных прав.
59. Современное правовое регулирование отношений в области охраны средств индивидуализации.
60. Правовое регулирование прав на коммерческое обозначение.
61. Использование товарного знака, знака обслуживания и наименования места происхождения товара, как механизма защиты.

**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)

«ОРГАНИЗАЦИЯ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (СЛУЖБА ИБ)»

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:

– Ускоренная адаптация студентов в предметную область информационная безопасность (защита интеллектуальной собственности), опираясь на весь спектр научных воззрений, на развитие и правовую защиту информационно - телекоммуникационной инфраструктуры и компьютерной информации;

– 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;

– Изучение правовых основ информационной безопасности и информирование студентов о законодательных источниках, подзаконных и ведомственных правовых актах обеспечивающих информационную безопасность личности, общества и государства;

– Формирование у студентов специализированной базы знаний по основным понятиям в области правовой защиты информации и охраны интеллектуальной собственности;

– Приобретение студентами первичных навыков по практическому формированию комплекса документов, составляющих правовую базу защиты информации и охраны интеллектуальной собственности на предприятиях и в организациях.

Задачами дисциплины является:

1. Теоретические основы обеспечения защиты интеллектуальной собственности на основе действующего российского законодательства с помощью с помощью современных принципов, методов, сил и средств в различных организационных структурах;

2. Практические аспекты правовой защиты интеллектуальной собственности по базовым направлениям защиты государственной, профессиональной, коммерческой тайны и конфиденциальной информации и формированием у обучающихся системы знаний.

2. Указания по проведению практических занятий

Тема 1. Правовые основы обеспечения информационной безопасности

Практическое занятие 1.

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

Образовательные технологии: ***групповая дискуссия***

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

Тема и содержание практического занятия:

Цель работы: Получить практические навыки анализа нормативно-правовых документов в области информационной безопасности

Основные положения темы занятия:

1. основные правовые аспекты, в области информационной безопасности применяемые для защиты интеллектуальной собственности;
2. необходимость правовой защиты продуктов творческой деятельности

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

б) Обзор касающихся изменений и дополнений нормативно – правовых документов по информационной безопасности и защите информации в рамках изучаемой темы (содоклад).

Учебные вопросы:

1. Основные угрозы информационной безопасности РФ.

2.Правовые режимы распространения информации в исключительных ситуациях, представляющих угрозу безопасности РФ.

3. Совершенствование правого регулирования информационной безопасности.

Продолжительность занятия: 4.0/3.0

Тема 2. Понятие и состав информационных систем и прав на них

Практическое занятие 2.

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

Образовательные технологии: ***групповая дискуссия***

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

Тема и содержание практического занятия:

Цель работы: Получить практические навыки анализа нормативно-правовых документов в области организации обработки информации в информационных системах различного назначения

Основные положения темы занятия:

1. основные правовые аспекты, в области информационной безопасности применяемые для защиты интеллектуальной собственности;

2. интеллектуальное право как право на результаты интеллектуальной деятельности

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

б) Обзор касающихся изменений и дополнений нормативно – правовых документов по информационной безопасности и защите информации в рамках изучаемой темы (содоклад).

Учебные вопросы:

1.Законодательная основа защиты государственной тайны.

2. Обеспечение защиты государственной тайны.

3. Нормативное регулирование оборота сведений, составляющих государственную тайну, в системе МВД РФ.

4. Уголовно – правовая защита сведений, составляющих государственную тайну.

Продолжительность занятия: 4.0//3.0

Тема 3. Институт правовой охраны программ для ЭВМ и баз данных

Практическое занятие 3.

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

Образовательные технологии: ***групповая дискуссия***

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

Тема и содержание практического занятия:

Цель работы: Получить практические навыки анализа нормативно-правовых документов в области организации обработки информации в информационных системах различного назначения

Основные положения темы занятия:

1. основные правовые аспекты, в области информационной безопасности применяемые для защиты интеллектуальной собственности;

2. исторические истоки патентного права

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

б) Обзор касающихся изменений и дополнений нормативно – правовых документов по информационной безопасности и защите информации в рамках изучаемой темы (содоклад).

Учебные вопросы:

1.Понятие и состав информационных систем.

2.Территориальные и ведомственные уровни формирования единого информационного пространства.

3. Правовая охрана и защита прав на информационно – телекоммуникационные системы.

4. Обзор касающихся изменений и дополнений нормативно – правовых документов по информационной безопасности и защите информации в рамках изучаемой темы.

Продолжительность занятия: 4.0/3.0

Тема 4. Институт правовой защиты тайны частной жизни и персональных данных

Практическое занятие 4.

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

Образовательные технологии: ***групповая дискуссия***

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

Тема и содержание практического занятия:

Цель работы: Получить практические навыки анализа нормативно-правовых документов в области организации обработки информации в информационных системах различного назначения

Основные положения темы занятия:

1. основные правовые аспекты, в области информационной безопасности применяемые для защиты интеллектуальной собственности;
2. объекты и субъекты промышленной собственности и патентного права

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

б) Обзор касающихся изменений и дополнений нормативно – правовых документов по информационной безопасности и защите информации в рамках изучаемой темы (содоклад).

Учебные вопросы:

1.Тенденции усиления борьбы с компьютерными преступлениями на международном уровне.

2. Основные положения общеевропейской Конвенции о киберпреступности.

3.Информационные и компьютерные преступления.

4.Термины и понятия связанные с правоотношениями в компьютерной сфере.

5. Криминалистическая характеристика компьютерных преступлений.

Продолжительность занятия: 4.0/3.0

Тема 5. Основные объекты интеллектуальной собственности и их правовая защита

Практическое занятие 5.

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

Образовательные технологии: ***групповая дискуссия***

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

Тема и содержание практического занятия:

Цель работы: Получить практические навыки анализа нормативно-правовых документов в области организации обработки информации в информационных системах различного назначения

Основные положения темы занятия:

1. основные правовые аспекты, в области информационной безопасности применяемые для защиты интеллектуальной собственности;
2. оформление прав патентообладателя

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

б) Обзор касающихся изменений и дополнений нормативно – правовых документов по информационной безопасности и защите информации в рамках изучаемой темы (содоклад).

Учебные вопросы:

1.Понятие и история правовой охраны программ для ЭВМ и баз данных.

2. Основные положения четвертой части Гражданского кодекса РФ, касающейся правовой охраны программ для ЭВМ и баз данных.

3. Выявление контрафакции программного обеспечения.

Продолжительность занятия: 40/3.0

Тема 6. Институт правовой защиты авторских и смежных прав

Практическое занятие 6.

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

Образовательные технологии: ***групповая дискуссия***

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

Тема и содержание практического занятия:

Цель работы: Получить практические навыки анализа нормативно-правовых документов в области организации обработки информации в информационных системах различного назначения

Основные положения темы занятия:

1. основные правовые аспекты, в области информационной безопасности применяемые для защиты интеллектуальной собственности;

2. оформление прав патентообладателя (заявка на изобретение).

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

б) Обзор касающихся изменений и дополнений нормативно – правовых документов по информационной безопасности и защите информации в рамках изучаемой темы (содоклад).

Учебные вопросы:

1.Международные нормативные правовые акты.

2.Российские официальные документы и нормативные правовые акты.

3. Понятие средств индивидуализации юридических лиц, товаров, работ, услуг и предприятий.

4.Современное правовое регулирование отношений в области охраны средств индивидуализации.

5. Действие в России международных правовых актов по охране средств индивидуализации.

Продолжительность занятия: 4.0/3.0

Тема 7. Институт правовой защиты изобретений, полезных моделей и промышленных образцов

Практическое занятие 7.

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

Образовательные технологии: ***групповая дискуссия***

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

Тема и содержание практического занятия:

Цель работы: Получить практические навыки анализа нормативно-правовых документов в области организации обработки информации в информационных системах различного назначения

Основные положения темы занятия:

1. основные правовые аспекты, в области информационной безопасности применяемые для защиты интеллектуальной собственности;

2. оформление прав патентообладателя (заявка на полезную модель и на промышленный образец).

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

б) Обзор касающихся изменений и дополнений нормативно – правовых документов по информационной безопасности и защите информации в рамках изучаемой темы (содоклад).

Учебные вопросы:

1.Понятие коммерческой тайны и ее генезис. 2.Действующие нормативно – правовые акты, устанавливающие требования по защите коммерческой тайны.

3.Основные положения Федерального закона « О коммерческой тайне».

4.Основные положения части четвертой Гражданского кодекса РФ, касающейся защиты коммерческой тайны.

5.Ответственность, связанная с нарушением законодательства о коммерческой тайне.

6. Зарубежный опыт правовой защиты коммерческой тайны.

Продолжительность занятия: 4.0/3.0

Тема 8. Институт правовой охраны наименований и товарных знаков (средств индивидуализации юридических лиц, товаров, работ, услуг и предприятий)

Практическое занятие 8.

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

Образовательные технологии: ***групповая дискуссия***

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

Тема и содержание практического занятия:

Цель работы: Получить практические навыки анализа нормативно-правовых документов в области организации обработки информации в информационных системах различного назначения

Основные положения темы занятия:

1. основные правовые аспекты, в области информационной безопасности применяемые для защиты интеллектуальной собственности;
2. объем правовой охраны предоставляемый патентом.

Вопросы для обсуждения:

а) Основной доклад (реферат) по теме занятия.

б) Обзор касающихся изменений и дополнений нормативно – правовых документов по информационной безопасности и защите информации в рамках изучаемой темы (содоклад).

Учебные вопросы:

1. Понятие результатов интеллектуальной деятельности, средств индивидуализации и иных объектов, созданных в результате деятельности, приравненной к интеллектуальной деятельности.
2. Защита интеллектуальных прав. Понятие и генезис авторских и смежных прав.
3. Современное правовое регулирование авторских прав.
4. Интеллектуальные права авторов произведений литературы, науки и искусства.
5. Правовая защита смежных прав. Ответственность за нарушение авторских и смежных прав.
6. Понятие патентного права.
7. Характеристика объектов патентного права.
8. Патент как форма охраны объектов патентного права.
9. Генезис авторских и смежных прав.
10. Передача исключительного права на изобретения, полезные модели и промышленные образцы.
11. Защита прав авторов и патентообладателей.
12. Участие России в работе международных организаций по защите прав авторов и патентообладателей.

Продолжительность занятия: 4.0/3.0

3. Указания по проведению лабораторных занятий

(нет)

Тема: Построение системы организационного обеспечения предприятия (организации) для проведения расследования инцидентов информационной безопасности

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

Тема и содержание практического занятия:

Цель работы: Получить практические навыки анализа нормативно-правовых документов в области организации обработки информации в информационных системах различного назначения и проведения расследования преступлений в области высоких технологий

Основные положения темы занятия:

1. основные правовые аспекты, в области информационной безопасности применяемые для предотвращения и расследования преступлений в области высоких технологий;
2. предотвращение и мониторинг.
3. компьютерная криминалистика.
4. разработка и внедрение СПО.

Продолжительность занятия: 16/12

4. Указания по проведению самостоятельной работы студентов

№ п/п	Наименование блока (раздела) дисциплины	Виды СРС
1.	**Тема 2. Основы информационно-аналитической деятельности при обеспечении информационной безопасности**	***Подготовка докладов по темам:*** 1. Международная система по противодействию легализации преступных доходов и финансированию терроризма, противодействие финансированию терроризма и экстремизма. 2. Формы и методы подготовки аналитической информации. 3. Информационные ресурсы в первичном (государственном) финансовом мониторинге.
2.	**Тема3. Методика информационно-аналитической работы**	***Подготовка докладов по темам:*** 1. Информационное взаимодействие и ресурсы в государственном финансовом мониторинге. 2. Основы контрольно-надзорной деятельности. 3. Международная гражданская служба.
3	**Тема 4. Методы изучения документальных источников**	***Подготовка докладов по темам:*** 1. Государственная гражданская служба в РФ. 2. Системы внутреннего контроля в субъектах финансового мониторинга; Финансовые расследования в международном (государственном) финансовом мониторинге.
4	**Тема 5. Формы и виды составления отчетов о проделанной информационно-аналитической работе**	***Подготовка докладов по темам:*** 1. Типологический анализ в первичном (государственном, международном) финансовом мониторинге. 2. Национальная система по противодействию легализации преступных доходов и финансированию терроризма.

5. Указания по проведению контрольных работ

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, 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.

5.3. Требования к оформлению

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

5.4. Примерная тематика контрольных работ:

1. Международная система по противодействию легализации преступных доходов и финансированию терроризма, противодействие финансированию терроризма и экстремизма.
2. Формы и методы подготовки аналитической информации.
3. Информационные ресурсы в первичном (государственном) финансовом мониторинге.
4. Информационное взаимодействие и ресурсы в государственном финансовом мониторинге.
5. Основы контрольно-надзорной деятельности.
6. Международная гражданская служба.
7. Государственная гражданская служба в РФ.
8. Системы внутреннего контроля в субъектах финансового мониторинга; Финансовые расследования в международном (государственном) финансовом мониторинге.
9. Типологический анализ в первичном (государственном, международном) финансовом мониторинге.
10. Национальная система по противодействию легализации преступных доходов и финансированию терроризма.
11. Сущность аналитической разведки.
12. Пределы возможностей аналитической разведки.
13. Данные, сведения, информация. Место аналитической разведки.
14. Аналитическая контрразведка. Информационное влияние. Репутация. Конкуренты.
15. Аналитическая разведка и национальная стратегия.
16. Разведка, журналистика, научная деятельность.
17. Уровни аналитической работы. Феномен истины. Работа с фактами.

18. Аналитическая разведка и официальная идеология. Определение круга интересов.
19. Структура службы. Размещение службы. Структура деятельности.
20. Учет работы сотрудников. Защита секретов. Обеспечение эффективности.
21. Творческие учреждения в системе аналитической разведки. Компоненты работы. Информационная задача. Опережение запросов. Минимизация ошибок.
22. Структура аналитической записки. Формулирование выводов. Корректность документа. Представление материалов.
23. Общие представления о мониторинге. Стратегический мониторинг. Оперативный мониторинг.
24. Задачи разведывательного мониторинга. Мониторинг средств массовой информации. Мониторинг массовых настроений.
25. Мониторинг массовой активности. Мониторинг учреждений. Мониторинг ведущих деятелей.
26. Система прогнозирования. Структура прогноза. Метод имитационного моделирования.
27. Метод Делфи. Метод морфологического анализа. Метод "дерева целей". Неформальное прогнозирование.
28. Думание за противника. Место прогнозирования в системе деятельности. Прогнозирование индивидуума.
29. Прогнозирование массовых настроений. Прогнозирование событий.
30. Поддержка решений. Системы оперативного прогнозирования.
31. Экспертные системы. Системы поддержки нетипового анализа числовых данных. Системы для контент - анализа.
32. Системы для фильтрования данных. Системы поддержки неформального анализа текстов. Базы данных аналитической разведки.
33. Интернет как средство разведки и влияния. Мониторинг в интернете.
34. Направленный поиск в интернете. Управление поиском в интернете. Управление доступом в интернет.
35. Управление хостингом. Управление дискуссиями на интернет - форумах. Управление электронной почтой. Рассылка электронных сообщений. Индивидуальное использование интернета.
36. Способы повышения эффективности. Личная информационная система. Использование компьютера. Теория влияния. Манипулирование руководителями.
37. Нейтрализация руководителей. Манипулирование массами. Поддержка интеллектуалов. Нейтрализация активистов. Влияние на выборы.
38. Противодействие влиянию на аналитическую разведку. Противодействие влиянию на руководителей. Противодействие влиянию на общество в целом.
39. Методический замысел исследования и его основные этапы. Формулировка гипотезы.

40. Структура и содержание этапов исследовательского процесса. Применение логических законов и правил. Информационная работа. Аналитическая работа.
41. Основные этапы информационно-аналитической работы. Аналогия как метод. От известного к неизвестному. Аналогия. Процентный метод. Аналогия. Характерный пример.
42. Проверка по аналогии. Изучение отдельных случаев как метод информационно-аналитической работы.
43. Планирование работы. Достоинства плана. Начало работы. Способы работы.
44. Запись планов. Ограниченность применения. Поиск информации. Документальные источники информации.
45. Организация справочно-информационной деятельности. Каталоги и картотеки. Библиографические указатели.
46. Последовательность поиска документальных источников информации. Работа с книгой. Техника чтения. Записи при чтении. Методы изучения документальных источников. Источники документации.
47. Техника изучения документов. Классические методы. Контентный анализ. Фиксирование информации.
48. Источники информации. Взятие информации из документов. Принципы оценки и анализа информации.
49. Безопасность информационной работы.
50. Информационная безопасность организации (учреждения).
51. Элементы системы безопасности. Внутренняя безопасность. Локальная информационных объектов. Виды угроз информационным объектам.
52. Методы и средства обеспечения информационной безопасности организации (фирмы).
53. Специальные аналитические технологии для предупреждения и расследования противоправных посягательств на безопасность.

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.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»

Интернет-ресурсы:

1. **http://eup.ru/catalog/all-all.asp – научно-образовательный портал.**
2. **http://informika.ru/ – образовательный портал**
3. **www.wikIsec.ru - Энциклопедия информационной безопасности. – Публикации, статьи.**
4. **www.biblioclub.ru** - Универсальная библиотека онлайн
5. **www.rucont.ru** - ЭБС «Руконт».
6. **http://www.academy.it.ru/ – академия АЙТИ.**
7. **http://www.minfin.ru - Официальный сайт Министерства финансов Российской Федерации**
8. **http://www.gov.ru/ - Официальный сервер органов государственной власти Российской Федерации.**
9. **http://www.fsb.ru/ - Официальный сайт Федеральной Службы Безопасности**
10. **http://www.fstec.ru/ - Официальный сайт Федеральной Службы по Техническому Экспортному Контролю**

8. Перечень информационных технологий

Перечень программного обеспечения: *MSOffice, Multisim.*
Информационные справочные системы:
1. Электронные ресурсы образовательной среды Университета
2. Информационно-справочные системы (Консультант; Гарант).
3. Рабочая программа и методическое обеспечение по курсу: «Организация системы обеспечения информационной безопасности (служба ИБ)».