Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ИРКУТСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Структурное подразделение «Институт информационных технологий и анализа данных»

УТВЕРЖДЕНА:
на заседании Совета института ИТиАД им. Е.И.Попова
Протокол №8 от 24 февраля 2025 г.

Рабочая программа дисциплины

«ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Направление: 10.03.01 Информационная безопасность

Организация и технологии защиты информации (в сфере техники и технологии)

Квалификация: Бакалавр

Форма обучения: очная

Документ подписан простой электронной подписью Составитель программы: Мамедов Эльшан Фахраддинович Дата подписания: 17.06.2025	Документ подписан простой электронной подписью Утвердил: Говорков Алексей Сергеевич Дата подписания: 17.06.2025	Документ подписан простой электронной подписью Согласовал: Сибиряк Юрий Владимирович Дата подписания: 10.06.2025

Год набора – 2025

Иркутск, 2025 г.

1 Перечень планируемых результатов обучения по дисциплине, соотнесённых с планируемыми результатами освоения образовательной программы

1.1 Дисциплина «Организационное и правовое обеспечение информационной безопасности» обеспечивает формирование следующих компетенций с учётом индикаторов их достижения

Код, наименование компетенции	Код индикатора компетенции
ОПК ОС-2.1 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	ОПК ОС-2.1.2
ОПК ОС-2.3 Способен разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности	ОПК ОС-2.3.1
ОПК ОС-5 Способен разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности	ОПК ОС-5.3

1.2 В результате освоения дисциплины у обучающихся должны быть сформированы

Код индикатора	Содержание индикатора	Результат обучения
ОПК ОС-5.3	Знает нормативные правовые акты, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; умеет оценить информационные риски в автоматизированных системах и определять меры, правила, процедуры, методы и средства для защиты информации в области обеспечения защиты государственной тайны и сертификации средств защиты информации, уметь осуществлять планирование и организацию работы персонала	**Знать** Знать меры защиты информации ограниченного доступа; содержание нормативных правовых актов, нормативных и методических документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю **Уметь** Уметь определять меры для организации защиты информации ограниченного доступа и разрабатывать организационно-распорядительные документы, регламентирующие защиту информации ограниченного доступа, в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской

		Федерации, Федеральной службы по техническому и экспортному контролю **Владеть** Владеть навыками применения действующей нормативной базы, нормативных и методических документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю для организации защиты информации ограниченного доступа
ОПК ОС-2.1.2	Способен квалифицированно применять нормативные правовые акты в конкретных сферах профессиональной деятельности, применять нормы стандартов (регуляторов) в области информационной безопасности для определения возможных источников информационных угроз, их вероятных целей и тактики	**Знать** состав и содержание Российских и международных нормативных правовых актов, нормативных и методических документов, межгосударственных и международных стандартов, регламентирующих деятельность по защите информации **Уметь** применять действующую нормативную базу, нормативные правовые акты, нормативные и методические документы для принятия правовых и организационных мер по защите информации; разрабатывать проекты нормативно-правовых актов и организационно-распорядительных документов, регламентирующих деятельность по защите информации. **Владеть** методами поиска, анализа и применения нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации, в сфере профессиональной деятельности
ОПК ОС-2.3.1	Способен применять актуальные методы по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности для обеспечения качественно нового уровня защиты информации на предприятии	**Знать** Знать содержание основных нормативных и методических документов, источники и базы научно- технической литературы, применимые в целях решения задач профессиональной деятельности. **Уметь** Уметь анализировать источники научно-технической литературы с целью дальнейшего применения для решения задач профессиональной деятельности.

		Владеть Владеть навыками осуществления подбора, изучения и обобщения научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности.

2 Место дисциплины в структуре ООП

Изучение дисциплины «Организационное и правовое обеспечение информационной безопасности» базируется на результатах освоения следующих дисциплин/практик: «Информационные технологии», «Основы информационной безопасности», «Аудит информационной безопасности», «Экономика защиты информации»

Дисциплина является предшествующей для дисциплин/практик: «Информационно-психологическая безопасность в современном обществе», «Персональные данные», «Основы управления информационной безопасностью», «Информационно-аналитическая деятельность по обеспечению комплексной безопасности», «Нормативная база, российские и международные стандарты по информационной безопасности»

3 Объем дисциплины

Объем дисциплины составляет – 4 ЗЕТ

Вид учебной работы	**Трудоемкость в академических часах** (Один академический час соответствует 45 минутам астрономического часа)	
	Всего	Семестр № 4
Общая трудоемкость дисциплины	144	144
Аудиторные занятия, в том числе:	64	64
лекции	32	32
лабораторные работы	0	0
практические/семинарские занятия	32	32
Самостоятельная работа (в т.ч. курсовое проектирование)	44	44
Трудоемкость промежуточной аттестации	36	36
Вид промежуточной аттестации (итогового контроля по дисциплине)	Экзамен	Экзамен

4 Структура и содержание дисциплины

4.1 Сводные данные по содержанию дисциплины

Семестр № 4

№ п/п	Наименование раздела и темы дисциплины	Виды контактной работы						СРС		Форма текущего контроля
		Лекции		ЛР		ПЗ(СЕМ)				
		№	Кол. Час.	№	Кол. Час.	№	Кол. Час.	№	Кол. Час.	
1	2	3	4	5	6	7	8	9	10	11

1	Информационные отношения и правовой режим защиты информации ограниченного доступа	1	4			1	2	1	6	Устный опрос
2	Правовая защита различных видов конфиденциальной информации	2	4			2, 3	4	1	6	Устный опрос
3	Защита персональных данных и государственное регулирование деятельности по защите информации	3	6			4	4	1	6	Устный опрос
4	Организационное обеспечение информационной безопасности	4	4			5, 6, 7	6	1	6	Устный опрос
5	Организация охраны, режима и работы с персоналом	5	4			8, 9	8	1	6	Устный опрос
6	Организация защиты информации в различных направлениях деятельности предприятия (организации)	6	4			10, 11	4	1	6	Устный опрос
7	Организация взаимодействия с федеральными органами исполнительной власти в сфере обеспечения информационной безопасности	7	6			12	4	1	8	Устный опрос
	Промежуточная аттестация								36	Экзамен
	Всего		32				32		80	

4.2 **Краткое содержание разделов и тем занятий**

Семестр № 4

№	Тема	Краткое содержание
1	Информационные отношения и правовой режим защиты информации ограниченного доступа	Информационные отношения как объект правового регулирования. Законодательство Российской Федерации в области информационной безопасности. Структура информационной сферы и характеристика ее элементов. Информация как объект

		правоотношений. Категории информации по условиям доступа к ней и распространения. Конституционные гарантии прав граждан в информационной сфере и механизм их реализации. Субъекты и объекты правоотношений в области информационной безопасности. Система нормативных правовых актов, регулирующие обеспечение информационной безопасности в Российской Федерации Понятие и виды информации ограниченного доступа по законодательству РФ. Правовой режим защиты государственной тайны. Система нормативных правовых актов, регламентирующих обеспечение сохранности сведений, составляющих государственную тайну в Российской Федерации. Государственная тайна как особый вид защищаемой информации и ее характерные признаки. Принципы и механизмы отнесения сведений к государственной тайне, их засекречивания и рассекречивания. Правовой режим защиты информации конфиденциального характера. Понятие информации конфиденциального характера по российскому законодательству. Основные виды конфиденциальной информации. Основные требования, предъявляемые к организации защиты конфиденциальной информации.
2	Правовая защита различных видов конфиденциальной информации	Институт правовой защиты служебной тайны. Правовые основы защиты служебной тайны. Нормативно-правовые акты, регулирующие правовую защиту служебной тайны. Защита в режиме служебной тайны сведений, доступ к которым ограничивается в соответствии с законодательством, при обращении и хранении таких сведений (информации) в органах государственной власти и органах местного самоуправления. Институт правовой защиты коммерческой тайны. Правовые основы защиты коммерческой тайны. Объекты и субъекты права на коммерческую тайну. Права и обязанности обладателя коммерческой тайны. Ответственность за нарушение прав на коммерческую тайну. Институт правовой защиты банковской тайны. Институт правовой защиты профессиональной тайны.
3	Защита персональных данных и государственное регулирование деятельности по защите информации	Институт правовой защиты персональных данных. Правовые основы защиты информации персонального характера. ФЗ «О персональных данных», подзаконные нормативно-правовые документы о порядке правовой защиты персональных данных. Государственный надзор и

		контроль обработки персональных данных. Государственное регулирование деятельности в области защиты информации. Понятие лицензирования по российскому законодательству. Виды деятельности, подлежащие лицензированию. Правовая регламентация лицензионной деятельности в области обеспечения информационной безопасности. Объекты лицензирования и участники лицензионных отношений в сфере защиты информации. Органы лицензирования и их полномочия. Организация лицензирования в сфере обеспечения информационной безопасности. Контроль за соблюдением лицензиатами условий ведения деятельности. Правовые основы сертификации в области защиты информации. Правонарушения в информационной сфере и особенности защиты от них. Особенности правонарушений в информационной сфере. Преступления в сфере компьютерной информации: виды, состав. Основы расследования преступлений в сфере компьютерной информации. Правовая защита информационных систем. Правовая защита результатов интеллектуальной деятельности.
4	Организационное обеспечение информационной безопасности	Понятие организационной защиты информации. Сущность организационных методов защиты информации. Соотношение организационных мер защиты информации с мерами правового и технического характера. Основные термины, связанные с организацией защиты информации. Организация режима секретности. Организационные меры, направленные на защиту государственной тайны. Режим секретности как основной порядок деятельности в сфере защиты государственной тайны. Особенности системы организационной защиты государственной тайны. Распределение между уровнями государственного управления полномочий, управленческих функций и задач по защите государственной тайны. Организация деятельности режимно-секретных органов. Установление и изменение степени секретности сведений, отнесенных к государственной тайне. Понятие «рассекречивание сведений». Основания для рассекречивания сведений. Допуск к государственной тайне. Порядок допуска и доступа к государственной тайне. Основные принципы допускной работы. Номенклатура должностей работников, подлежащих оформлению на допуск и порядок ее составления и утверждения. Документальное оформление для отправки на согласование.

		Процедура оформления и переоформления допусков и ее документирование, подлежащее согласованию с органами государственной безопасности. Организация доступа к сведениям, составляющим государственную тайну.
5	Организация охраны, режима и работы с персоналом	Понятие «охрана». Цели и задачи охраны. Объекты охраны. Виды, способы и особенности охраны различных объектов. Понятие о рубежах охраны. Многорубежная система охраны. Факторы выбора методов и средств охраны. Организация режимных мероприятий. Понятие «режим», цели и задачи режимных мероприятий. Виды режима. Организация пропускного режима. Основные положения инструкции об организации пропускного режима и работе бюро пропусков. Виды пропускных документов. Порядок организации работы бюро пропусков. Контрольно-пропускные пункты, их оборудование и организация работы. Понятие «внутриобъектовый режим» и его общие требования. Противопожарный режим и его обеспечение. Работа с персоналом, обладающим конфиденциальной информацией. Подбор и расстановка кадров. Организация обучения персонала. Основные формы обучения и методы контроля знаний. Мотивация персонала к выполнению требований по защите информации. Организация контроля соблюдения персоналом требований режима защиты информации. Методы проверки персонала. Организация служебного расследования по фактам разглашения персоналом конфиденциальной информации. Организационные меры по защите информации при увольнении сотрудника.
6	Организация защиты информации в различных направлениях деятельности предприятия (организации)	Организация подготовки и проведения конфиденциальных переговоров. Основные требования, предъявляемые к подготовке и проведению конфиденциальных переговоров. Основные этапы проведения конфиденциальных переговоров. Подготовка помещения для проведения конфиденциальных переговоров. Организация защиты информации при приеме в организации посетителей, командированных лиц, иностранных представителей. Требования режима защиты информации при приеме в организации посетителей. Организация работы с иностранными представителями. Требования к помещениям, в которых проводится прием иностранных представителей. Обеспечение защиты информации при выезде за рубеж командируемых лиц. Организация работы службы безопасности

		предприятия. Концепция безопасности предприятия (организации) и ее содержание. Политика информационной безопасности. Подразделения, обеспечивающие ИБ предприятия: основные функции, содержание деятельности, структура, обязанности сотрудников. Варианты организационных структур, обеспечивающих защиту информации. Основные документы службы информационной безопасности.
7	Организация взаимодействия с федеральными органами исполнительной власти в сфере обеспечения информационной безопасности	Организационно-правовая структура, цели, функции и задачи Федеральной службы безопасности РФ, Федеральной службы по техническому и экспортному контролю РФ, Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций РФ (Роскомнадзор). Организационно-правовое взаимодействие служб ИБ организаций (предприятий) с ФСБ России, ФСТЭК России и Роскомнадзором. Характеристика ФЗ "О безопасности критической информационной инфраструктуры". Нормативные, методические и руководящие документы ФСБ России и ФСТЭК России в сфере обеспечения информационной безопасности и защиты информации.

4.3 Перечень лабораторных работ

Лабораторных работ не предусмотрено

4.4 Перечень практических занятий

Семестр № 4

№	Темы практических (семинарских) занятий	Кол-во академических часов
1	Информационные отношения как объект правового регулирования	2
2	Правовой режим защиты государственной тайны	2
3	Правовой режим защиты информации конфиденциального характера	2
4	Институт правовой защиты персональных данных	4
5	Государственное регулирование деятельности в области защиты информации	2
6	Преступления в сфере компьютерной информации	2
7	Понятие и сущность организационной защиты информации	2
8	Организация режима секретности	4
9	Допуск к государственной тайне	4

10	Организация служебного расследования по фактам утраты информации	2
11	Организация подготовки и проведения совещаний и заседаний по конфиденциальным вопросам	2
12	Организационно-правовое взаимодействие с регуляторами в сфере информационной безопасности	4

4.5 Самостоятельная работа

Семестр № 4

№	Вид СРС	Кол-во академических часов
1	Подготовка к практическим занятиям	44

В ходе проведения занятий по дисциплине используются следующие интерактивные методы обучения: Дискуссия, Кейс-технология

5 Перечень учебно-методического обеспечения дисциплины

5.1 Методические указания для обучающихся по освоению дисциплины

5.1.1 Методические указания для обучающихся по практическим занятиям

https://el.istu.edu/course/index.php?categoryid=1107

5.1.2 Методические указания для обучающихся по самостоятельной работе:

https://el.istu.edu/course/index.php?categoryid=1107

6 Фонд оценочных средств для контроля текущей успеваемости и проведения промежуточной аттестации по дисциплине

6.1 Оценочные средства для проведения текущего контроля

6.1.1 семестр 4 | Устный опрос

Описание процедуры.

Проведение устного опроса в форме «вопрос-ответ».
Вопросы для контроля:

Тема 3. Защита персональных данных и государственное регулирование деятельности по защите информации
1. Понятие, права и обязанности оператора персональных данных.
2. Полномочия органов власти по контролю и надзору за выполнением требований по защите персональных данных при обработке в ИСПДн.

Критерии оценивания.

Полнота ответа: Раскрытие всех аспектов вопроса, использование ключевых понятий, терминов.
Точность и достоверность: Правильность определений, формул, фактов, дат, имен, ссылок на источники.
Глубина понимания: Демонстрация понимания сути явлений, причинно-следственных связей, умение анализировать, синтезировать, обобщать, а не просто воспроизводить заученное.
Логичность и структурированность: Последовательность изложения, наличие введения, основной части, вывода.
Культура речи: Грамотность, ясность, использование профессиональной терминологии.
Умение аргументировать: Подтверждение своих тезисов примерами, доказательствами, ссылками на теории.
Ответы на дополнительные/уточняющие вопросы: Способность развить тему, применить знания в нестандартной ситуации.

ответ раскрыт полностью – 5 баллов
ответ раскрыт частично – 2-4 баллов
имеет только общее представление о проблеме – 1 балл
не ответил – 0 баллов

6.2 Оценочные средства для проведения промежуточной аттестации

6.2.1 Критерии и средства (методы) оценивания индикаторов достижения компетенции в рамках промежуточной аттестации

Индикатор достижения компетенции	Критерии оценивания	Средства (методы) оценивания промежуточной аттестации
ОПК ОС-5.3	Демонстрирует высокий уровень знаний нормативных правовых актов РФ и стандартов в сфере информационной безопасности киберфизических систем, руководящих и методических документов ФСТЭК России и ФСБ России при применении экспертных систем комплексной оценки безопасности автоматизированных информационных и телекоммуникационных систем	Проверочная работа
ОПК ОС-2.1.2	Демонстрирует высокий уровень знаний о применении нормативных правовых актов в конкретных сферах профессиональной деятельности, стандартов (регуляторов) в области информационной безопасности для определения возможных источников информационных угроз, их вероятных целей и тактики	Проверочная работа
ОПК ОС-2.3.1	Демонстрирует высокий уровень	Проверочная

	знаний о применении актуальных методов по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности для обеспечения качественно нового уровня защиты информации на предприятии	работа

6.2.2 Типовые оценочные средства промежуточной аттестации

6.2.2.1 Семестр 4, Типовые оценочные средства для проведения экзамена по дисциплине

6.2.2.1.1 Описание процедуры

Перечень теоретических вопросов, практических заданий и ситуаций, выносимых на экзамен, доводятся преподавателем до студентов в начале изучения программы. Формулировки вопросов, заданий должны быть четкими, краткими, понятными, исключающими двойное толкование. Могут быть применены тестовые задания или задания комбинированного характера. Количество вариантов для устных заданий должно быть больше чем число студентов, сдающих экзамен не менее, чем на 3. Количество вариантов для письменных заданий должно быть не менее двух.
Теоретические вопросы к экзамену
1. Информационные отношения как объект правового регулирования.
2. Законодательство Российской Федерации в области информационной безопасности. Структура информационной сферы и характеристика ее элементов.
3. Информация как объект правоотношений.
4. Категории информации по условиям доступа к ней и распространения.
5. Конституционные гарантии прав граждан в информационной сфере и механизм их реализации.
6. Субъекты и объекты правоотношений в области информационной безопасности.
7. Система нормативных правовых актов, регулирующих обеспечение информационной безопасности в Российской Федерации.
8. Понятие и виды информации ограниченного доступа по законодательству РФ.
9. Правовой режим защиты государственной тайны.
10. Система нормативных правовых актов, регламентирующих обеспечение сохранности сведений, составляющих государственную тайну в Российской Федерации.
11. Государственная тайна как особый вид защищаемой информации и ее характерные признаки.
12. Принципы и механизмы отнесения сведений к государственной тайне, их засекречивания и рассекречивания.
13. Правовой режим защиты информации конфиденциального характера.
14. Понятие информации конфиденциального характера по российскому законодательству.
15. Основные виды конфиденциальной информации.
16. Основные требования, предъявляемые к организации защиты конфиденциальной информации.
17. Институт правовой защиты служебной тайны.
18. Правовые основы защиты служебной тайны.
19. Нормативно-правовые акты, регулирующие правовую защиту служебной тайны.

20. Защита в режиме служебной тайны сведений, доступ к которым ограничивается в соответствии с законодательством, при обращении и хранении таких сведений (информации) в органах государственной власти и органах местного самоуправления. Институт правовой защиты коммерческой тайны.
21. Правовые основы защиты коммерческой тайны.
22. Объекты и субъекты права на коммерческую тайну.
23. Права и обязанности обладателя коммерческой тайны.
24. Ответственность за нарушение прав на коммерческую тайну.
25. Институт правовой защиты банковской тайны.
26. Институт правовой защиты профессиональной тайны.
27. Институт правовой защиты персональных данных.
28. Правовые основы защиты информации персонального характера.
29. ФЗ «О персональных данных», подзаконные нормативно-правовые документы о порядке правовой защиты персональных данных.
30. Государственный надзор и контроль обработки персональных данных.
31. Государственное регулирование деятельности в области защиты информации.
32. Правовые основы сертификации в области защиты информации.
33. Правонарушения в информационной сфере и особенности защиты от них.
34. Особенности правонарушений в информационной сфере.
35. Преступления в сфере компьютерной информации: виды, состав.
36. Основы расследования преступлений в сфере компьютерной информации.
37. Правовая защита информационных систем.
38. Понятие организационной защиты информации.
39. Сущность организационных методов защиты информации.
40. Соотношение организационных мер защиты информации с мерами правового и технического характера.
41. Основные термины, связанные с организацией защиты информации.
42. Организация режима секретности.
43. Организационные меры, направленные на защиту государственной тайны.
44. Режим секретности как основной порядок деятельности в сфере защиты государственной тайны.
45. Особенности системы организационной защиты государственной тайны.
46. Допуск к государственной тайне. Порядок допуска и доступа к государственной тайне.
47. Работа с персоналом, обладающим конфиденциальной информацией.
48. Организация контроля соблюдения персоналом требований режима защиты информации. Методы проверки персонала.
49. Подразделения, обеспечивающие ИБ предприятия: основные функции, содержание деятельности, структура, обязанности сотрудников.
50. Варианты организационных структур, обеспечивающих защиту информации.
51. Основные документы службы информационной безопасности.
52. Организационно-правовая структура, цели, функции и задачи Федеральной службы безопасности РФ.
53. Организационно-правовая структура, цели, функции и задачи Федеральной службы по техническому и экспортному контролю РФ.
54. Организационно-правовая структура, цели, функции и задачи Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций РФ (Роскомнадзора).
55. Организационно-правовое взаимодействие служб ИБ организаций (предприятий) с ФСБ России, ФСТЭК России и Роскомнадзором.
56. Правовое регулирование деятельности Федеральной службы безопасности РФ.

57. Правовое регулирование деятельности Федеральной службы по техническому и экспортному контролю РФ.
58. Правовое регулирование деятельности Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций РФ (Роскомнадзора).
59. Характеристика ФЗ «О безопасности критической информационной инфраструктуры».
60. Нормативные, методические и руководящие документы ФСБ России и ФСТЭК России в сфере обеспечения информационной безопасности и защиты информации.

Пример задания:

1 Организация контроля соблюдения персоналом требований режима защиты информации.
2 Подразделения, обеспечивающие ИБ предприятия: основные функции, содержание деятельности, структура, обязанности сотрудников.
3 Характеристика ФЗ «О безопасности критической информационной инфраструктуры».

6.2.2.1.2 Критерии оценивания

Отлично	**Хорошо**	**Удовлетворительно**	**Неудовлетворительно**
ответ правильный, логически выстроен, использована профессиональная терминология. Обучающийся правильно интерпретирует полученный результат.	ответ в целом правильный, логически выстроен, использована профессиональная терминология. Обучающийся в целом правильно интерпретирует полученный результат.	ответ в основном правильный, логически выстроен, использована профессиональная терминология.	ответы на теоретическую часть неправильные или неполные.

7 **Основная учебная литература**

1. Осавелюк Е. А. Информационная безопасность государства и общества в контексте деятельности СМИ : монография / Е. А. Осавелюк, 2023. - 92.

2. Прохорова О. В. Информационная безопасность и защита информации / О. В. Прохорова, 2023. - 124.

3. Усов Е. Г. Защита информации : электронный курс / Е. Г. Усов, 2023

4. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / ред.: Т. А. Полякова, А. А. Стрельцов, 2022. - 325.

5. Организационное и правовое обеспечение информационной безопасности : учебник для бакалавриата и магистратуры / Т. А. Полякова [и др.]; ред.: Т. А. Полякова, А. А. Стрельцов, 2024. - 357.

8 Дополнительная учебная литература и справочная

1. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для бакалавриата и магистратуры вузов по юридическим направлениям и специальностям / Т. А. Полякова [и др.]; под ред. Т. А. Поляковой и А. А. Стрельцова, 2016. - 324.

9 Ресурсы сети Интернет

1. http://library.istu.edu/
2. https://e.lanbook.com/

10 Профессиональные базы данных

1. http://new.fips.ru/
2. http://www1.fips.ru/

11 Перечень информационных технологий, лицензионных и свободно распространяемых специализированных программных средств, информационных справочных систем

1. Microsoft DreamSpark Premium Electronic Software Delivery_2018

2. Microsoft Office 2007 Standard - 2003 Suites и 2007 Suites - поставка 2010

12 Материально-техническое обеспечение дисциплины

1. Проектор мультимедиа BenQ MW621ST(с экраном 3*3 м)

2. Экран ScreenMedia GoldView 274*206 настенный