МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ЮРИДИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ О.Е. КУТАФИНА (МГЮА)»

Оренбургский институт (филиал)

Кафедра социальных и гуманитарных наук

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

КИБЕРБЕЗОПАСНОСТЬ И ПРАВОВОЕ РЕГУЛИРОВАНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Б1.В.17

год набора – 2026

Код и наименование специальности:	40.05.01 Правовое обеспечение национальной безопасности
Уровень высшего образования:	специалитет
Специализация ОПОП ВО:	Государственно-правовая
Формы обучения:	очная, заочная
Квалификация:	юрист

Оренбург – 2026

Программа утверждена на заседании кафедры социальных и гуманитарных наук протокол № 7 от «25» марта 2026 года.

Авторы:
Черняев С.В. – кандидат технических наук, доцент кафедры социальных и гуманитарных наук Оренбургского института (филиала) Университета имени О.Е. Кутафина (МГЮА);
Габдуллина О.Г. – кандидат технических наук, социальных и гуманитарных наук Оренбургского института (филиала) Университета имени О.Е. Кутафина (МГЮА);

Рецензенты:
Кулантаева И.А. – кандидат педагогических наук, доцент кафедры математических методов и моделей в экономике Оренбургского государственного университета;
Солодкая М.С. – доктор философских наук, профессор социальных и гуманитарных наук Оренбургского института (филиала) Университета имени О.Е. Кутафина (МГЮА).

Габдуллина О.Г., Черняев С.В.
Кибербезопасность и правовое регулирование информационной безопасности: рабочая программа дисциплины (модуля) / О.Г. Габдуллина, С.В. Черняев — Оренбург: Оренбургский институт (филиал) Университета имени О.Е. Кутафина (МГЮА), 2026.

Программа составлена в соответствии с требованиями ФГОС ВО.

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Цели и задачи освоения дисциплины (модуля)

Дисциплина (модуль) «Кибербезопасность и правовое регулирование информационной безопасности» имеет **целью** формирование и развитие у обучающихся компетенций, обеспечивающих профессиональную деятельность применительно к общественным отношениям в сфере кибербезопасности и информационной безопасности личности, общества и государства. Так данная дисциплина направлена на формирование у обучающихся практических навыков по использования информационных систем в области защиты информации в киберсреде.

Основные **задачи** дисциплины «Кибербезопасность и правовое регулирование информационной безопасности»:

- дать представление об основных правовых актах в области защиты государственной тайны и информационной безопасности при работе с различными источниками информации, информационными ресурсами и технологиями в сфере профессиональной деятельности;
- дать представление об основных технических методах обеспечения информационной безопасности в киберпространстве;
- дать представление об основах криптографической защиты информации;
- дать представление о технологии формирования электронной цифровой подписи как средства защиты информации;
- дать представление о способах и средствах защиты информации в телекоммуникационных системах;
- дать представление о способах и средствах защиты информационных процессов в компьютерных системах.
- сформировать практические навыки в применении средств защиты информации и криминалистического анализа информации в киберпространстве.

1.2. Место дисциплины (модуля) в структуре ОПОП ВО

Дисциплина (модуль) «Кибербезопасность и правовое регулирование информационной безопасности» входит в Блок 1 «Дисциплины (модули)» части, формируемой участниками образовательных отношений ОПОП ВО.

Дисциплина (модуль «Кибербезопасность и правовое регулирование информационной безопасности» базируется на учебной дисциплине «Информатика и информационные технологии в профессиональной деятельности» базовой части Б1.О ОПОП ВО.

Перед началом изучения дисциплины «Кибербезопасность и правовое регулирование информационной безопасности» обучающийся должен:

- знать: основные понятия и принципы функционирования информационных систем и технологий; нормативную базу в области создания и распространения информационных ресурсов;

- уметь: использовать информационные ресурсы в правоприменительной деятельности;

- владеть: навыками использования компьютерной техники и основных информационных технологий, необходимых в правовой работе.

Освоение дисциплины (модуля) «Кибербезопасность и правовое регулирование информационной безопасности» даёт необходимые знания для изучения других дисциплин программы специалитета: «Криминалистическое обеспечение национальной безопасности»: «Противодействие экстремистской деятельности», а также обеспечивает информационную поддержку дисциплин, предусмотренных программой специалитета.

1.3. Формируемые компетенции и индикаторы их достижения (планируемые результаты освоения дисциплины (модуля))

По итогам изучения учебной дисциплины (модуля) «Кибербезопасность и правовое регулирование информационной безопасности» обучающийся должен обладать следующими профессиональными компетенциями в соответствии с ФГОС ВО:

ПК-2. Способен квалифицировано применять правовые нормы и принимать правоприменительные акты в сфере обеспечения законности и правопорядка, безопасности личности, общества и государства;

ПК-3. Способен осуществлять правоохранительную деятельность, в том числе функции и полномочия по обеспечению безопасности, законности и правопорядка, по защите прав и свобод человека и гражданина.

Разделы (темы) дисциплины (модуля)	Код и наименование формируемых компетенций	Индикатор достижения компетенций (планируемый результат освоения дисциплины (модуля))
Раздел 1. Государственная политика обеспечения информационной безопасности Российской Федерации: 1.Развитие законодательства в области защиты информации. 2.Основные вызовы в Стратегии развития информационного общества до 2030 года.	**ПК-2.** Способен квалифицировано применять правовые нормы и принимать правоприменительные акты в сфере обеспечения законности и правопорядка, безопасности личности, общества и государства	**ИПК 2.1** Знает содержание нормативных правовых актов, регулирующих обеспечение законности и правопорядка, безопасности личности, общества и государства **ИПК 2.2** Знает функции и полномочия органов государственной власти, обеспечивающих законность и правопорядок, безопасность личности, общества и государства **ИПК 2.3** Понимает механизм реализации норм права,

3.Трансформация поля угроз в киберпространстве.		регламентирующих вопросы обеспечения законности и правопорядка, безопасности личности, общества и государства **ИПК 2.4** Осуществляет поиск, обобщение, анализ информации, имеющей значение для реализации правовых норм в сфере обеспечения законности и правопорядка, безопасности личности, общества и государства **ИПК 2.5** Владеет навыками принятия правоприменительных актов в сфере обеспечения законности и правопорядка, безопасности личности, общества и государства
Раздел 2. Правовое обеспечение информационной безопасности. Информация ограниченного доступа и её правовой режим: 1.Система информационного законодательства в области защиты информации. 2.Персональные данные как социальная и правовая категория. 3.Классификация видов тайн в современном российском законодательстве.	**ПК-2.** Способен квалифицировано применять правовые нормы и принимать правоприменительные акты в сфере обеспечения законности и правопорядка, безопасности личности, общества и государства	**ИПК 2.1** Знает содержание нормативных правовых актов, регулирующих обеспечение законности и правопорядка, безопасности личности, общества и государства **ИПК 2.2** Знает функции и полномочия органов государственной власти, обеспечивающих законность и правопорядок, безопасность личности, общества и государства **ИПК 2.3** Понимает механизм реализации норм права, регламентирующих вопросы обеспечения законности и правопорядка, безопасности личности, общества и государства **ИПК 2.4** Осуществляет поиск, обобщение, анализ информации, имеющей значение для реализации правовых норм в сфере обеспечения законности и правопорядка, безопасности личности, общества и государства **ИПК 2.5** Владеет навыками принятия правоприменительных актов в сфере обеспечения законности и правопорядка, безопасности личности, общества и государства
Раздел 3. Организационное обеспечение информационной	**ПК-2.** Способен квалифицировано применять правовые нормы и принимать	**ИПК 2.1** Знает содержание нормативных правовых актов, регулирующих обеспечение законности и правопорядка,

безопасности: 1.Организационные меры защиты информации. 2. Международные и российские стандарты в области защиты информации. 3.Полномочия ФСТЭК, ФСБ, Роскомнадзора в области защиты информации	правоприменительные акты в сфере обеспечения законности и правопорядка, безопасности личности, общества и государства	безопасности личности, общества и государства **ИПК 2.2** Знает функции и полномочия органов государственной власти, обеспечивающих законность и правопорядок, безопасность личности, общества и государства **ИПК 2.3** Понимает механизм реализации норм права, регламентирующих вопросы обеспечения законности и правопорядка, безопасности личности, общества и государства **ИПК 2.4** Осуществляет поиск, обобщение, анализ информации, имеющей значение для реализации правовых норм в сфере обеспечения законности и правопорядка, безопасности личности, общества и государства **ИПК 2.5** Владеет навыками принятия правоприменительных актов в сфере обеспечения законности и правопорядка, безопасности личности, общества и государства
Раздел 4. **Технические методы обеспечения информационной безопасности:** 1. Реализация комплексного подхода к защите информации 2.Технологии физической защиты информации. 3. Современные российские технологии формирования доверенной среды в информационных системах. 4. Защита от утечек по акустическому каналу связи	**ПК-2.** Способен квалифицировано применять правовые нормы и принимать правоприменительные акты в сфере обеспечения законности и правопорядка, безопасности личности, общества и государства	**ИПК 2.1** Знает содержание нормативных правовых актов, регулирующих обеспечение законности и правопорядка, безопасности личности, общества и государства **ИПК 2.2** Знает функции и полномочия органов государственной власти, обеспечивающих законность и правопорядок, безопасность личности, общества и государства **ИПК 2.3** Понимает механизм реализации норм права, регламентирующих вопросы обеспечения законности и правопорядка, безопасности личности, общества и государства **ИПК 2.4** Осуществляет поиск, обобщение, анализ информации, имеющей значение для реализации правовых норм в сфере обеспечения законности и правопорядка, безопасности личности, общества и государства

		ИПК 2.5 Владеет навыками принятия правоприменительных актов в сфере обеспечения законности и правопорядка, безопасности личности, общества и государства
Раздел 5. Методы шифрования данных для обеспечения информационной безопасности: 1.Ассиметричное шифрование. 2. Вычисление хеш-функций. 3. Инфраструктура открытых ключей. Сертификаты ключей X.509 4. Правовые и технические особенности реализации ЭЦП и функционирования удостоверяющих центров 5. Атаки на систему электронной цифровой подписи	**ПК-3.** Способен обеспечивать законность и правопорядок, безопасность личности, общества и государства	**ИПК 3.1** Понимает механизм обеспечения законности и правопорядка, безопасности личности, общества и государства **ИПК 3.2** Знает содержание деятельности органов государственной власти, обеспечивающих законность и правопорядок, безопасность личности, общества и государства **ИПК 3.3** Умеет выявлять угрозы нарушения законности и правопорядка, безопасности личности, общества и государства **ИПК 3.4** Умеет выявлять нарушения законности и правопорядка, безопасности личности, общества и государства, причины и условия, способствующие их совершению **ИПК 3.5** Умеет применять нормы права, регулирующие полномочия органов государственной власти, обеспечивающих законность и правопорядок, безопасность личности, общества и государства **ИПК 3.6** Определяет меры, принятие которых необходимо для своевременного и полного устранения выявленных нарушений законности и правопорядка, безопасности личности, общества и государства
Раздел 6. Криптографическая защита информации: 1.История развития криптографии. 2. Классификация систем шифрования/ 3. Атаки на криптографические алгоритмы 4.Программное обеспечение «True Crypt»	**ПК-3.** Способен обеспечивать законность и правопорядок, безопасность личности, общества и государства	**ИПК 3.1** Понимает механизм обеспечения законности и правопорядка, безопасности личности, общества и государства **ИПК 3.2** Знает содержание деятельности органов государственной власти, обеспечивающих законность и правопорядок, безопасность личности, общества и государства **ИПК 3.3** Умеет выявлять угрозы нарушения законности и правопорядка, безопасности личности, общества и государства

		ИПК 3.4 Умеет выявлять нарушения законности и правопорядка, безопасности личности, общества и государства, причины и условия, способствующие их совершению **ИПК 3.5** Умеет применять нормы права, регулирующие полномочия органов государственной власти, обеспечивающих законность и правопорядок, безопасность личности, общества и государства **ИПК 3.6** Определяет меры, принятие которых необходимо для своевременного и полного устранения выявленных нарушений законности и правопорядка, безопасности личности, общества и государства
Раздел 7. Защита информации в телекоммуникационных системах: 1.Классификация угроз безопасности 2.Хакеры: социальное определение и анализ мотиваций преступного поведения. 3.Особенности построения защиты информации в телекоммуникационных сетях.	**ПК-3.** Способен обеспечивать законность и правопорядок, безопасность личности, общества и государства	**ИПК 3.1** Понимает механизм обеспечения законности и правопорядка, безопасности личности, общества и государства **ИПК 3.2** Знает содержание деятельности органов государственной власти, обеспечивающих законность и правопорядок, безопасность личности, общества и государства **ИПК 3.3** Умеет выявлять угрозы нарушения законности и правопорядка, безопасности личности, общества и государства **ИПК 3.4** Умеет выявлять нарушения законности и правопорядка, безопасности личности, общества и государства, причины и условия, способствующие их совершению **ИПК 3.5** Умеет применять нормы права, регулирующие полномочия органов государственной власти, обеспечивающих законность и правопорядок, безопасность личности, общества и государства **ИПК 3.6** Определяет меры, принятие которых необходимо для своевременного и полного устранения выявленных нарушений законности и правопорядка, безопасности личности, общества и государства
Раздел 8. Защита информационных	**ПК-3.** Способен обеспечивать	**ИПК 3.1** Понимает механизм обеспечения законности и

процессов в компьютерных системах. Криминалистический анализ информации: 1.Классификация способов защиты информации в компьютерных системах от случайных и преднамеренных угроз. 2.Система разграничения доступа к информации. Процедуры идентификации и аутентификации субъектов доступа в компьютерных системах.	законность и правопорядок, безопасность личности, общества и государства	правопорядка, безопасности личности, общества и государства **ИПК 3.2** Знает содержание деятельности органов государственной власти, обеспечивающих законность и правопорядок, безопасность личности, общества и государства **ИПК 3.3** Умеет выявлять угрозы нарушения законности и правопорядка, безопасности личности, общества и государства **ИПК 3.4** Умеет выявлять нарушения законности и правопорядка, безопасности личности, общества и государства, причины и условия, способствующие их совершению **ИПК 3.5** Умеет применять нормы права, регулирующие полномочия органов государственной власти, обеспечивающих законность и правопорядок, безопасность личности, общества и государства **ИПК 3.6** Определяет меры, принятие которых необходимо для своевременного и полного устранения выявленных нарушений законности и правопорядка, безопасности личности, общества и государства

II. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Объем дисциплины (модуля) «Кибербезопасность и правовое регулирование информационной безопасности» составляет 2 з.е., 72 академических часа. Форма промежуточной аттестации – зачет.

2.1. Тематические планы дисциплины

2.1.1. Тематический план для очной формы обучения

№ п/п	Разделы (темы) дисциплины (модуля)	Семестр	Виды учебной деятельности и объём (в академических часах)			Технология образовательного процесса	Форма текущего контроля/ Форма промежуточной аттестации
			Л	**ПЗ**	**СР**		

1	**Раздел 1. Государственная политика обеспечения информационной безопасности Российской Федерации:** 1.Развитие законодательства в области защиты информации. 2.Основные вызовы в Стратегии развития информационного общества до 2030 года. 3.Трансформация поля угроз в киберпространстве.	6	2	2	4	Лекция-презентация, управляемая дискуссия,	Интерактивный опрос, доклады
2	**Раздел 2. Правовое обеспечение информационной безопасности. Информация ограниченного доступа и её правовой режим:** 1.Система информационного законодательства в области защиты информации. 2.Персональные данные как социальная и правовая категория. 3.Классификация видов тайн в современном российском законодательстве.	6	2	6	4	Лекция-презентация, управляемая дискуссия,	Интерактивный опрос, презентации
3	**Раздел 3. Организационное обеспечение информационной безопасности:** 1.Организационные меры защиты информации.	6	2	2	4	Лекция-презентация, работа со специализированными Интернет-ресурсами.	Компьютерное тестирование

	2. Международные и российские стандарты в области защиты информации. 3.Полномочия ФСТЭК, ФСБ, Роскомнадзора в области защиты информации						
4	**Раздел 4. Технические методы обеспечения информационной безопасности:** 1. Реализация комплексного подхода к защите информации 2.Технологии физической защиты информации. 3. Современные российские технологии формирования доверенной среды в информационных системах. 4. Защита от утечек по акустическому каналу связи	6	2	2	4	Лекция-презентация, управляемая дискуссия, работа со специализированными Интернет-ресурсами	Компьютерное тестирование
5	**Раздел 5. Методы шифрования данных для обеспечения информационной безопасности:** 1.Ассиметричное шифрование. 2. Вычисление хеш-функций. 3. Инфраструктура открытых ключей. Сертификаты ключей X.509 4. Правовые и технические особенности реализации ЭЦП и функционирования	6	2	4	2	Лекция-презентация, работа со специализированными Интернет-ресурсами. Использование бесплатных версий программного обеспечения по формированию ЭЦП (система PGP)	Выполнение индивидуальных модельных заданий «Пробный обмен информацией с применением средств формирования ЭЦП»

	удостоверяющих центров 5. Атаки на систему электронной цифровой подписи						
6	**Раздел 6. Криптографическая защита информации:** 1.История развития криптографии. 2. Классификация систем шифрования/ 3. Атаки на криптографические алгоритмы 4.Программное обеспечение «True Crypt»	6	2	4	2	Лекция-презентация	Работа с специализированным криптографическим программным обеспечением
7	**Раздел 7. Защита информации в телекоммуникационных системах:** 1.Классификация угроз безопасности 2.Хакеры: социальное определение и анализ мотиваций преступного поведения. 3.Особенности построения защиты информации в телекоммуникационных сетях.	6	2	4	2	Лекция-презентация, работа со специализированными Интернет-ресурсами по внедрению VPN и IDS систем	Выполнение индивидуальных модельных заданий «Защита коммерческого предложения по поставке VPN (IDS)»
8	**Раздел 8. Защита информационных процессов в компьютерных системах. Криминалистический анализ информации:** **1.Классификация** способов защиты информации в	6	2	4	2	Решение модельных заданий по системам защиты информации на компьютеризированном рабочем месте	Выполнение индивидуальных модельных заданий «Защита результатов выполнения практического задания»

	компьютерных системах от случайных и преднамеренных угроз. 2.Система разграничения доступа к информации. Процедуры идентификации и аутентификации субъектов доступа в компьютерных системах.						
	ВСЕГО		**16**	**32**	**24**	**Зачёт**	

2.1.2. Тематический план для заочной формы обучения

№ п/п	Разделы (темы) дисциплины (модуля)	Семестр	Виды учебной деятельности и объём (в академических часах)			Технология образовательного процесса	Форма текущего контроля/ Форма промежуточной аттестации
			Л	**ПЗ**	**СР**		
1	**Раздел 1. Государственная политика обеспечения информационной безопасности Российской Федерации:** 1.Развитие законодательства в области защиты информации. 2.Основные вызовы в Стратегии развития информационного общества до 2030 года. 3.Трансформация поля угроз в киберпространстве.	5	1	2	8	Лекция-презентация, управляемая дискуссия,	Интерактивный опрос, доклады
2	**Раздел 2. Правовое обеспечение информационной безопасности. Информация ограниченного доступа и её правовой**	5	1	2	8	Лекция-презентация, управляемая дискуссия,	Интерактивный опрос, презентации

	режим: 1.Система информационного законодательства в области защиты информации. 2.Персональные данные как социальная и правовая категория. 3.Классификация видов тайн в современном российском законодательстве.						
	Раздел 3. Организационное обеспечение информационной безопасности: 1.Организационные меры защиты информации. 2. Международные и российские стандарты в области защиты информации. 3.Полномочия ФСТЭК, ФСБ, Роскомнадзора в области защиты информации	5	-	-	9	Работа со специализированными Интернет-ресурсами	Компьютерное тестирование
3	**Раздел 4. Технические методы обеспечения информационной безопасности:** 1. Реализация комплексного подхода к защите информации 2.Технологии физической защиты информации. 3. Современные российские технологии формирования доверенной среды в информационных системах. 4. Защита от утечек по акустическому каналу связи	5	1	-	9	Работа со специализированными Интернет-ресурсами	Компьютерное тестирование

5	**Раздел 5. Методы шифрования данных для обеспечения информационной безопасности:** 1.Ассиметричное шифрование. 2. Вычисление хеш-функций. 3. Инфраструктура открытых ключей. Сертификаты ключей X.509 4. Правовые и технические особенности реализации ЭЦП и функционирования удостоверяющих центров 5. Атаки на систему электронной цифровой подписи	5	-	-	5	Работа со специализированными Интернет-ресурсами. Использование бесплатных версий программного обеспечения по формированию ЭЦП (система PGP)	Выполнение индивидуальных модельных заданий «Пробный обмен информацией с применением средств формирования ЭЦП»
6	**Раздел 6. Криптографическая защита информации:** 1.История развития криптографии. 2. Классификация систем шифрования/ 3. Атаки на криптографические алгоритмы 4.Программное обеспечение «True Crypt»	5	1	-	5	Работа со специализированными Интернет-ресурсами по криитографии	Работа с специализированным криптографическим программным обеспечением
7	**Раздел 7. Защита информации в телекоммуникационных системах:** 1.Классификация угроз безопасности 2.Хакеры: социальное определение и анализ мотиваций преступного поведения. 3.Особенности построения защиты информации в телекоммуникационных сетях.	5	1	2	5	Работа со специализированными Интернет-ресурсами по внедрению VPN и IDS систем	Выполнение индивидуальных модельных заданий «Защита коммерческого предложения по поставке VPN (IDS)»

8	**Раздел 8. Защита информационных процессов в компьютерных системах. Криминалистический анализ информации: 1.Классификация** способов защиты информации в компьютерных системах от случайных и преднамеренных угроз. 2.Система разграничения доступа к информации. Процедуры идентификации и аутентификации субъектов доступа в компьютерных системах.	5	1	2	5	Решение модельных заданий по системам защиты инфор-мации на компьютери-зированном рабочем месте	Выполнение индивидуальных модельных заданий «Защита результатов выполнения практического задания»
	ВСЕГО		**6**	**8**	**54**	**Зачёт (4)**	

2.2. Занятия лекционного типа

Лекция 1. *Организационное обеспечение информационной безопасности*

Содержание:

1. Служебная и профессиональная тайна.
2. Тайна частной жизни и персональные данные.
3. Коммерческая и банковская тайна.
4. Организационное обеспечение безопасности Российской Федерации.
5. Уполномоченные федеральные органы в области защиты информации и пределы их полномочий.

Задания для подготовки:

1. В чем отличие персональных данных от личной информации?
2. Подготовьте перечень персональных данных чаще всего распространяемых в сети Интернет.
3. Подготовить список полномочий ФСЭК России в области защиты информации.

Лекция 2 *Технические методы обеспечения информационной безопасности*

Содержание:

1. Реализация комплексного подхода к защите информации
2. Технологии физической защиты информации.
3. Современные российские технологии формирования доверенной среды в информационных системах.
4. Защита от утечек по акустическому каналу связи.

Задания для подготовки:

1. В чем отличие персональных данных от личной информации?
2. Подготовьте перечень персональных данных чаще всего распространяемых в сети Интернет.
3. Подготовить список полномочий ФСЭК России в области защиты информации.

Лекция 3. *Методы шифрования данных для обеспечения информационной безопасности*

Содержание:

1. Ассиметричное шифрование.
2. Вычисление хеш-функций.
3. Инфраструктура открытых ключей. Сертификаты ключей X.509.
4. Правовые и технические особенности реализации ЭЦП и функционирования удостоверяющих центров.
5. Атаки на систему электронной цифровой подписи.

Задания для подготовки:

1. Что понимают под ассиметричным шифрованием? Какова обобщенная схема шифрования с открытым ключом?
2. Как осуществляется одностороннее криптографическое преобразование (вычисление хеш-функций)?
3. В чем состоит алгоритм «RSA»?
4. Как создается и верифицируется ЭЦП?
5. Каков российский стандарт ЭЦП на основе ГОСТ Р 34.10-2012?
6. Что представляет собой инфраструктура открытых ключей?
7. Каковы сертификаты ключей X.509?
8. Каковы правовые и технические особенности реализации ЭЦП и функционирования удостоверяющих центров в РФ?
9. Каковы основные атаки на систему электронной цифровой подписи?

Лекция 4. *Криптографическая защита информации*

Содержание:

1. История развития криптографии.
2. Классификация систем шифрования.
3. Атаки на криптографические алгоритмы.

4. Программное обеспечение «True Crypt».

Задания для подготовки:

1. Какие вы знаете виды классификаций систем шифрования?
2. В чем суть атаки на криптографические алгоритмы?
3. В чем преимущества программы «True Crypt»*?*

Лекция 5. *Защита информации в телекоммуникационных системах*

Содержание:
1. Классификация угроз безопасности.
2. Хакеры: социальное определение и анализ мотиваций преступного поведения.
3. Особенности построения защиты информации в телекоммуникационных сетях.

Задания для подготовки:

1. Нарисуйте схему иллюстрирующую принцип работы файерволла.
2. Используя графические возможности редактора «MS Word» представьте схематически совокупность основных защит операционной системы.
3. Используя графические возможности редактора «MS Word» представьте схематически принцип работы «песочницы».
4. Используя графические возможности редактора «MS Word» представьте схематически аппаратно-программный файрволл.

Лекция 6. *Защита информационных процессов в компьютерных системах. Криминалистический анализ информации*

Содержание:
1. Классификация способов защиты информации в компьютерных системах от случайных и преднамеренных угроз.
2. Система разграничения доступа к информации.
3. Процедуры идентификации и аутентификации субъектов доступа в компьютерных системах.

Задания для подготовки:
1. Какие способы защиты информации в компьютерных системах от случайных и преднамеренных угроз вы знаете
2. Перечислите виды доступа к информации
3. В чем суть процедуры идентификации и аутентификации субъектов доступа в компьютерных системах?

2.3. Занятия семинарского типа

Практическое занятие 1. *Государственная политика обеспечения информационной безопасности Российской Федерации*

1. Развитие законодательства в области защиты информации.
2. Сравнительный анализ положений Доктрин информационной безопасности 2000 года и 2016 года. Защита традиционных духовно-нравственных ценностей.
3. Информационное оружие.
4. Основные вызовы в Стратегии развития информационного общества до 2030 года.
5. Трансформация поля угроз в киберпространстве.

Задания для подготовки:

Студентам рекомендуется подготовить презентацию по одной из следующих тем:

1. Этапы развития российского законодательства в сфере защиты информации.
2. Сравнительный анализ положений Доктрин информационной безопасности 2000 года и 2016 года.
3. Основные виды информационного оружия.
4. Основные вызовы в Стратегии развития информационного общества до 2030 года.
5. Трансформация поля угроз в киберпространстве.

Практические занятия 2, 3, 4. *Правовое обеспечение информационной безопасности. Информация ограниченного доступа и её правовой режим*

1. Структура информационной сферы. Основные составляющие национальных интересов России (интересы личности, общества и государства) в информационной сфере.
2. Виды угроз информационной безопасности Российской Федерации.
3. Источники угроз информационной безопасности..
4. Направления обеспечения информационной безопасности государства.
5. Система информационного законодательства в области защиты информации.
6. Институт государственной тайны.
7. Понятие коммерческой и служебной тайны.
8. Персональные данные как социальная и правовая категория.
9. Международные и российские стандарты в области защиты информации.

10. Политика безопасности в органах власти и организациях.
11. Система органов исполнительной власти и их полномочия в области защиты информации.
12. Полномочия ФСТЭК, ФСБ, Роскомнадзора в области защиты информации.

Задания для подготовки:

Студентам рекомендуется подготовить презентацию по одной из следующих тем:

1. Основные составляющие национальных интересов России (интересы личности, общества и государства) в информационной сфере.
2. Виды угроз информационной безопасности Российской Федерации.
3. Основные источники угроз информационной безопасности России.
4. Направления обеспечения информационной безопасности государства.
5. Система российского информационного законодательства в области защиты информации.
6. Особенности института государственной тайны в Российской Федерации.
7. Общее и особенное коммерческой и служебной тайны в Российской Федерации.
8. Особенности персональных данных как социальной и правовой категории в Российской Федерации.
9. Общее и различное в международных и российских стандартах в сфере защиты информации.
13. Полномочия ФСТЭК, ФСБ, Роскомнадзора в области защиты информации.

Практическое занятие 5, 6. *Методы шифрования данных для обеспечения информационной безопасности*

Содержание:

1. Ассиметричное шифрование.
2. Вычисление хеш-функций.
3. Инфраструктура открытых ключей. Сертификаты ключей X.509.
4. Правовые и технические особенности реализации ЭЦП и функционирования удостоверяющих центров.
5. Атаки на систему электронной цифровой подписи.

Задания для подготовки:

Студентам рекомендуется подготовить презентацию по одной из следующих тем

1. Обобщенная схема шифрования с открытым ключом.
2. Одностороннее криптографическое преобразование (вычисление хеш-функций).
3. Алгоритм «RSA».

4. Инфраструктура открытых ключей.
5. Сертификаты ключей X.509.

Практическое занятие 7, 8. *Технические методы обеспечения информационной безопасности*

1. Комплексный (системный) подход и классификация основных методов защиты информации.
2. Основные способы защиты информации.
3. Понятие технических угроз и их классификация.
4. Методы нарушения конфиденциальности, целостности и доступности информации
5. Понятие информационного оружия.
6. Технологии формирования доверенной среды в информационных системах.
7. Защита от утечек по акустическому каналу.

Задания для подготовки:

1. Распознать технические угрозы в конкретном случае информационного обмена.
2. Сформировать доверенную среду в информационной системе.
3. Организовать защиту от утечек по акустическому каналу в конкретной ситуации информационного обмена.

Практическое занятие 9, 10. *Электронная подпись. Технология формирования ЭЦП (4 часа).*

1. Ассиметричное шифрование. Обобщенная схема шифрования с открытым ключом.
2. Одностороннее криптографическое преобразование (вычисление хеш-функций).
3. Описание алгоритма «RSA».
4. Создание и верификация ЭЦП. Российский стандарт ЭЦП на основе ГОСТ Р 34.10-2012.
5. Инфраструктура открытых ключей. Сертификаты ключей X.509.
6. Правовые и технические особенности реализации ЭЦП и функционирования удостоверяющих центров.
7. Атаки на систему электронной цифровой подписи.

Задания для подготовки:

Студентам рекомендуется подготовить презентацию по одной из следующих тем:

1. Российский стандарт ЭЦП на основе ГОСТ Р 34.10-2012.

2. Правовые и технические особенности реализации ЭЦП и функционирования удостоверяющих центров в Российской Федерации.
3. Атаки на систему электронной цифровой подписи.

Практическое занятие 11, 12. *Основы криптографической защиты информации*

1. История развития криптографии.
2. Классификация систем шифрования.
3. Потоковые шифры.
4. Блочное шифрование.
5. Методы замены и перестановки.
6. Стандарты «DES» и «AES».
7. Отечественные алгоритмы симметричного шифрования на основе ГОСТ 28147-89.
8. Проблемы криптоанализа.
9. Криптостойкость алгоритмов шифрования.

Задания для подготовки:

Студентам рекомендуется подготовить презентацию по одной из следующих тем:

1. Этапы развития криптографии.
2. Классификация систем шифрования.
3. Особенности стандартов «DES» и «AES».
4. Особенности отечественных алгоритмов симметричного шифрования на основе ГОСТ 28147-89.

Практическое занятие 13, 14. *Защита информации в телекоммуникационных системах*

1. Угрозы безопасности современных информационно-вычислительных и телекоммуникационных сетей.
2. Классификация угроз безопасности. Методы и средства воздействия на безопасность сетей.
3. Хакеры: социальное определение и анализ мотиваций преступного поведения.
4. Сравнительный анализ методов информационного воздействия и противодействия в сети «Интернет».
5. Направления по защите от враждебных воздействий на безопасность сетей.
6. Особенности построения защиты информации в телекоммуникационных сетях.

7. Современные технические и программные средства сетевой защиты компьютерной информации.
8. Межсетевые экраны: классификация и особенности использования. Виды и основные функции систем обнаружения вторжений.
9. Система анализа информационной безопасности, построенная на понятии, определении и управлении рисками.

Задания для подготовки:

Студентам рекомендуется подготовить презентацию по одной из следующих тем:

1. Классификация угроз безопасности современных информационно-вычислительных и телекоммуникационных сетей.
2. Методы и средства воздействия на безопасность современных информационно-вычислительных и телекоммуникационных сетей.
3. Сравнительный анализ методов информационного воздействия и противодействия в сети «Интернет».
4. Направления по защите от враждебных воздействий на безопасность сетей.
5. Современные технические и программные средства сетевой защиты компьютерной информации.
6. Межсетевые экраны: классификация и особенности использования. Виды и основные функции систем обнаружения вторжений.

Практическое занятие 15, 16. *Защита информационных процессов в компьютерных системах*

1. Основные определения и положения защиты информации в компьютерных системах.
2. Случайные и преднамеренные угрозы безопасности информации в компьютерных системах.
3. Понятие и классификация видов и методов несанкционированного доступа.
4. Определение и модель злоумышленника. Классификация способов защиты информации в компьютерных системах от случайных и преднамеренных угроз.
5. Защита информации от несанкционированного доступа. Система разграничения доступа к информации.
6. Процедуры идентификации и аутентификации субъектов доступа в компьютерных системах.
7. Управление доступом на уровне файлов.
8. Контроль целостности программных средств и информации. Защита процесса загрузки операционной системы. Создание функционально замкнутой среды пользователя.

9. Методы и средства защиты данных от несанкционированного доступа. Система защиты от исследования и копирования информации (данных).
10. Вредоносные программы: определение и классификация.

Задания для подготовки:

Студентам рекомендуется подготовить презентацию по одной из следующих тем:

1. «Случайные и преднамеренные угрозы безопасности информации в компьютерных системах».
2. «Классификация видов и методов несанкционированного доступа».
3. «Классификация способов защиты информации в компьютерных системах от случайных и преднамеренных угроз».
4. «Методы и средства защиты данных от несанкционированного доступа».
5. «Система защиты от исследования и копирования информации (данных)».
6. «Вредоносные программы: определение и классификация».

2.3. Самостоятельная работа

Самостоятельная работа студента по дисциплине (модулю) «Кибербезопасность и правовое регулирование информационной безопасности» включает следующие **виды**:

- аудиторная работа (работа студентов над заданиями под руководством преподавателя на занятиях);
- внеаудиторная работа (работа студентов вне занятий по заданию преподавателя).

Самостоятельная работа студента по дисциплине «Кибербезопасность и правовое регулирование информационной безопасности» включает следующие **формы**:

- чтение и конспектирование учебной и монографической литературы;
- подготовка презентации по отдельным вопросам практического занятия;
- работа со специализированными порталами в сети «Интернет»;
- освоение на практике пробных и бесплатных версий специализированных программных продуктов;
- подготовка к тестированию.

Модель (особенности) самостоятельной работы студентов по отдельным разделам и темам дисциплины (модуля) очной формы обучения

№ раздела	Тема раздела	Темы презентаций	На что нужно обратить особое внимание

1	2	3	4
1.	Раздел 1. Государственная политика обеспечения информационной безопасности Российской Федерации	1.Развитие законодательства в области защиты информации. 2.Сравнительный анализ положений Доктрин информационной безопасности 2000 года и 2016 года. 3.Информационное оружие – миф или реальность? 4.Основные вызовы в Стратегии развития информационного общества до 2030 года. 5. Трансформация поля угроз в киберпространстве.	1. Какие этапы развития информационного законодательства можно выделить? С чем это связано? 2. Изменилось ли понимание спектра угроз в доктринальных определениях? 3. Какие угрозы наиболее существенны в сфере защиты прав личности? 4. Приведите классификацию типов информационного оружия. Есть ли примеры реальной подготовки и применения средств информационного оружия? 5. Какие направления доминируют в в Стратегии развития информационного общества до 2030 года ? 6. Что понимается под киберпространством? Какие вызовы в сфере безопасности сетевых технологий актуальны в настоящее время?
2.	Раздел 2. Правовое обеспечение информационной безопасности. Информация ограниченного доступа и её правовой режим	1.Система информационного законодательства в области защиты информации. 2.Персональные данные как социальная и правовая категория. 3.Классификация видов тайн в современном российском законодательстве. 4.Организационные меры защиты информации. 5. Международные и российские стандарты в области защиты информации. 6.Полномочия ФСТЭК, ФСБ, Роскомнадзора в области защиты информации	1. На каких уровнях осуществляется нормативное регулирование в области защиты информации? В чем заключаются правомочия реализуемые на каждом из уровней? 2. В чем выражаются особенности правового статуса персональных данных? Что из себя представляет «специальная категория» персональных данных? 3. В каких нормативных актах разграничиваются полномочия органов исполнительной власти в области защиты информации?
3.	Раздел 3. Организационное обеспечение информационной безопасности	1. Реализация комплексного подхода к защите информации 2.Технологии физической защиты информации. 3. Современные российские технологии формирования доверенной среды в информационных системах. 4. Защита от утечек по	1. Какие современные и перспективные технологии могут быть использованы в области физической защиты информации? 2. Что понимается под комплексным подходом к защите информации? 3. Какие программные и

		акустическому каналу.	технические средства предназначены для формирования доверенной среды защиты информации? 4. Что представляет собой акустический канал распространения информации? Какие технические средства предназначены для обеспечения защиты по акустическому каналу ?
4.	Раздел 4. Технические методы обеспечения информационной безопасности	1.История развития криптографии. 2. Классификация систем шифрования/ 3. Атаки на криптографические алгоритмы 4. Программное обеспечение «True Crypt»	1. Какие криптографические средства использовались в докомпьютерную эпоху? 2. Какие современные системы шифрования вы знаете? 3. Что представляет собой наука криптоаналитика? 4. Программное обеспечение «True Crypt» назначение и основные возможности.
5.	Раздел 5. Методы шифрования данных для обеспечения информационной безопасности	1.Ассиметричное шифрование. 2. Вычисление хеш-функций. 3. Инфраструктура открытых ключей. Сертификаты ключей X.509 4. Правовые и технические особенности реализации ЭЦП и функционирования удостоверяющих центров 5. Атаки на систему электронной цифровой подписи	1.Какие используются криптографические хеш-функции? 2. Что такое цифровая подпись? 3.Что такое инфраструктура открытых ключей? 4.Какие российские и международные стандарты на формирование цифровой подписи существуют? 5.Какие основные криптографические протоколы используются в сетях? 6. Что такое криптографическая хеш-функция?
6.	Раздел 6. Криптографическая защита информации	1. Классификация угроз безопасности 2. Хакеры: социальное определение и анализ мотиваций преступного поведения. 3. Особенности построения защиты информации в телекоммуникационных сетях.	1. Каковы основные угрозы компьютерной безопасности при работе в сети Интернет? 2. В чем заключается криминологическая характеристика деятельности хакеров? 3. Приведите уголовно-правовую характеристику преступлений в сети Интернет.
7.	Раздел 7. Защита информации в телекоммуника	1. Классификация способов защиты информации в компьютерных системах от случайных и преднамеренных	1. Какие виды компьютерных угроз существуют? 2. Что такое брандмауэр? 3. Что такое антивирусная

	ционных системах	угроз.	программа? 4. Что такое эвристический алгоритм поиска вирусов? 5. Что такое сигнатурный поиск вирусов?
	Раздел 8. Защита информационных процессов в компьютерных системах. Криминалистический анализ информации	1. Система разграничения доступа к информации. 2. Процедуры идентификации и аутентификации субъектов доступа в компьютерных системах.	1. Методы противодействия сниффингу? 2. Какие программные реализации программно-аппаратных средств защиты информации вы знаете? 3. Что такое механизм контроля и разграничения доступа? 4.Какую роль несет журналирование действий в программно-аппаратных средствах защиты информации? 5.Что такое средства стеганографической защиты информации?

Модель (особенности) самостоятельной работы студентов по отдельным разделам и темам дисциплины (модуля) заочной формы обучения

Самостоятельная работа студентов заочной формы обучения строится с учётом значительного сокращения аудиторных занятий по сравнению с очной формой обучения. Следует также учитывать особенность распределения занятий по семестрам. Потому основной вид учебной работы состоит в самостоятельном освоении тем, предусмотренных программой дисциплины. Для формирования умений и навыков в использовании программных средств студентам заочной формы обучения необходимо самостоятельно выполнить практические задания, предложенные кафедрой.

№ раздела	Тема раздела	Темы презентаций	На что нужно обратить особое внимание
1	2	3	4
1.	Раздел 1. Государственная политика обеспечения информационной безопасности Российской Федерации	1.Развитие законодательства в области защиты информации. 2.Сравнительный анализ положений Доктрин информационной безопасности 2000 года и 2016 года. 3.Информационное оружие – миф или реальность? 4.Основные вызовы в	1. Какие этапы развития информационного законодательства можно выделить? С чем это связано? 2. Изменилось ли понимание спектра угроз в доктринальных определениях? 3. Какие угрозы наиболее существенны в сфере защиты прав личности?

		Стратегии развития информационного общества до 2030 года. 5. Трансформация поля угроз в киберпространстве.	4. Приведите классификацию типов информационного оружия. Есть ли примеры реальной подготовки и применения средств информационного оружия? 5. Какие направления доминируют в в Стратегии развития информационного общества до 2030 года ? 6. Что понимается под киберпространством? Какие вызовы в сфере безопасности сетевых технологий актуальны в настоящее время?
2.	Раздел 2. Правовое обеспечение информационной безопасности. Информация ограниченного доступа и её правовой режим	1.Система информационного законодательства в области защиты информации. 2.Персональные данные как социальная и правовая категория. 3.Классификация видов тайн в современном российском законодательстве. 4.Организационные меры защиты информации. 5. Международные и российские стандарты в области защиты информации. 6.Полномочия ФСТЭК, ФСБ, Роскомнадзора в области защиты информации	1. На каких уровнях осуществляется нормативное регулирование в области защиты информации? В чем заключаются правомочия реализуемые на каждом из уровней? 2. В чем выражаются особенности правового статуса персональных данных? Что из себя представляет «специальная категория» персональных данных? 3. В каких нормативных актах разграничиваются полномочия органов исполнительной власти в области защиты информации?
3.	Раздел 3. Организационное обеспечение информационной безопасности	1. Реализация комплексного подхода к защите информации 2.Технологии физической защиты информации. 3. Современные российские технологии формирования доверенной среды в информационных системах. 4. Защита от утечек по акустическому каналу.	1. Какие современные и перспективные технологии могут быть использованы в области физической защиты информации? 2. Что понимается под комплексным подходом к защите информации? 3. Какие программные и технические средства предназначены для формирования доверенной среды защиты информации? 4. Что представляет собой акустический канал распространения информации? Какие технические средства предназначены для обеспечения защиты по акустическому каналу ?

4.	Раздел 4. Технические методы обеспечения информационной безопасности	1.История развития криптографии. 2. Классификация систем шифрования/ 3. Атаки на криптографические алгоритмы 4. Программное обеспечение «True Crypt»	1. Какие криптографические средства использовались в докомпьютерную эпоху? 2. Какие современные системы шифрования вы знаете? 3. Что представляет собой наука криптоаналитика? 4. Программное обеспечение «True Crypt» назначение и основные возможности.
5.	Раздел 5. Методы шифрования данных для обеспечения информационной безопасности	1.Ассиметричное шифрование. 2. Вычисление хеш-функций. 3. Инфраструктура открытых ключей. Сертификаты ключей X.509 4. Правовые и технические особенности реализации ЭЦП и функционирования удостоверяющих центров 5. Атаки на систему электронной цифровой подписи	1.Какие используются криптографические хеш-функции? 2. Что такое цифровая подпись? 3.Что такое инфраструктура открытых ключей? 4.Какие российские и международные стандарты на формирование цифровой подписи существуют? 5.Какие основные криптографические протоколы используются в сетях? 6. Что такое криптографическая хеш-функция?
6.	Раздел 6. Криптографическая защита информации	1. Классификация угроз безопасности 2. Хакеры: социальное определение и анализ мотиваций преступного поведения. 3. Особенности построения защиты информации в телекоммуникационных сетях.	1. Каковы основные угрозы компьютерной безопасности при работе в сети Интернет? 2. В чем заключается криминологическая характеристика деятельности хакеров? 3. Приведите уголовно-правовую характеристику преступлений в сети Интернет.
7.	Раздел 7. Защита информации в телекоммуникационных системах	1. Классификация способов защиты информации в компьютерных системах от случайных и преднамеренных угроз.	1. Какие виды компьютерных угроз существуют? 2. Что такое брандмауэр? 3. Что такое антивирусная программа? 4. Что такое эвристический алгоритм поиска вирусов? 5. Что такое сигнатурный поиск вирусов?
	Раздел 8. Защита информационных процессов в	1. Система разграничения доступа к информации. 2. Процедуры идентификации и аутентификации субъектов	1. Методы противодействия сниффингу? 2. Какие программные реализации программно-

	компьютерных системах. Криминалистический анализ информации	доступа в компьютерных системах.	аппаратных средств защиты информации вы знаете? 3. Что такое механизм контроля и разграничения доступа? 4.Какую роль несет журналирование действий в программно-аппаратных средствах защиты информации? 5.Что такое средства стеганографической защиты информации?

III. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

3.1. Контрольные вопросы и модельные задания для проведения текущего контроля по дисциплине (модулю)

1. Дайте определение понятия «информационная безопасность».
2. Перечислите интересы личности, общества и государства в информационной сфере.
3. Сформулировать основные положения государственной политики обеспечения информационной безопасности Российской Федерации.
4. Дайте характеристику первоочередных мероприятий по реализации государственной политики обеспечения информационной безопасности Российской Федерации.
5. Используя справочные правовые системы и ресурсы интернет выполнить анализ положений «Стратегии национальной безопасности Российской Федерации до 2020 года» в части касающийся вопросов обеспечения информационной безопасности.
6. Составить перечень Федеральных законов в сфере обеспечения информационной безопасности, представленных на сайте Федеральной службы по техническому и экспортному контролю.
7. Перечислите основные виды угроз информационной безопасности.
8. Выполните анализ источников угроз информационной безопасности Российской Федерации по материалам различных нормативных документов.
9. Дайте характеристику основных методов обеспечения информационной безопасности.
10. Объясните, как соотносятся понятия «безопасность информации» и «защита информации».
11. Перечислите основные руководящие документы ФСТЭК России в сфере защиты информации.
12. Дайте характеристику методов защиты информации в государственных информационных системах.

13. Используя справочные правовые системы и ресурсы интернет подготовить перечень и краткую характеристику основных методов обеспечения информационной безопасности РФ.
14. Изучить содержание правовых, организационно-технических и экономических методов защиты информации.
15. Используя справочные правовые системы составить подборку национальных стандартов в области защиты информации.
16. По материалам руководящих документы ФСТЭК России подготовить обзор и выполнить анализ мер защиты информации в государственных информационных системах.
17. В чем состоит комплексный (системный) подход к защите информации?
18. Какова классификация основных методов защиты информации?
19. Каковы основные способы защиты информации?
20. Что понимают под техническими угрозами? Какова классификация технических угроз?
21. Каковы основные методы нарушения конфиденциальности, целостности и доступности информации?
22. Что понимают под «информационным оружием»?
23. Каковы технологии формирования доверенной среды в информационных системах?
24. Каковы основные средства защиты от утечек по акустическому каналу?
25. Распознать технические угрозы в конкретном случае информационного обмена.
26. Сформировать доверенную среду в информационной системе.
27. Организовать защиту от утечек по акустическому каналу в конкретной ситуации информационного обмена.
28. Какие задачи решает современная криптография?
29. Сформулируйте требования к криптографическим системам защиты информации.
30. Дайте определения понятиям: алфавит, криптограмма, криптографическая система, криптографический протокол, символ, шифр, электронная подпись.
31. В чем заключается правило шифрования методом Цезаря?
32. Почему невозможно вскрыть криптограмму, содержащую код для кодового замка?
33. Что такое криптографическая атака?
34. Какие типы криптографических атак существуют?
35. Назовите основные группы методов шифрования с закрытым ключом.
36. Приведите примеры шифров перестановки.
37. Сформулируйте общие принципы для методов шифрования подстановкой.
38. Что понимают под ассиметричным шифрованием? Какова обобщенная схема шифрования с открытым ключом?

39. Как осуществляется одностороннее криптографическое преобразование (вычисление хеш-функций)?
40. В чем состоит алгоритм «RSA»?
41. Как создается и верифицируется ЭЦП?
42. Каков российский стандарт ЭЦП на основе ГОСТ Р 34.10-2012?
43. Что представляет собой инфраструктура открытых ключей?
44. Каковы сертификаты ключей X.509?
45. Каковы правовые и технические особенности реализации ЭЦП и функционирования удостоверяющих центров в РФ?
46. Каковы основные атаки на систему электронной цифровой подписи?
47. С помощью справочных правовых систем найти федеральные законы «Об электронной цифровой подписи» и «Об электронной подписи».
48. Определить, какому виду электронной подписи соответствует электронная цифровая подпись?
49. В каких правоотношениях может использоваться простая электронная подпись, усиленная неквалифицированная электронная подпись, усиленная квалифицированная электронная подпись, электронная цифровая подпись?
50. Найти в сети Интернет сайты удостоверяющих центров электронной подписи.
51. Нарисуйте схему иллюстрирующую принцип работы файерволла.
52. Используя графические возможности редактора «MS Word» представьте схематически совокупность основных защит операционной системы.
53. Используя графические возможности редактора «MS Word» представьте схематически принцип работы «песочницы».
54. Используя графические возможности редактора «MS Word» представьте схематически аппаратно-программный файрволл.

3.2. Примерные задания для письменного или компьютерного тестирования

1. Задачами государственной информационной политики являются
а) совершенствование правовой системы;
б) формирование единого информационного пространства России;
в) обеспечение информационной безопасности личности, общества и государства;
г) вхождение России в мировое информационное пространство

2. Информационная безопасность - это
а) состояние защищенности информации, циркулирующей в обществе;
б) состояние правовой защищенности информационных ресурсов, информационных продуктов, информационных услуг;

в) состояние защищенности информационных ресурсов, обеспечивающее их формирование, использование и развитие в интересах граждан, организаций, государства;
г) состояние защищенности национальных интересов Российской Федерации в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства

3. Расставьте следующие понятия в порядке от частного к общему:
а) безопасность информации;
б) информационная безопасность;
в) защищенность информации

4. Совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности изложены в
а) Конституции РФ;
б) Гражданском Кодексе РФ;
в) Доктрине информационной безопасности РФ
г) Федеральном законе «Об информации, информационных технологиях и о защите информации»

5. Защита информации представляет собой принятие следующих мер:
а) правовых;
б) технических;
в) экономических;
г) организационных

6. Защита информации направлена на:
а) обеспечение мирового господства России в информационной сфере;
б) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
в) соблюдение конфиденциальности информации ограниченного доступа;
г) реализацию права на доступ к информации

7. Впишите пропущенное слово
… тайна – это защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

8. Система защиты государственной тайны включает:

а) совокупность органов защиты государственной тайны;
б) средства и методы защиты сведений, составляющих государственную тайну, и их носителей;
в) сведения, составляющие государственную тайну;
г) мероприятий, проводимых в целях защиты сведений, составляющих государственную тайну.

9. Средства защиты сведений, составляющих государственную тайну, включают:
а) программно-технические средства;
б) криптографические средства;
в) экономические средства;
г) средства контроля эффективности защиты информации;
д) организационно-правовые средства.

10. Сведения, которые не могут составлять государственную тайну:
а) о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан;
б) о фактах нарушения прав и свобод человека и гражданина;
в) о разработке, технологии, производстве, об объемах производства, о хранении, об утилизации ядерных боеприпасов;
г) о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности;
д) о привилегиях, компенсациях и социальных гарантиях, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям.

3.3. Контрольные вопросы и модельные задания для проведения промежуточной аттестации по итогам освоения дисциплины (модуля)

ВОПРОСЫ К ЗАЧЕТУ

1. Основные этапы формирования и реализации государственной политики в информационной сфере.
2. Стратегия развития информационного общества.
3. Понятие «информационной безопасности».
4. Место информационной безопасности в системе национальной безопасности РФ. Стратегия национальной безопасности РФ.
5. Доктрина информационной безопасности РФ.
6. Основные положения государственной политики обеспечения информационной безопасности Российской.
7. Характеристика информационного законодательства.

8. Основные положения федерального закона «Об информации, информационных технологиях и о защите информации», касающиеся вопросов информационной безопасности.
9. Государственная программа РФ «Информационное общество (2011–2020 годы)».
10. Виды и источники угроз информационной безопасности Российской Федерации.
11. Методы обеспечения информационной безопасности Российской Федерации: классификация и общая характеристика.
12. Основные функции системы обеспечения информационной безопасности Российской Федерации.
13. Структура организационной основы системы обеспечения информационной безопасности Российской Федерации
14. Защита информации. Место защиты информации в информационной безопасности.
15. Системный подход к защите информации. Правовые, организационно-технические и экономические методы защиты информации.
16. Стандартизация и сертификация в сфере информационной безопасности: российский и зарубежный опыт.
17. Система национальных стандартов в сфере защиты информации.
18. Руководящие документы ФСТЭК России в сфере защиты информации.
19. Понятие электронного обмена данными и электронного документооборота.
20. Понятие электронного документа и его особенности.
21. Понятие электронной подписи.
22. Виды электронной подписи: простая, усиленная неквалифицированная, усиленная квалифицированная.
23. Аппаратные и программные средства электронной подписи.
24. Удостоверяющие центры.
25. Требования к удостоверяющим центрам.
26. Аккредитация удостоверяющих центров.
27. Предмет и задачи криптографии. Основные определения.
28. Требования к криптографическим системам защиты информации.
29. Криптографические атаки.
30. Простейшие методы шифрования с закрытым ключом. Методы замены.
31. Понятие «хеш-функции» и её назначение.
32. Методы шифрования с открытым ключом.
33. Цифровая подпись на основе алгоритмов с открытым ключом.
34. Требования к алгоритмам шифрования с открытым ключом.
35. Классификация угроз информационной безопасности в вычислительных сетях.
36. Использование антивирусных программ.
37. Обеспечение безопасности в сети Интернет.
38. Межсетевые экраны: понятие и принципы использования.

3.4. Темы докладов с презентацией для самостоятельной работы студентов

По предложенным ниже темам можно подготовить доклады с презентацией. Длительность доклада 5 минут. Редактор для создания презентации – PowerPoint. Количество слайдов не более 15.

1. Развитие законодательства в области защиты информации.
2. Сравнительный анализ положений Доктрин информационной безопасности 2000 года и 2016 года.
3. Информационное оружие – миф или реальность?
4. Основные вызовы в Стратегии развития информационного общества до 2030 года.
5. Трансформация поля угроз в киберпространстве.
6. Система информационного законодательства в области защиты информации.
7. Персональные данные как социальная и правовая категория.
8. Классификация видов тайн в современном российском законодательстве.
9. Организационные меры защиты информации.
10. Международные и российские стандарты в области защиты информации.
11. Полномочия ФСТЭК, ФСБ, Роскомнадзора в области защиты информации
12. Реализация комплексного подхода к защите информации
13. Технологии физической защиты информации.
14. Современные российские технологии формирования доверенной среды в информационных системах.
15. Защита от утечек по акустическому каналу.
16. История развития криптографии.
17. Классификация систем шифрования.
18. Атаки на криптографические алгоритмы.
19. Программное обеспечение «True Crypt».
20. Ассиметричное шифрование.
21. Вычисление хеш-функций.
22. Инфраструктура открытых ключей. Сертификаты ключей X.509
23. Правовые и технические особенности реализации ЭЦП и функционирования удостоверяющих центров
24. Атаки на систему электронной цифровой подписи
25. Классификация угроз безопасности
26. Хакеры: социальное определение и анализ мотиваций преступного поведения.

27. Особенности построения защиты информации в телекоммуникационных сетях.
28. Классификация способов защиты информации в компьютерных системах от случайных и преднамеренных угроз.
29. Система разграничения доступа к информации.
30. Процедуры идентификации и аутентификации субъектов доступа в компьютерных системах.

IV. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

4.1. Основная литература

1. Организационное и правовое обеспечение информационной безопасности : учебник для вузов / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 357 с. — (Высшее образование). — ISBN 978-5-534-19108-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/583236
2. Суворова, Г. М. Информационная безопасность : учебник для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/588515.
3. Внуков, А. А. Основы информационной безопасности: защита информации / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/587458
4. Правовая информатика : учебник и практикум для вузов / С. Г. Чубукова, Т. М. Беляева, А. Т. Кудинов, Н. В. Пальянова ; под редакцией С. Г. Чубуковой. — 4-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 338 с. — (Высшее образование). — ISBN 978-5-534-19012-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/590549.

4.2. Дополнительная литература

1. Василенко, И. А. Геополитика современного мира : учебник / Василенко, И. А. - М. : Юрайт, 2015. - 421 с.
2. Панасенко С.П. Алгоритмы шифрования. Специальный справочник. – СПб.: БХВ-Петербург, 2009. – 576 с.: ил.

3. Баранова Е.К. Моделирование системы защиты информации. Практикум: учеб. пособие для студентов вузов / Е. К. Баранова, А. В. Бабаш. - М. : РИОР : ИНФРА-М, 2015. - 120 с. - (Высшее образование : Бакалавриат)
4. Платонов В.В. Программно-аппаратные средства защиты информации: учебник для студентов вузов, обуч. по направл. подгот. "Информ. безопасность" / В. В. Платонов. - 2-е изд., стер. - М. : Академия, 2014. - 336 с.
5. Защита информации: учеб. пособие для студентов вузов (бакалавриат и магистратура) / А. П. Жук, Е. П. Жук, О. М. Лепешкин, А. И. Тимошкин. - М. : РИОР : ИНФРА-М, 2013. - 392 с. - (Высшее образование : Бакалавриат; Магистратура).
6. Расторгуев С. П. Основы информационной безопасности: учеб. пособие. М.: Академия, 2009. – 187 с.
7. Технические средства и методы защиты информации: Учебник для вузов / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.; под ред. А.П. Зайцева и А.А. Шелупанова. – М.: ООО «Издательство Машиностроение», 2009 – 508 с.
8. Практическая криптография: алгоритмы и их программирование / А. В. Аграновский, Р.А. Хади – М.: СОЛОН-Пресс, 2009. - 256 с.
9. Мао В. Современная криптография: теория и практика. :Пер. с англ. – М.: Издательский дом "Вильямс", 2005. –768 с.
10. Ховард М., Лебланк Д., Виега Д. 19 смертных грехов, угрожающих безопасности программ. – М.: Издательский Дом ДМК-пресс, 2006. – 288 с.: ил.
11. Смит Р.Э. Аутентификация: от паролей до открытых ключей.: Пер. с англ. – М.: Издательский дом "Вильямс", 2002. –432 с.: ил.
12. Касперски К. Компьютерные вирусы изнутри и снаружи. – СПб.: Питер, 2006. – 527 с.: ил.
13. Низамутдинов М.Ф. Тактика защиты и нападения на Web-приложения. – СПб.: БХВ-Петербург, 2005. – 432 с.: ил.
14. Алферов А.П., Зубов А.Ю, Кузьмин А.С., Черемушкин А.В. Основы криптографии: Учебное пособие, 2-е изд., испр. и доп. – М.:Гелиос АРВ, 2002. – 380 с.: ил.
15. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие для студентов образоват. учреждений сред. проф. образования, обуч. по спец. "Информатика и вычислит. техника" / В. Ф. Шаньгин. - М. : ФОРУМ : ИНФРА-М, 2016. - 416 с.
16. Васильков А.В. Информационные системы и их безопасность: учеб. пособие [для студентов образоват. учреждений сред. проф. образования] / А. В. Васильков, А. А. Васильков, И. А. Васильков. - М. : ФОРУМ, 2015. - 528 с. : ил. - (Профессиональное образование).

4.3. Нормативные акты и судебная практика

1. Конституция Российской Федерации.
2. "Доктрина информационной безопасности Российской Федерации" (утв. Указом Президента РФ от 5.12.2016 г. № 646).
3. «Стратегия развития информационного общества в Российской Федерации на 2017 - 2030 годы» (утв. Указом Президента 09.05.2017 № 203).
4. Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации".
5. "Кодекс Российской Федерации об административных правонарушениях" от 30.12.2001 № 195-ФЗ
6. "Уголовный кодекс Российской Федерации" от 13.06.1996 № 63-ФЗ
7. Глава 14. «Защита персональных данных работника» Трудового кодекса Российской Федерации" от 30.12.2001 № 197-ФЗ.
8. "Гражданский кодекс Российской Федерации (часть четвертая «Интеллектуальная собственность»)" от 18.12.2006 № 230-ФЗ.
9. Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных".
10. Федеральный закон от 27.12.2002 №184-ФЗ "О техническом регулировании".
11. Федеральный закон от 29.07.2004 № 98-ФЗ "О коммерческой тайне".
12. Федеральный закон от 28.12.2010 № 390-ФЗ "О безопасности".
13. Закон РФ от 21.07.1993 № 5485-1 "О государственной тайне".
14. Федеральный закон от 06.04.2011 № 63-ФЗ "Об электронной подписи".
15. Указ Президента РФ от 21.05.2012 № 636 (ред. от 03.04.2017) "О структуре федеральных органов исполнительной власти".
16. Указ Президента РФ от 09.11.2022 №809 (ред. от 04.03.2026) «Об утверждении Основ государственной политики по сохранению и укреплению традиционных российских духовно-нравственных ценностей».

4.4. Стандарты

1. ГОСТ Р 50922—2006. Защита информации. Основные термины и определения.
2. ГОСТ Р 53114—2008. За щита информации. Обеспечение информационной безопасности в организации. Основные термины и определения.
3. ГОСТ 27.002—89. Надежность в технике. Основные понятия. Термины и определения.

4.5. Периодические издания

1. Журнал «Специальная техника» (ВАК). Сайт журнала - http://ess.ru/index.htm;
2. Журнал «Спецтехника и связь» (ВАК). Сайт журнала - http://www.st-s.su/index.htm;
3. Журнал «Защита информации. Инсайд»; Сайт журнала - http://www.inside-zi.ru/
4. Журнал «Безопасность информационных технологий». Сайт журнала - сайт журнала http://www.pvti.ru/articles 14.htm.
5. Информационный бюллетень “Jet Info”. Издатель: компания «Инфосистемы Джет». Сайт журнала - www.ietinfo.ru.
6. Бюро научно-технической информации «Техника для спецслужб». - http://www.bnti.ru/about.asp.
7. Журнал «Information Security/Информационная безопасность». Издатель: компания «Гротек». - http://www.itsec.ru

V. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

5.1 Материально-техническое и учебно-методическое обеспечение программы специалитета

ОПОП ВО обеспечена помещениями, которые представляют собой учебные аудитории для проведения учебных занятий, предусмотренных программой специалитета, оснащенные оборудованием и техническими средствами обучения, а также материально-техническими средствами, необходимыми для осуществления специальной профессиональной подготовки обучающихся, состав которых определяется в рабочих программах дисциплин (модулей).

Помещения для самостоятельной работы обучающихся располагаются по адресу: Оренбург, ул. Комсомольская, 50. Они оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в ЭИОС Университета и включают в себя:

1. Электронный читальный зал:

кресло для индивидуальной работы – 3 шт,

компьютер в сборе: системный блок корпус черный Standart-ATX накопитель SATA III, жесткий диск 1 ТБ, мышь USB, клавиатура USB, монитор LG 21"LED - 8 шт. (компьютерная техника подключена к сети «Интернет» и обеспечивает доступ в электронную информационно-образовательную среду)

2.Аудитория для самостоятельной работы (№518) на 15 посадочных мест:

стол преподавателя -1 шт.,

стул преподавателя -1 шт.,

парты ученические -15 шт.,

стул ученический -15 шт.,

доска магнитная -1 шт.,

стационарный информационно-демонстрационный стенд-1 шт.,

компьютер в сборе: системный блок корпус черный Standart-ATX накопитель SATA III, жесткий диск 1 ТБ, мышь USB, клавиатура USB, монитор LG 21"LED - 8 шт. (компьютерная техника подключена к сети «Интернет» и обеспечивает доступ в электронную информационно-образовательную среду).

ОПОП ВО обеспечена необходимым для реализации перечнем материально-технического обеспечения, который включает в себя:

5.1.1. Фотолаборатория (лаборатория цифровой фотографии). Она предназначена для осуществления информационного и учебно-методического обеспечения образовательного процесса ОПОП ВО по специальности 40.05.01 Правовое обеспечение национальной безопасности и направлена на формирование практических навыков и умений обучающихся. Фотолаборатория (лаборатория цифровой фотографии) расположена по адресу: Оренбург, ул. Комсомольская, 50, ауд. 610а. Фотолаборатория (лаборатория цифровой фотографии) является одним из элементов материально-технической базы, обеспечивающей проведение отдельных видов практической подготовки обучающихся по дисциплине (модулю) «Криминалистическое обеспечение национальной безопасности». Задачами деятельности фотолаборатории являются:

овладение обучающимися знаниями об основных теоретических и методологических положениях криминалистической фотографии и видеозаписи; системе современных методов и приёмов фотографии и видеозаписи; процедуры фото- и видеосъёмки в ходе проведения следственных действий; формирования и использования криминалистических учетов; использования возможностей современных технических средств фото- и видеофиксации в процессе расследования преступлений, гражданском и арбитражном процессе, производстве по делам об административных правонарушениях.

формирование у обучающихся навыков и умений работы с фото-, видеоаппаратурой и иным оборудованием для криминалистической фотографии и видеозаписи при выявлении и фиксации следов на месте происшествия, осмотре предметов, документов и иных объектов, проведении опознавательной съемки в ходе подготовки опознания живых лиц, трупов, предметов; фиксации хода и результатов иных следственных действий.

В фотолаборатории имеются: съемочная аппаратура, аксессуары, проекционное оборудование, оборудование для обработки и печати фотоизображения, расходные материалы. Более подробная информация о фотолаборатории содержится в соответствующем паспорте.

5.1.2. Центр (класс) деловых игр. Центр (класс) деловых игр предназначен для осуществления информационного и учебно-методического обеспечения образовательного процесса программы специалитета по

специальности 40.05.01 Правовое обеспечение национальной безопасности и направлен на формирование практических навыков и умений обучающихся. Центр (класс) деловых игр расположен по адресу: Оренбург, ул. Комсомольская, 50, ауд. 713. Центр (класс) деловых игр является одним из элементов материально-технической базы, обеспечивающей проведение отдельных видов практической подготовки обучающихся, по дисциплине (модулю) «Социология для юристов». Задачами и функциями Центра являются:

– выполнение обязательных требований к условиям реализации основной профессиональной образовательной программы высшего образования по специальности 40.05.01 Правовое обеспечение национальной безопасности;

– развитие у обучающихся перспективного, инновационного мышления, ориентированного на развитие социальных процессов, а не только адаптацию к ним;

– интегрирование на практических занятиях научного обоснования как правотворческой и правоприменительной деятельности, так и управления условиями повышения эффективности законодательной системы;

– определение возможности максимальной активизации всех обучающихся, присутствующих на занятии;

– моделирование на практических занятиях наиболее приближенных к реальности задач информационно-аналитической и прогнозно-аналитической работы в области социальной организации. Более подробная информация о Центре содержится в соответствующем паспорте.

5.1.3. Спортивный зал

В реализации ОПОП ВО задействованы спортивный зал, расположен по адресу: Оренбург, ул. Комсомольская, 50. Учебно-тренировочные занятия по физической культуре и спорту базируются на широком использовании теоретических знаний и применении разнообразных средств физической культуры и спорта. Их направленность связана с обеспечением необходимой двигательной активности достижением и поддержанием оптимального уровня физической и функциональной подготовленности в период обучения; приобретением личного опыта совершенствования и коррекции индивидуального физического развития, функциональных и двигательных возможностей; с освоением жизненно и профессионально необходимых навыков, психофизических качеств.

5.1.4. Кабинет криминалистики и криминалистический полигон. В кабинетах, расположенных по адресу: Оренбург, ул. Комсомольская, 50, ауд. 610, 07 проводятся занятия по дисциплине (модулю) «Криминалистика», которые направлены на формирование у обучающихся:

знаний об объекте, предмете, методах криминалистики, классификации следов преступления, основных технико-криминалистических средствах и

методах их собирания и исследования; тактике производства следственных действий; формах и методах организации раскрытия, расследования и профилактике преступлений; методике раскрытия и расследования отдельных видов и групп преступлений;

умений толковать различные юридические факты, правоприменительную и правоохранительную практику; применять технико-криминалистические средства и методы; правильно ставить вопросы, подлежащие разрешению при проведении предварительных исследований и судебных экспертиз; анализировать и правильно оценивать содержание заключений эксперта (специалиста); объяснять суть и значение криминалистической методики расследования преступлений отдельного вида (группы); выявлять, давать оценку и содействовать пресечению коррупционного поведения, осуществлять предупреждение правонарушений, выявлять и устранять причины и условия, способствующие их совершению;

навыков применения при осмотре места происшествия технико-криминалистических средств и методов поиска, обнаружения, фиксации, изъятия и предварительного исследования следов и вещественных доказательств; участия в качестве специалиста при производстве следственных и иных процессуальных действий; навыков ведения экспертно-криминалистических учетов, организации справочно-информационных и информационно-поисковых систем; консультирования субъектов правоприменительной деятельности по вопросам производства и проведения судебных экспертиз, возможностям применения криминалистических средств и методов при установлении фактических обстоятельств расследуемого правонарушения; навыков анализа и обобщения экспертной практики при установлении причин и условий, способствующих совершению правонарушений, разработки предложений, направленных на их устранение.

Кабинет криминалистики оснащен наглядными учебными пособиями, учебными фильмами, тренажерами, техническими средствами и оборудованием, плакатами, обеспечивающими реализацию проектируемых результатов обучения, в том числе:

1) интерактивный электронной доской, электронным проектором, персональным компьютером, позволяющими демонстрировать учебные видеофильмы, обучающие программы, презентации. На пяти ноутбуках установлена программа «Осмотр места происшествия», позволяющая имитировать места совершения различных преступлений и проводить виртуальный осмотр места происшествия по предложенной модели, составлять протокол осмотра.

2) унифицированными криминалистическими чемоданами, укомплектованными необходимыми приборами и приспособлениями для качественного проведения следственных действий;

3) портативными контактными микроскопами Микро, LevenhucZenoCash ZC-12, ультрафиолетовыми осветителями ШАГ-4, ОЛД-

41, применяемые для визуализации ультрафиолетовых меток и других защитных элементов на банкнотах и ценных бумагах.

4) дактилоскопическим сканером «Папилон ДС-30М» с программным обеспечением;

4) массово-габаритными макетами автомата АК, пистолетов ПМ, ТТ, ПЯ, револьвера Наган, наборами стреляных пуль и гильз для баллистических исследований, образцы пулевых повреждений на тканях;

5) цифровыми фотоаппаратами, металлоискателями;

6) унифицированным портфелем для сбора и изъятия микрочастиц «Микрон» для обнаружения, фиксации, изъятия микрообъектов;

7) ширмой для производства учебного опознания в условиях, исключающих визуальный контакт;

8) манекенами и набором имитаторов огнестрельных и иных ранений, а также магнитными кистями, дактилоскопическими красками, порошками и пленками, валиками комплектом йодного дактилоскопирования;

9) другим техническим средствами, материалами.

Более подробная информация о кабинете содержится в Паспорте кабинета криминалистики.

5.1.5. Кабинеты информатики (компьютерные классы) задействован в реализации учебной дисциплины (модуля) «Информатика и информационные технологии в профессиональной деятельности». Он рассчитан на одновременную работу 26-ти обучающихся за персональными компьютерами Pegatron и изучение программных средств, операционных систем, разработки электронных презентаций, освоение технологий подготовки текстовых документов, работы с электронными таблицами, с системами обработки больших данных, с правовой информацией в справочных правовых системах. Кабинет расположен по адресу: Оренбург, ул. Комсомольская, 50, ауд. №512,514.

5.1.6. Кабинеты иностранных языков расположены по адресу: Оренбург, ул. Комсомольская, 50, ауд. №№ 405, 406, 407, 409 задействованы в реализации учебной дисциплины (модуля) «Иностранный язык». Учебные аудитории предназначены поднятию уровня коммуникативного владения иностранным языком при выполнении основных видов речевой деятельности (говорения, письма, чтения и аудирования).

5.2. Перечень программного обеспечения (ПО), установленного на компьютерах, задействованных в образовательном процессе по ОПОП ВО

Институт обеспечен необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства, состав которого определяется в рабочих

программах дисциплин (модулей) и подлежит обновлению при необходимости.

Все аудитории, задействованные в образовательном процессе по реализации ОПОП ВО, оснащены следующим ПО:

№ №	Описание ПО	Наименование ПО, программная среда, СУБД	Вид лицензирования
ПО, устанавливаемое на рабочую станцию			
1.	Операционная система	Microsoft Windows 7 Microsoft Windows 8.1 Microsoft Windows 10	Лицензия
		ООО «+АЛЬЯНС» услуги по предоставлению неисключительных прав(лицензий) на программное обеспечение. По договорам № 242-223/20 от 19.06.2020 г.	
2.	Антивирусная защита	Kaspersky Endpoint Security для Windows	Лицензия
		ООО «Програмос-Проекты» По договорам: № УТ0021486 от 19.07.2016 г. № УТ0024065 от 03.07.2017 №УТ0026711 от 17.07.2018 № 24-223/19 от 05.07.2019 №УТ0031243/9-223/20 от 16.07.2020 №УТ0032987 01.07.2021 №50-223/22 от 14.07.2022 №54-223/23 от 10.08.2023	
3.	Офисные пакеты	Microsoft Office 2019	Лицензия
4.	Программа для ЭВМ «Виртуальный осмотр места происшествия: Учебно-методический комплекс»	По договору: 328-У от 19.02.2021 г.	Лицензия
5.	Архиваторы	WinRar	Открытая лицензия
6.	Интернет браузер	Yandex	Открытая лицензия
7.	Программа для просмотра файлов PDF	PDF24	Открытая лицензия
		Foxit Reader	Открытая лицензия
8.	Программа для просмотра файлов DJVU	DjVuviewer	Открытая лицензия
9.	Пакет кодеков	K-LiteCodecPack	Открытая лицензия
10.	Программа для редактирования фото	Picasa	Открытая лицензия
11.	Программа для работы с графикой	PaintNet	Открытая лицензия
12.	Видеоплеер	WindowsMediaPlayer	В комплекте с ОС

13.	Программа для удаленного доступа	AnyDesk	Открытая лицензия
14.	Программа для проведения конференций	Zoom	Открытая лицензия
12.	Справочно- правовые системы (СПС)	Консультант плюс	Открытая лицензия
		Гарант	Открытая лицензия
13	Услуги по поставке обновленной версии ПО ("АС Нагрузка", Планы Мини","Планы СПО")		Лицензия
		ООО "Лаборатория Математического моделирования и информационных систем" По договорам: №9113 от 16.02.2022 №1005-23 от 03.03.2023 №2480-24 от 21.03.2024	

5.3 Электронно-образовательная система (электронная библиотека) и электронная информационно-образовательная среда

Электронно-образовательная система (электронная библиотека) и электронная информационно-образовательная среда обеспечивают возможность одновременного доступа 100 процентов обучающихся из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети «Интернет», как на территории Университета, так и вне ее. Обучающимся обеспечен доступ (удаленный доступ), в том числе в случае применения электронного обучения, дистанционных образовательных технологий, к современным профессиональным базам данных и информационным справочным системам, состав которых определен в рабочих программах учебных дисциплин (модулей). Полнотекстовая рабочая программа учебной дисциплины (модуля) размещена в Цифровой научно-образовательной и социальной сети Университета (далее - ЦНОСС), в системе которой функционируют «Электронные личные кабинеты обучающегося и научно-педагогического работника». Доступ к материалам возможен через введение индивидуального пароля. ЦНОСС предназначена для создания личностно-ориентированной информационно-коммуникационной среды, обеспечивающей информационное взаимодействие всех участников образовательного процесса Университета, в том числе предоставление им общедоступной и персонализированной справочной, научной, образовательной, социальной информации посредством сервисов, функционирующих на основе прикладных информационных систем Университета.

Помимо электронных библиотек Университета, он обеспечен индивидуальным неограниченным доступом к следующим удаленным

справочно-правовым системам, профессиональным базам данных, электронно-библиотечным системам, подключенным в Университете на основании лицензионных договоров, и имеющим адаптированные версии сайтов для обучающихся с ограниченными возможностями здоровья:

5.3.1. Информационные справочные системы:

1.	ИС «Континент»	сторонняя	http://continent-online.com	ООО «Агентство правовой интеграции «КОНТИНЕНТ», договоры: - № 20040220 от 02.03. 2020 г. с 20.03.2020 г. по 19.03.2021 г.; - № 21021512 от 16.03.2021 г. с 20.03.2021 г. по 19.03.2022 г.; - № 22021712 от 09.03.2022 г. с 20.03 2022 г. по 19.03.2023 г.; - № 23020811 от 06.03.2023 г. с 20.03.2023 г. по 19.03.2024 г. - № 24020711 от 14 марта 2024 г. с 20.03.2024 г. по 19.03. 2025 г. (12 мес.)
2.	СПС WestlawAcademics	сторонняя	https://uk.westlaw.com	Филиал Акционерного общества «Томсон Рейтер (Маркетс) Юроп СА», договоры: - №RU03358/19 от 11.12.2019 г., с 01.01.2020 г. по 31.12.2020 г.; - № ЭБ-6/2021 от 06.11.2020 г. с 01.01.2021 г. по 31.12.2021 г.; - № ЭР-5/2022 от 27.10.2021 г. с 01.01.2022 по 31.12.2022 г.; - № 32211783551 от 16.11.2022 г. с 01.01.2023 г. по 31.12.2023 г. - № ЭР - 4/2023 от 30.11.2023 г. с 01.01.2024 г. по 31.12.2024 г. - № ЭР - 3/2025 от 29.10.2024 г. с 01.01.2025 г по 31.12.2025 г.
3.	КонсультантПлюс	сторонняя	http://www.consultant.ru	Открытая лицензия для образовательных организаций
4.	Гарант	сторонняя	https://www.garant.ru	Открытая лицензия для образовательных организаций

5.3.2. Профессиональные базы данных:

1.	Web of Science	сторонняя	https://apps.webofknowledge.com	ФГБУ «Государственная публичная научно-техническая библиотека России» сублицензионные договоры:

				- № WOS/668 от 02.04.2018 г.; - № WOS/349 от 05.09.2019 г. ФГБУ «Российский фонд фундаментальных исследований» (РФФИ) сублицензионные договоры: - № 20-1566-06235 от 22.09.2020 г.; - № 21-1706-06235 от 14.07.2021 г.
2.	Scopus	сторонняя	https://www.scopus.com	ФГБУ «Государственная публичная научно-техническая библиотека России» сублицензионные договоры: - № SCOPUS/668 от 09 января 2018 г.; - № SCOPUS/349 от 09 октября 2019 г.; ФГБУ «Российский фонд фундаментальных исследований» (РФФИ) сублицензионные договоры: - № 20-1575-06235 от 09.12.2020 г.; - № 21-1702-06235 от14.07.2021 г.
3.	Коллекции полнотекстовых электронных книг информационного ресурса EBSCOHost БД eBookCollection	сторонняя	http://web.a.ebscohost.com	ООО «ЦНИ НЭИКОН», договор № 03731110819000006 от 18.06.2019 г. бессрочно
4.	Национальная электронная библиотека(НЭБ)	сторонняя	https://rusneb.ru	ФГБУ «Российская государственная библиотека», договор № 101/НЭБ/4615 от 01.08.2018 г. с 01.08.2018 по 31.07.2023 г. (безвозмездный)
5.	Президентская библиотека имени Б.Н. Ельцина	сторонняя	https://www.prlib.ru	ФГБУ «Президентская библиотека имени Б. Н. Ельцина, Соглашение о сотрудничестве № 23 от 24.12.2010 г., бессрочно
6.	НЭБ eLIBRARY.RU	сторонняя	http://elibrary.ru	ООО «РУНЕБ», договоры: - № SU-13-03/2019-1 от 27.03.2019 г. с 01.04.2019 г. по 31.03.2020 г.; - № ЭР-1/2020 от 17.04.2020 г. с

				17.04.2020 г. по 16.04.2021 г.; - № ЭР-2/2021 от 25.03.2021 с 01.04.2021 г. по 31.03.2022 г.; - № ЭР-3/2022 от 04.03.2022 г. с 01.04.2022 г. по 31.03.2022 г. - № SU-1494/2023 от 22.03.2023 - № SU – 1494/2024 от 28.03.2024 г. – 1 год - № ЭР - 1/2025 от 21.03.2025
7.	LegalSource	сторонняя	http://web.a.ebscohost.com	ООО «ЦНИ НЭИКОН», договоры - № 414-EBSCO/2020 от 29.11.2019 г., с 01.01.2020 г. по 31.12.2020 г.; - № ЭБ-5/2021 от 02.11.2020 г. с 01.01.2021 г. по 31.12.2021 г.; - № ЭР-2/2022 от 01.10.2021 г. с - 01.01.2022 по 31.12.2022 г. ООО «ИнфоЛига», договор № 414-EBSCO/23 от 21.10.2022 г. с 01.01.2023 г. по 31.12.2023 г.
8.	ЛитРес: Библиотека	сторонняя	http://biblio.litres.ru	ООО «ЛитРес», договоры: - № 290120/Б-1-76 от 12.03.2020 г. с 12.03.2020 г. по 11.03.2021 г.; - № 160221/В-1-157 от 12.03.2021 г. с 12.03.2021 г. по 11.03.2022 г.; - № ЭР-6/2022 от 18.03.2022 г. с 18.03.2022 г. по 17.03.2023 г.; - № 130223/Б-1-136 от 02.03.2023 г. с 18.03.2023 г. по 17.03.2024 г. -№ 210224/ИТ-Б-181 от 05.03.2024 - 1 год - № 180225/ИТ-Б-178 от 24.02.2025г.
9.	Виртуальный читальный зал Российской государственной библиотеки	сторонняя	https://search.rsl.ru	ФГБУ «Российская государственная библиотека», договор № 32312116538 от 14.02.2023 г. - № 095/04/0025 от 26.02.2024 г. - № 095/04/0019 от 24.02.2025 г.

5.3.3. Электронно-библиотечные системы:

1.	ЭБС ZNANIUM.COM	сторонняя	http://znanium.com	ООО «Научно-издательский центр ЗНАНИУМ», договоры: с 01.01.2019 г. по 31.12.2019 г.; - № 3/2019 эбс от 29.11.2019 г. с 01.01.2020 г. по 31.12.2020 г. № 3/2021 эбс от 02.11.2020 г. с 01.01.2021 г. по 31.12.2021 г. - № 1/2022 эбс от 01.10.2021 г. с

				01.01.2022 г. по 31.12.2022 г. - № 32211747575 эбс от 07.10.2022 г. с 01.01.2023 г. по 31.12.2023 г. -№ ЭР-3/2024 от 30 ноября 2023 г. с 01.01.2024 г по 31.12.2024 г. - № ЭР - 2/2025 от 23.10.2024 г. с 01.01.2025 г по 31.12.2025 г.
2.	ЭБС Book.ru	сторонняя	http://book.ru	ООО «КноРус медиа», договоры: с 01.01.2019 г. по 31.12.2019 г.; - № ЭБ-2/2019 от 29.11.2019 г. с 01.01.2020 г. по 31.12.2020 г. №ЭБ-4/2021 от 02.11.2020 г. с 01.01.2021 г. по 31.12.2021 г. - № ЭР-4/2022 от 01.10.2021 г. с 01.01.2022 г. по 31.12.2022 г. - № 32211783653 от 21.10.2022 г. с 01.01.2023 г. по 31.12.2023 г. - № ЭР – 2/2023 от 30 ноября 2023 г. с 01.01.2024 по 31.12.2024 г. - № ЭР - 1/2025 от 14.10.2024 г. с 01.01.2025 г по 31.12.2025 г.
3.	ЭБС Проспект	сторонняя	http://ebs.prospekt.org	ООО «Проспект», договоры: -№ ЭБ-1/2019 от 03.07.2019 г. с 03.07.2019 г. по 02.07.2020 г; - № ЭБ-2/2020 от 03.07.2020 г. с 03.07.2020 г. по 03.07.2021 г. - № ЭР – 3/2021 от 21.06.2021 г. с 03.07.2021 г. по 02.07.2022 г. - № 32211498857 от 24.06.2022 г. с 03.07.2022 г. по 02.07.2023 г. - № 32312506505 от 27.06.2023 г. с 27.06.2023 г. по 27.06.2024 - №ЭР - 3/2024 от 13 06.2024 г.
4.	ЭБС Юрайт	сторонняя	http://www.biblio-online.ru	ООО «Электронное издательство Юрайт», договоры: -№ ЭБ-1/2019 от 01.04.2019 г. с 01.04.2019 г. по 31.03.2020 г.; - № ЭБ-1/2020 от 01.04.2020 г. с 01.04.2020 г. по 31.03.2021 г. -№ ЭР- 1/2021 от 23.03.2021 г. с 03.04. 2021 г. по 02.04.2022 г. № ЭР-7/2022 от 09.03.2022 г. с 03.04.2022 по 02.04.2023 г. -№ ЭР – 1/2024 от 25 марта 2024 г. с 03 04.2024 по 02.04.2025 г. - № ЭР - 2/2025 от 21.03.2025 г. с 03.04.2025 г. по 02.04.2026 г.
5.	ЭБС Издательства	сторонняя	https://elknigi.ru/	договоры: - № ЭР – 1/ 2023 г. от 30.03.2023

	«Юстицинформ»			г. – 1 год - № ЭР – 2/2024 от 29.03.2024 г. – 1 год - № ЭР - 3/2025 от 09.04.2025 - 1 год

5.4. Сведения о доступе к информационным системам и информационно-телекоммуникационным сетям, к которым обеспечивается доступ обучающихся, в том числе приспособленных для использования инвалидами и лицами с ограниченными возможностями здоровья

Обучающиеся из числа инвалидов и лиц с ОВЗ обеспечены печатными и (или) электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.

Для инвалидов и лиц с ограниченными возможностями здоровья созданы условия доступа к информационным системам, информационно-телекоммуникационным сетям и электронным образовательным ресурсам: читальный зал располагается на первом этаже недалеко от входа, предназначенного для маломобильных групп обучающихся, рабочие места в читальном зале оборудованы современными эргономичными моноблоками с качественными экранами, а также аудио-гарнитурами, на каждом компьютере имеется возможность увеличения фрагментов изображения или текста с помощью экранной лупы, озвучивания отображаемого на экране текста. В ЭБС применяются специальные адаптивные технологии для лиц с ограниченными возможностями зрения: версия сайта для слабовидящих, эксклюзивный адаптивный ридер, программа невизуального доступа к информации, коллекция аудиоизданий.

Для формирования условий библиотечного обслуживания инвалидов и лиц с ограниченными возможностями здоровья в Университете выполняется комплекс организационных и технических мероприятий:

1. Наличие рабочих мест в Электронном читальном зале с увеличенным пространством для работы, выделено и обозначено табличкой со знаком доступности для всех категорий инвалидности.
2. **Обеспечено комплексное обслуживание в читальных залах:**

– поиск изданий по электронному каталогу;

– возможность получения изданий из любого отдела Библиотеки.

3. **Обеспечено удаленное обслуживание:**

– официальный сайт Университета – www.msal.ru и, следовательно, страничка Библиотеки, адаптирована для слабовидящих;

– возможен поиск изданий по электронному каталогу;

– возможен онлайн-заказ изданий.

4. Рабочее место оборудовано:

– выведена экранная лупа Windows 7 на «рабочий стол» экрана компьютера;

– бесплатной программой NVDA - NVDA программа экранного доступа для операционных систем семейства Windows, позволяющая незрячим и слабовидящим пользователям работать на компьютере выводя всю необходимую информацию с помощью речи.