ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ В ПРАВОВОЙ ДЕЯТЕЛЬНОСТИ
09.03.02 Информационные системы и технологии
2026 год набора
Приложение В
к основной профессиональной образовательной программе
по направлению подготовки 09.03.02 Информационные системы и технологии,
утвержденной приказом от 15.06.2026 г. № 64-О

АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОБРАЗОВАТЕЛЬНАЯ ОРГАНИЗАЦИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
«КУБАНСКИЙ ИНСТИТУТ ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ»
(АНОО ВО «КИПО»)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.О.20 Технологии защиты информации в правоохранительной деятельности

Направление подготовки
09.03.02 Информационные системы и технологии

Направленность (профиль)
Информационные системы и технологии в правовой деятельности

Уровень высшего образования
Бакалавриат

Квалификация
Бакалавр

Форма обучения
очная/ очно-заочная/заочная

Год набора
2026

ИНФОРМАЦИОННЫЕ СИСТЕМЫ
И ТЕХНОЛОГИИ В ПРАВОВОЙ ДЕЯТЕЛЬНОСТИ
09.03.02 Информационные системы и технологии
2026 год набора

Рабочая программа дисциплины (модуля) Б1.О.20 «Технологии защиты информации в правоохранительной деятельности» предназначена для реализации основной профессиональной образовательной программы высшего образования.

Составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 09.03.02 Информационные системы и технологии (Приказ Минобрнауки РФ от 19.09.2017 г. № 926, зарегистрирован в Минюсте РФ от 12.10.2017 г. № 48535).

ИНФОРМАЦИОННЫЕ СИСТЕМЫ
И ТЕХНОЛОГИИ В ПРАВОВОЙ ДЕЯТЕЛЬНОСТИ
09.03.02 Информационные системы и технологии
2026 год набора

СОДЕРЖАНИЕ

ИНФОРМАЦИОННЫЕ СИСТЕМЫ
И ТЕХНОЛОГИИ В ПРАВОВОЙ ДЕЯТЕЛЬНОСТИ
09.03.02 Информационные системы и технологии
2026 год набора

1 Цели и задачи изучения дисциплины (модуля)

1.1 Цель освоения дисциплины

Целью изучения дисциплины Б1.О.20 «Технологии защиты информации в правоохранительной деятельности» является формирование у обучающихся теоретических знаний и практических навыков в области применения современных технологий, методов и средств защиты информации для обеспечения информационной безопасности в деятельности правоохранительных органов.

1.2 Задачи дисциплины

1. Изучить теоретические основы и нормативно-правовое регулирование информационной безопасности применительно к правоохранительной деятельности.
2. Освоить классификацию и характеристики угроз информационной безопасности, а также основные методы и технологии их выявления, предупреждения и нейтрализации.
3. Сформировать навыки применения организационных и технических мер защиты информации в правоохранительных органах.
4. Развить умения использования специального программного и аппаратного обеспечения для защиты информации, средств криптографической защиты и электронной подписи.
5. Овладеть методиками противодействия компьютерным преступлениям, обеспечения безопасности персональных данных и защищённого электронного документооборота в правоохранительных органах.

1.3 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Б1.О.20 «Технологии защиты информации в правоохранительной деятельности» относится к обязательной части Блока 1 «Дисциплины (модули)» учебного плана.

В соответствии с рабочим учебным планом дисциплина изучается на 3 курсе по очной, на 3 курсе очно-заочной и на 3 курсе заочной формы обучения.

Вид промежуточной аттестации: зачет.

1.4 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Изучение данной учебной дисциплины направлено на формирование у обучающихся следующих компетенций:

Код и наименование компетенции	Код и наименование индикаторов достижения результатов обучения по дисциплине	Планируемые результаты обучения
ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**ОПК-3.1.** Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. **ОПК-3.2.** Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. **ОПК-3.3.** Имеет навыки подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по	**Знать:** основные возможности, предоставляемые современными информационно-коммуникационными технологиями для решения стандартных задач профессиональной деятельности в правоохранительной сфере; принципы и методы информационной и библиографической культуры, их составляющие и пути формирования применительно к профессиональной деятельности ; основные требования информационной безопасности при работе с информационными

Код и наименование компетенции	Код и наименование индикаторов достижения результатов обучения по дисциплине	Планируемые результаты обучения
	научно-исследовательской работе с учетом требований информационной безопасности.	системами и базами данных в правоохранительных органах; нормативно-правовую базу, регламентирующую защиту информации и обращение с документами ограниченного доступа; информационные процессы профессиональной деятельности, включая сбор, обработку, хранение и передачу служебной информации ; методы выявления, предупреждения и нейтрализации угроз информационной безопасности в повседневной профессиональной деятельности. **Уметь:** применять информационно-коммуникационные технологии для решения стандартных профессиональных задач с учетом основных требований информационной безопасности ; осуществлять поиск, анализ и обобщение правовой и служебной информации из различных источников с соблюдением установленных правил доступа; использовать справочно-правовые системы, ведомственные базы данных и информационные ресурсы для выполнения профессиональных задач; осуществлять самодиагностику уровня профессиональной информационной компетентности и определять направления её повышения ; применять организационные и технические меры защиты информации при работе с электронными документами и базами данных; правильно оформлять и хранить служебную документацию, содержащую сведения ограниченного распространения; использовать средства криптографической защиты информации и электронной подписи при обмене документами. **Владеть:** навыками применения информационно-коммуникационных технологий в профессиональной деятельности с учетом основных

Код и наименование компетенции	Код и наименование индикаторов достижения результатов обучения по дисциплине	Планируемые результаты обучения
		требований информационной безопасности ; навыками подготовки аналитических обзоров, аннотаций, рефератов и научных докладов по вопросам защиты информации и правоохранительной деятельности; навыками составления библиографических описаний и оформления списков литературы в соответствии с установленными стандартами (ГОСТ Р 7.0.100-2018) ; навыками поиска научной и нормативно-технической информации в специализированных базах данных с соблюдением правил информационной безопасности; навыками публичного представления результатов научно-исследовательской работы с учётом требований к защите служебной информации; навыками документирования результатов профессиональной деятельности и составления отчётной документации в соответствии с установленными требованиями.

Результаты обучения по дисциплине достигаются в рамках осуществления всех видов контактной и самостоятельной работы обучающихся в соответствии с утвержденным учебным планом.

Индикаторы достижения компетенций считаются сформированными при достижении соответствующих им результатов обучения.

2. Структура и содержание дисциплины

2.1 Распределение трудоёмкости дисциплины по видам работ

Общая трудоёмкость дисциплины составляет 4 зачетных единицы (144 час.), их распределение по видам работ представлено в таблице

Виды работ	Всего часов		
	ОФО	ОЗФО	ЗФО
Контактная работа, в том числе:	**38**	**38**	**6**
Аудиторные занятия (всего):	**38**	**38**	**6**
занятия лекционного типа	12	**12**	**2**
практические занятия	26	**26**	**4**
Иная контактная работа:	**-**	**-**	**-**
Контрольная работа	**-**	**-**	**-**
Курсовая работа	**-**	**-**	**-**
Самостоятельная работа, в том числе:	**106**	**106**	**134**
Самоподготовка по темам (разделам) дисциплины	86	86	**104**
Подготовка к текущему контролю	20	20	**30**

Контроль:		**-**	**-**	**-**
Промежуточная аттестация (зачет)		-	**-**	**-**
Общая трудоемкость	**час.**	**144**	**144**	**144**
	в том числе контактная работа	**38**	**38**	**6**
	зач. ед	**4**	**4**	**4**

2.2 Содержание дисциплины

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.
Разделы (темы) дисциплины, изучаемые на 3 курсе (очная форма обучения)

№	Наименование темы/раздела	Количество часов				
		Всего	В том числе в виде практической подготовки	Аудиторная работа		Внеаудиторная работа (СР)
				Л	ПЗ	
1.	Нормативно-правовое регулирование защиты информации в правоохранительной сфере. 1.1. Система законодательства РФ в области информационной безопасности. ФЗ №149 «Об информации, информационных технологиях и о защите информации». 1.2. ФЗ №152 «О персональных данных»: требования к операторам ПДн в правоохранительных органах. Категории ПДн. 1.3. Закон РФ №5485-1 «О государственной тайне». Грифование сведений. Допуск к государственной тайне. 1.4. Приказы ФСТЭК России, ФСБ России, МВД России в области защиты информации.	37	-	3	8	26
2.	Угрозы информационной безопасности и методы их нейтрализации в правоохранительных системах. 2.1. Основные угрозы безопасности информации: перехват, модификация, уничтожение, блокирование данных. 2.2. Социальная инженерия и фишинг как угрозы для сотрудников правоохранительных органов. 2.3. Вредоносное программное обеспечение (вирусы, трояны, программы-шпионы). 2.4. Модель нарушителя информационной безопасности. Классы защищенности ИС.	35	-	3	6	26

3.	Организационные и технические меры защиты информации. 3.1. Политика информационной безопасности в правоохранительном органе. 3.2. Управление доступом: идентификация, аутентификация, авторизация. Биометрические системы. 3.3. Антивирусная защита. Межсетевые экраны (фаерволы). Системы обнаружения вторжений (IDS/IPS). 3.4. Резервное копирование и восстановление данных. Аудит информационной безопасности.	35	-	3	6	26
4.	Криптографическая защита информации и защита гостайны. 4.1. Основы криптографии. Симметричные и асимметричные алгоритмы шифрования. 4.2. Электронная подпись: назначение, виды, применение в правоохранительной деятельности. 4.3. Средства криптографической защиты информации (СКЗИ). Лицензирование деятельности в области криптографии. 4.4. Защита сведений, составляющих государственную тайну, в информационных системах. Аттестация объектов информатизации.	37		3	6	28
	ИТОГО по разделам дисциплины	144	-	12	26	106
	Контрольная работа	-	-	-	-	-
	Курсовая работа	-	-	-	-	-
	Промежуточная аттестация (зачет)	-	-	-	-	-
	Общая трудоемкость по дисциплине	144	-	12	26	106

Разделы (темы) дисциплины, изучаемые на 3 курсе (очнор-заочная форма обучения)

№	Наименование темы/раздела	Количество часов				
		Всего	В том числе в виде практической подготовки	Аудиторная работа		Внеаудиторная работа (СР)
				Л	ПЗ	

1.	Нормативно-правовое регулирование защиты информации в правоохранительной сфере. 1.1. Система законодательства РФ в области информационной безопасности. ФЗ №149 «Об информации, информационных технологиях и о защите информации». 1.2. ФЗ №152 «О персональных данных»: требования к операторам ПДн в правоохранительных органах. Категории ПДн. 1.3. Закон РФ №5485-1 «О государственной тайне». Грифование сведений. Допуск к государственной тайне. 1.4. Приказы ФСТЭК России, ФСБ России, МВД России в области защиты информации.	37	-	3	8	26
2.	Угрозы информационной безопасности и методы их нейтрализации в правоохранительных системах. 2.1. Основные угрозы безопасности информации: перехват, модификация, уничтожение, блокирование данных. 2.2. Социальная инженерия и фишинг как угрозы для сотрудников правоохранительных органов. 2.3. Вредоносное программное обеспечение (вирусы, трояны, программы-шпионы). 2.4. Модель нарушителя информационной безопасности. Классы защищенности ИС.	35	-	3	6	26
3.	Организационные и технические меры защиты информации. 3.1. Политика информационной безопасности в правоохранительном органе. 3.2. Управление доступом: идентификация, аутентификация, авторизация. Биометрические системы. 3.3. Антивирусная защита. Межсетевые экраны (фаерволы). Системы обнаружения вторжений (IDS/IPS). 3.4. Резервное копирование и восстановление данных. Аудит информационной безопасности.	35	-	3	6	26
4.	Криптографическая защита информации и защита гостайны. 4.1. Основы криптографии. Симметричные и асимметричные алгоритмы шифрования. 4.2. Электронная подпись: назначение, виды, применение в правоохранительной деятельности. 4.3. Средства криптографической защиты информации (СКЗИ). Лицензирование деятельности в области криптографии. 4.4. Защита сведений, составляющих государственную тайну, в информационных системах. Аттестация объектов информатизации.	37		3	6	28
	ИТОГО по разделам дисциплины	144	-	12	26	106
	Контрольная работа	-	-	-	-	-
	Курсовая работа	-	-	-	-	-
	Промежуточная аттестация (зачет)	-	-	-	-	-

	Общая трудоемкость по дисциплине	144	-	12	26	106

Разделы (темы) дисциплины, изучаемые на 3 курсе (заочная форма обучения)

№	Наименование темы/раздела	Количество часов				
		Всего	В том числе в виде практической подготовки	Аудиторная работа		Внеаудиторная работа (СР)
				Л	ПЗ	
1.	Нормативно-правовое регулирование защиты информации в правоохранительной сфере. 1.1. Система законодательства РФ в области информационной безопасности. ФЗ №149 «Об информации, информационных технологиях и о защите информации». 1.2. ФЗ №152 «О персональных данных»: требования к операторам ПДн в правоохранительных органах. Категории ПДн. 1.3. Закон РФ №5485-1 «О государственной тайне». Грифование сведений. Допуск к государственной тайне. 1.4. Приказы ФСТЭК России, ФСБ России, МВД России в области защиты информации.	44	-	1	1	46
2.	Угрозы информационной безопасности и методы их нейтрализации в правоохранительных системах. 2.1. Основные угрозы безопасности информации: перехват, модификация, уничтожение, блокирование данных. 2.2. Социальная инженерия и фишинг как угрозы для сотрудников правоохранительных органов. 2.3. Вредоносное программное обеспечение (вирусы, трояны, программы-шпионы). 2.4. Модель нарушителя информационной безопасности. Классы защищенности ИС.	44	-		2	44
3.	Организационные и технические меры защиты информации. 3.1. Политика информационной безопасности в правоохранительном органе. 3.2. Управление доступом: идентификация, аутентификация, авторизация. Биометрические системы. 3.3. Антивирусная защита. Межсетевые экраны (фаерволы). Системы обнаружения вторжений (IDS/IPS). 3.4. Резервное копирование и восстановление данных. Аудит информационной безопасности.	43	-	1	1	44

4.	Криптографическая защита информации и защита гостайны. 4.1. Основы криптографии. Симметричные и асимметричные алгоритмы шифрования. 4.2. Электронная подпись: назначение, виды, применение в правоохранительной деятельности. 4.3. Средства криптографической защиты информации (СКЗИ). Лицензирование деятельности в области криптографии. 4.4. Защита сведений, составляющих государственную тайну, в информационных системах. Аттестация объектов информатизации.					
	ИТОГО по разделам дисциплины	144	-	2	4	134
	Контрольная работа	-	-	-	-	-
	Курсовая работа	-	-	-	-	-
	Промежуточная аттестация (зачет)	-	-	-	-	-
	Общая трудоемкость по дисциплине	144	-	2	4	134

Примечание: Л – лекции, ПЗ – практические занятия / семинары, СР – самостоятельная работа обучающегося

При изучении дисциплины могут применятся электронное обучение, дистанционные образовательные технологии в соответствии с ФГОС ВО.

2.3 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине)

Самостоятельная работа – это индивидуальная познавательная деятельность обучающегося как на аудиторных занятиях, так и во внеаудиторное время. Самостоятельная работа должна быть многогранной и иметь четко выраженную направленность на формирование конкретных компетенций.

Цель самостоятельной работы – овладение знаниями, профессиональными умениями и навыками, опытом исследовательской деятельности и обеспечение формирования профессиональных компетенций, воспитание потребности в самообразовании, ответственности и организованности, творческого подхода к решению проблем.

Самостоятельная работа обучающихся направлена на углубленное изучение разделов и тем рабочей программы. Самостоятельная работа предполагает изучение литературных источников, выполнение контрольных заданий и работ, проведение исследований разного характера. Работа основывается на анализе литературных источников и других материалов, а также реальных фактов, личных наблюдений.

Самостоятельная работа включает разнообразный комплекс видов и форм работы обучающихся:

- работа с лекционным материалом, предусматривающая проработку конспекта лекций и учебной литературы;
- поиск (подбор) и обзор литературы, электронных источников информации по заданной проблеме курса, написание реферата (доклада, эссе), исследовательской работы по заданной проблеме;
- выполнение задания по пропущенной или плохо усвоенной теме;
- изучение материала, вынесенного на самостоятельную проработку (отдельные темы, параграфы);
- подготовка к практическим занятиям;

- подготовка к промежуточной аттестации.

№ п/п	Вид учебно-методического обеспечения
1.	Методические рекомендации по самостоятельной работе обучающихся.
2.	Методические рекомендации по изучению дисциплины.
3.	Вопросы для письменного/устного собеседования, реферат, сообщение, доклад, эссе, практико-ориентированные задания, мини-кейсы, задания в виде расчетных задач, ситуационные задачи.

Задания для самостоятельной работы обучающихся по дисциплине Б1.О.20 «Технологии защиты информации в правоохранительной деятельности» представлены в учебно-методическом отделе.

Контроль результатов самостоятельной работы обучающихся может осуществляться в пределах времени, отведенного на обязательные учебные занятия и внеаудиторную самостоятельную работу обучающихся по дисциплине, может проходить в письменной, устной или смешанной форме.

Учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) при изучении данной дисциплины предоставлена возможность выбора технологий обучения в зависимости от степени заболевания и осознания своей деятельности. При этом содержание программы дисциплины не изменяется, изменяются, как правило, форма обучения и образовательные технологии. Также обучающимся, имеющим инвалидность, и лицам с ограниченными возможностями здоровья созданы условия комфортного психологического климата в процессе обучения и возможности оказания помощи в установлении полноценных межличностных отношений с другими обучающимися.

3. Образовательные технологии, применяемые при освоении дисциплины (модуля)

В ходе изучения дисциплины предусмотрено использование следующих образовательных технологий: лекции, практические занятия, проблемное обучение, модульная технология, подготовка письменных аналитических работ, самостоятельная работа обучающихся.

Компетентностный подход в рамках преподавания дисциплины реализуется в использовании интерактивных технологий и активных методов (проектных методик, мозгового штурма, разбора конкретных ситуаций, анализа педагогических задач, педагогического эксперимента, иных форм) в сочетании с внеаудиторной работой.

Информационные технологии, применяемые при изучении дисциплины: использование информационных ресурсов, доступных в информационно-телекоммуникационной сети Интернет.

Адаптивные образовательные технологии, применяемые при изучении дисциплины – для лиц с ограниченными возможностями здоровья предусмотрена организация консультаций с использованием электронной почты.

4. Фонд оценочных средств для текущего контроля успеваемости и промежуточной аттестации по дисциплине (модулю)

ИНФОРМАЦИОННЫЕ СИСТЕМЫ
И ТЕХНОЛОГИИ В ПРАВОВОЙ ДЕЯТЕЛЬНОСТИ
09.03.02 Информационные системы и технологии
2026 год набора

Оценочные средства предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины Б1.О.20 «Технологии защиты информации в правоохранительной деятельности». Материалы для проведения текущего контроля успеваемости и промежуточной аттестации размещены в фонде оценочных средств по дисциплине Б1.О.20 «Технологии защиты информации в правоохранительной деятельности».

4.1. Структура оценочных средств для текущего контроля и промежуточной аттестации по дисциплине (модулю)

№ п/п	Код и наименование индикаторов достижения результатов обучения по дисциплине	Результаты обучения	Наименование оценочного средства	
			Текущий контроль	Промежуточная аттестация
1	ОПК-3.1. Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	**Знать:** основные возможности, предоставляемые современными информационно-коммуникационными технологиями для решения стандартных задач профессиональной деятельности в правоохранительной сфере; принципы и методы информационной и библиографической культуры, их составляющие и пути формирования применительно к профессиональной деятельности ; основные требования информационной безопасности при работе с информационными системами и базами данных в правоохранительных органах; нормативно-правовую базу, регламентирующую защиту информации и обращение с документами ограниченного доступа; информационные процессы профессиональной деятельности, включая сбор, обработку, хранение и передачу служебной информации ; методы выявления, предупреждения и нейтрализации угроз информационной безопасности в повседневной профессиональной деятельности. **Уметь:** применять информационно-коммуникационные технологии	Подготовка докладов/сообщений, вопросы для обсуждения по темам, задания открытого и закрытого типа	Вопросы на экзамене
2	ОПК-3.2. Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.		Подготовка докладов/сообщений, вопросы для обсуждения по темам, задания открытого и закрытого типа	Вопросы на экзамене
3	ОПК-3.3. Имеет навыки подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по		Подготовка докладов/сообщений, вопросы для обсуждения по темам, задания открытого и закрытого типа	Вопросы на экзамене

	научно-исследовательской работе с учетом требований информационной безопасности.	для решения стандартных профессиональных задач с учетом основных требований информационной безопасности ; осуществлять поиск, анализ и обобщение правовой и служебной информации из различных источников с соблюдением установленных правил доступа; использовать справочно-правовые системы, ведомственные базы данных и информационные ресурсы для выполнения профессиональных задач; осуществлять самодиагностику уровня профессиональной информационной компетентности и определять направления её повышения ; применять организационные и технические меры защиты информации при работе с электронными документами и базами данных; правильно оформлять и хранить служебную документацию, содержащую сведения ограниченного распространения; использовать средства криптографической защиты информации и электронной подписи при обмене документами. **Владеть:** навыками применения информационно-коммуникационных технологий в профессиональной деятельности с учетом основных требований информационной безопасности ; навыками подготовки аналитических обзоров, аннотаций, рефератов и научных докладов по вопросам защиты информации и правоохранительной деятельности; навыками составления библиографических описаний и оформления списков литературы в соответствии с установленными стандартами (ГОСТ Р 7.0.100-2018) ;		

		навыками поиска научной и нормативно-технической информации в специализированных базах данных с соблюдением правил информационной безопасности; навыками публичного представления результатов научно-исследовательской работы с учётом требований к защите служебной информации; навыками документирования результатов профессиональной деятельности и составления отчётной документации в соответствии с установленными требованиями.		

4.2. Типовые задания для текущего контроля и вопросы (теоретические и практические) для промежуточной аттестации по дисциплине (модулю)

Задания для текущего контроля и вопросы (теоретические и практические) для промежуточной аттестации, необходимые для оценки образовательных достижений обучающихся.

Текущий контроль успеваемости для обучающихся

Темы докладов, рефератов, сообщений

1. Система законодательства РФ в области защиты информации в правоохранительных органах.
2. ФЗ №152 «О персональных данных»: требования к обработке ПДн в судах и правоохранительных органах.
3. Закон РФ «О государственной тайне»: грифование, допуск, ответственность.
4. Основные угрозы информационной безопасности в информационных системах МВД России.
5. Социальная инженерия как угроза для сотрудников правоохранительных органов.
6. Криптографическая защита информации в государственных информационных системах.
7. Электронная подпись в судебной системе и правоохранительной деятельности.
8. Организация антивирусной защиты в органах внутренних дел.
9. Межсетевые экраны и системы обнаружения вторжений в правоохранительных сетях.
10. Аттестация объектов информатизации как элемент системы защиты гостайны.

Тестовые задания (закрытого типа)

1. Процесс предоставления определенных полномочий лицу или группе лиц на выполнение некоторых действий в информационной системе — это:
А) Идентификация
Б) Аутентификация

В) Авторизация
Г) Регистрация
2. Какой вид атак позволяет злоумышленнику перехватывать и читать передаваемые по сети данные?
А) Атаки на целостность
Б) Атаки на доступность
В) Атаки на конфиденциальность
Г) Атаки на аутентификацию
3. Что такое межсетевой экран (firewall)?
А) Программа для анализа логов сервера
Б) Устройство или ПО, которое фильтрует сетевой трафик и блокирует нежелательные соединения
В) Сбор данных о состоянии системы и обнаружение уязвимостей
Г) Утилита для удаленного доступа к другому компьютеру
4. Информация, составляющая государственную тайну, не может иметь гриф:
А) «Секретно»
Б) «Совершенно секретно»
В) «Особой важности»
Г) «Для служебного пользования»
5. Что такое фишинг?
А) Вид атаки на сервер, когда злоумышленник внедряет зловредный код в систему
Б) Метод шифрования данных для защиты от перехвата
В) Атака, направленная на получение конфиденциальной информации путём обмана пользователя
Г) Устройство для контроля входящего и исходящего трафика в сети

Шкала оценивания результатов по заданиям для проведения текущего контроля успеваемости по дисциплине

% верных решений (ответов)	Шкала оценивания
85-100	5 - отлично
71-84	4 - хорошо
50-70	3 - удовлетворительно
0-49	2 - неудовлетворительно

Текущий контроль успеваемости для обучающихся по очной форме

Контрольная работа представляет собой систематическое, достаточно полное изложение авторского решения соответствующей проблемы и выполнение заданий в рамках дисциплины, которая является одним из видов текущего контроля успеваемости обучающихся очной формы обучения.

Цели контрольной работы:

- проверка и оценка знаний обучающихся;
- закрепление практических навыков применения теоретических подходов и методов анализа на учебных примерах и задачах;
- получение информации об уровне самостоятельности и активности обучающегося, об эффективности форм и методов учебной работы.

Контрольные работы выполняются обучающимися в сроки, предусмотренные учебным планом и календарным учебным графиком.

Контрольная работа выполняется в рукописном или в печатном (компьютерном) варианте на листах формата А4 в 1 экземпляре с соблюдением установленного формата. Текст набирается

шрифтом Times New Roman 12, через 1 интервал, абзацный отступ - 1,25 см, выравнивание по ширине страницы. Страница должна иметь следующие поля: левое - 25 мм, правое - 10 мм, верхнее и нижнее - 20 мм. Титульный лист содержит информацию об обучающемся выполнившем контрольную работу (ФИО обучающегося, направление подготовки, группа); наименование дисциплины; ФИО преподавателя, проверяющего работу.

Задания для контрольных работ разрабатываются преподавателем дисциплины по вариантам, которые содержат:

1) Задание в форме ответа на теоретический вопрос по теме (разделу) – объем не более 2-3 страниц;
2) Задания, составленные в форме тестов (2 задания открытого и закрытого типа, разработанные в фонде оценочных средств).

Готовая контрольная работа в электронном виде прикрепляется в электронную образовательную среду Moodle в профиль обучающегося выполнившего работу до начала сессии. Если работа в рукописном варианте, то она должна быть отсканирована и прикреплена.

Шкала и критерии оценивания контрольной работы

№ п/п	Критерии	Зачтено
Теоретический вопрос		
1	Глубина проработки материала	Основные теоретические положения по вопросу раскрыты. Имеются элементы обоснования выводов
2	Представление	Имеются элементы систематизации информации, факты применения профессиональной терминологии
3	Использование рекомендованной литературы	Основные источники рекомендованной литературы использованы
4	Грамотность изложения и качество оформления	Продемонстрирована культура речи. Соблюдены основные требования к оформлению
Выполнение тестовых заданий		

Если работа не отвечает названным критериям, выставляется оценка «не зачтено».

Зачтено-экзаменационные материалы для промежуточной аттестации (зачет)

Теоретические вопросы к зачету

1. Понятие информационной безопасности. Основные составляющие: конфиденциальность, целостность, доступность.
2. Система законодательства РФ в области защиты информации в правоохранительной сфере.
3. ФЗ №149 «Об информации, информационных технологиях и о защите информации»: основные положения.
4. ФЗ №152 «О персональных данных»: категории персональных данных, требования к операторам.
5. Закон РФ №5485-1 «О государственной тайне»: понятие гостайны, порядок допуска, грифование.
6. Приказы ФСТЭК России в области защиты информации (общие требования, аттестация объектов информатизации).
7. Приказы ФСБ России в области криптографической защиты информации.
8. Ответственность за нарушения в области информационной безопасности (КоАП РФ, УК РФ).
9. Основные угрозы информационной безопасности в правоохранительных системах.
10. Вредоносное программное обеспечение: классификация, методы

распространения, способы защиты.

11. Социальная инженерия как угроза: методы, примеры, противодействие.
12. Модель нарушителя информационной безопасности. Классы защищенности ИС.
13. Политика информационной безопасности: структура, содержание, внедрение.
14. Управление доступом: идентификация, аутентификация, авторизация.
15. Антивирусная защита: виды антивирусов, организация обновлений.
16. Межсетевые экраны (фаерволы): назначение, виды, правила фильтрации.
17. Системы обнаружения и предотвращения вторжений (IDS/IPS).
18. Резервное копирование и восстановление данных: стратегии, периодичность, хранение.
19. Аудит информационной безопасности: цели, методы, периодичность.
20. Основы криптографии. Симметричные и асимметричные алгоритмы шифрования.
21. Электронная подпись: назначение, виды, применение в правоохранительной деятельности.
22. Средства криптографической защиты информации (СКЗИ). Лицензирование деятельности.
23. Защита сведений, составляющих государственную тайну, в информационных системах.
24. Аттестация объектов информатизации: этапы, документация, периодичность.
25. Защита персональных данных в информационных системах правоохранительных органов.
26. DLP-системы (Data Loss Prevention): назначение, принципы работы.
27. Организация защищенного документооборота в судах и правоохранительных органах.
28. Требования к защите информации при использовании облачных сервисов в госорганах.
29. Планирование мероприятий по защите информации. План защиты информации.
30. Принципы работы систем «Антиплагиат» и их использование в научной деятельности.

Практические задания к зачету

Задание 1. Анализ нормативно-правового акта

Проанализируйте фрагмент ФЗ №152 «О персональных данных» (статья 6 «Условия обработки персональных данных»). Ответьте на вопросы:

1. На каких основаниях правоохранительные органы могут обрабатывать персональные данные без согласия субъекта?
2. Какие меры защиты ПДн должны быть приняты оператором?
3. Какая ответственность предусмотрена за нарушение требований закона?

Задание 2. Оценка угроз информационной безопасности

Для информационной системы суда (работает в сети суда, содержит ПДн участников процессов, подключена к ВПН) проведите анализ угроз. Заполните таблицу:

Угроза	Источник	Вероятность	Последствия	Меры защиты
Утечка через USB-накопитель	Сотрудник	Высокая	Раскрытие ПДн	Блокировка USB, DLP

Угроза	Источник	Вероятность	Последствия	Меры защиты
...	...	...	...	...

Задание 3. Составление политики информационной безопасности

Разработайте фрагмент Политики информационной безопасности для районного суда (раздел «Правила работы с персональными данными»). Укажите не менее 5 конкретных правил для сотрудников.

Задание 4. Расчет требований к парольной политике

Рассчитайте требования к парольной политике для информационной системы с классом защищенности 2. Используйте приказ ФСТЭК России от 11.02.2013 №17. Определите:

1. Минимальную длину пароля
2. Сложность пароля (количество типов символов)
3. Срок действия пароля
4. Количество запоминаемых паролей
5. Блокировку после неудачных попыток

Задание 5. Оформление электронной подписи

Опишите порядок получения и использования электронной подписи сотрудником прокуратуры для отправки документов в вышестоящие органы. Какие виды ЭП используются? Как обеспечивается юридическая значимость?

Задание 6. Оценка стоимости мер защиты

Рассчитайте ориентировочную стоимость внедрения следующих мер защиты информации для районного суда (25 АРМ):

1. Установка и настройка антивирусной защиты
2. Внедрение системы резервного копирования
3. Проведение аттестации объекта информатизации

Задание 7. Разбор инцидента ИБ

Опишите алгоритм действий ответственного за информационную безопасность при обнаружении вредоносного ПО на рабочей станции судьи:

1. Какие первоочередные меры?
2. Кому сообщается?
3. Какие документы оформляются?
4. Как восстанавливается работа?

Задание 8. Оформление библиографического списка

Составьте библиографический список (5 источников) по теме «Защита персональных данных в судебной системе» в соответствии с ГОСТ Р 7.0.100-2018. Включите:

1) 1 федеральный закон
2) 1 учебник
3) 2 научные статьи из eLIBRARY.RU
4) 1 нормативно-правовой акт (приказ)

Критерии оценивания промежуточной аттестации: зачет

Оценка	Критерии оценивания по зачету
«зачтено»	заслуживает обучающийся, полностью или практически полностью освоивший знания, умения, компетенции и теоретический материал, учебные задания не оценены максимальным числом баллов, в основном

	сформировал практические навыки.
«не зачтено»:	заслуживает обучающийся, не освоивший знания, умения, компетенции и теоретический материал, учебные задания не выполнил, практические навыки не сформированы.

Оценочные средства для инвалидов и лиц с ограниченными возможностями здоровья выбираются с учетом их индивидуальных психофизических особенностей.

– при необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на экзамене;

– при проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование технических средств, необходимых им в связи с их индивидуальными особенностями;

– при необходимости для обучающихся с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине (модулю) предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

– в печатной форме увеличенным шрифтом,

– в форме электронного документа.

Для лиц с нарушениями слуха:

– в печатной форме,

– в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:

– в печатной форме,

– в форме электронного документа.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

5. Методические указания для обучающихся по освоению дисциплины (модуля)

Дисциплина реализуется посредством проведения контактной работы с обучающимися (включая проведение текущего контроля успеваемости), самостоятельной работы обучающихся и промежуточной аттестации.

При проведении учебных занятий по дисциплине обеспечивается развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств (включая проведение интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализ ситуаций и имитационных моделей, преподавание дисциплины в форме курса, составленного на основе результатов научных исследований, проводимых институтом, в том числе с учетом региональных особенностей профессиональной деятельности выпускников и потребностей работодателей).

Результат обучения считается сформированным, если теоретическое содержание курса освоено полностью; при устных собеседованиях обучающийся исчерпывающе, последовательно, четко и логически стройно излагает учебный материал; свободно справляется с задачами, вопросами и другими видами заданий, требующих применения знаний, использует в ответе дополнительный материал; все предусмотренные рабочей учебной программой задания выполнены в соответствии с установленными требованиями, обучающийся способен анализировать полученные результаты; проявляет самостоятельность при выполнении заданий.

Результат обучения считается несформированным, если обучающийся при выполнении заданий не демонстрирует знаний учебного материала, допускает ошибки, неуверенно, с большими затруднениями выполняет задания, не демонстрирует необходимых умений, качество выполненных заданий не соответствует установленным требованиям.

Методические указания для обучающихся по освоению дисциплины на занятиях лекционного типа

Лекционный курс предполагает систематизированное изложение основных вопросов тематического плана. В ходе лекционных занятий раскрываются базовые вопросы в рамках каждой темы дисциплины. Обозначаются ключевые аспекты тем, а также делаются акценты на наиболее сложные и важные положения изучаемого материала. Материалы лекций являются опорной основой для подготовки обучающихся к практическим занятиям и выполнения заданий самостоятельной работы, а также к мероприятиям текущего контроля успеваемости и промежуточной аттестации по дисциплине.

В ходе лекционных занятий необходимо вести конспектирование учебного материала. Возможно ведение конспекта лекций в виде интеллект-карт.

Методические указания для обучающихся по освоению дисциплины на занятиях практического типа

Практические (семинарские) занятия представляют собой детализацию лекционного теоретического материала, проводятся в целях закрепления курса и охватывают все основные разделы. Основной формой проведения семинаров и практических занятий является обсуждение наиболее проблемных и сложных вопросов по отдельным темам, а также решение задач и разбор примеров и ситуаций в аудиторных условиях.

Практические (семинарские) занятия обучающихся обеспечивают:

- проверку и уточнение знаний, полученных на лекциях;
- получение умений и навыков составления докладов и сообщений, обсуждения вопросов по учебному материалу дисциплины;
- подведение итогов занятий по рейтинговой системе, согласно технологической карте дисциплины.

Методические указания по самостоятельной работе обучающихся

Самостоятельная работа обеспечивает подготовку обучающегося к аудиторным занятиям и мероприятиям текущего контроля и промежуточной аттестации по изучаемой дисциплине. Результаты этой подготовки проявляются в активности обучающегося на занятиях и в качестве выполненных практических заданий и других форм текущего контроля.

При выполнении заданий для самостоятельной работы рекомендуется проработка материалов лекций по каждой пройденной теме, а также изучение рекомендуемой литературы.

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья большое значение имеет индивидуальная учебная работа (консультации) – дополнительное разъяснение учебного материала.

Индивидуальные консультации по предмету являются важным фактором, способствующим индивидуализации обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или лицом с ограниченными возможностями здоровья.

6. Материально-техническое и учебно-методическое обеспечение по дисциплине (модулю)

Основная литература:

1. Хлебников, А.А., Информационные технологии : учебник / А.А. Хлебников. — Москва : КноРус, 2022. — 465 с. — ISBN 978-5-406-08923-1. — URL:https://book.ru/book/942103 . — Текст : электронный.

2. Информационные технологии в юридической деятельности : учебник для вузов / под общей редакцией П. У. Кузнецова. — 5-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 396 с. — (Высшее образование). — ISBN 978-5-534-20461-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/582670.

3. Информационные технологии в юридической деятельности : учебник и практикум для вузов / под редакцией В. Д. Элькина. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2026. — 472 с. — (Высшее образование). — ISBN 978-5-534-12733-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/582601.

4. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. с. 2 — URL: https://urait.ru/bcode/530927/p.2

5. Иванова, Л. И. Информационные технологии в юридической деятельности : учебное пособие / Л. И. Иванова, К. К. Сирбиладзе, О. Н. Цветкова. — Москва : КноРус, 2023. — 284 с. — ISBN 978-5-406-11871-9. — URL: https://book.ru/book/949879.

6. Шаблинский, И. Г. Правовое регулирование информационных отношений в сфере обработки персональных данных: учебное пособие для вузов / И. Г. Шаблинский ; под редакцией М. А. Федотова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 52 с. — (Высшее образование). — ISBN 978-5-534-17209-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/532609 .

Дополнительная литература

1. Информационное право : учебник для вузов / под редакцией Н. Н. Ковалевой. — Москва : Издательство Юрайт, 2025. — 353 с. — (Высшее образование). — ISBN 978-5-534-13786-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/567645.

2. Волков, А. М. Правовое обеспечение профессиональной деятельности в IT-сфере. Схемы, таблицы, определения, комментарии : учебник для вузов / А. М. Волков, Е. А. Лютягина. — Москва : Издательство Юрайт, 2026. — 281 с. — (Высшее образование). — ISBN 978-5-534-14114-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/588626

Интернет-ресурсы, в том числе современные профессиональные базы данных и информационные справочные системы

Электронно-библиотечные системы (ЭБС) и базы данных

Доступ к ЭБС предоставляется из любой точки, в которой имеется доступ к сети «Интернет», как на территории Института, так и вне ее (удаленный доступ).

1. Образовательная платформа «ЮРАЙТ» - URL: https://urait.ru/
2. Электронно-библиотечная система «BOOK.ru» - URL: https://www.book.ru.
3. Научная электронная библиотека eLIBRARY.RU - URL: https://elibrary.ru (крупнейшая российская база научных публикаций, доступ к рефератам и полным текстам статей).
4. КиберЛенинка - URL: https://cyberleninka.ru (научная электронная библиотека открытого доступа).

Информационные справочные системы

Справочная правовая система «Консультант Плюс» - доступ по локальной сети с

компьютеров библиотеки и компьютерных классов.

Профессиональные базы данных и ресурсы свободного доступа

Официальные органы государственной власти и управления

1. Министерство науки и высшего образования РФ https://m.minobrnauki.gov.ru/
2. Министерство экономического развития РФ https://www.economy.gov.ru
3. Министерство цифрового развития, связи и массовых коммуникаций РФ https://digital.gov.ru
4. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) https://rkn.gov.ru
5. Федеральное агентство по техническому регулированию и метрологии (Росстандарт) https://www.rst.gov.ru

Профессиональные сообщества, ассоциации и порталы

1. Ассоциация Менеджеров России https://amr.ru
2. Федеральный образовательный портал «Экономика. Социология. Менеджмент» http://ecsocman.hse.ru
3. Портал «Мой бизнес» https://xn--90aifddrld7a.xn--p1ai
4. База данных «Библиотека управления» (Корпоративный менеджмент) https://www.cfin.ru/rubricator.shtml
5. Habr https://habr.com
6. Stack Overflow https://stackoverflow.com
7. MDN Web Docs https://developer.mozilla.org
8. GitHub https://github.com
9. CodeProject https://www.codeproject.com
10. Microsoft Learn https://learn.microsoft.com

Международные научные и академические ресурсы (открытый доступ)

1. IEEE Xplore https://ieeexplore.ieee.org
2. Wiley Online Library https://onlinelibrary.wiley.com/
3. Архив журналов РАН (Издательство «Наука») http://www.libnauka.ru
4. ACM Digital Library https://dl.acm.org
5. SpringerLink https://link.springer.com

Комплект лицензионного и свободно распространяемого программного обеспечения:

1. LibreOffice - офисный пакет
2. PDFedit – программа для работы с pdf
3. Yandex Browser – браузер
4. Менеджер архивов
5. Libre Base – программа для работы с БД
6. Inkscape – ПО для компьютерной графики
7. DIA – ПО для блока схем и диаграмм
8. GiMP - Программа обработки изображений

Перечень материально-технического обеспечения включает:

учебные аудитории для проведения занятий лекционного типа, занятий практического (семинарского) типа, групповых и индивидуальных консультаций, текущего контроля и

промежуточной аттестации, а также помещения для самостоятельной работы оснащенные компьютерной техникой с подключением к сети "Интернет" и доступом в электронную информационно-образовательную среду Института.

Наименование помещения. Перечень основного оборудования	Адрес
Учебная аудитория № 304 (компьютерный класс) Учебная аудитория для проведения занятий лекционного и практического типа, выполнения курсовых работ, групповых и индивидуальных консультаций, текущего контроля, промежуточной аттестации. Оборудование: рабочее место преподавателя (1); рабочие места обучающихся (25); персональный компьютер с лицензионным ПО и возможностью выхода в интернет (26); мультимедийное оборудование (1); доска учебная (1); книжный шкаф (1); сплит-система (1); учебно-наглядные пособия; доступ в электронную информационно-образовательную среду Института.	350002, Краснодарский край, г. Краснодар, Центральный внутригородской округ, ул. им. Леваневского, д. 187/1
Аудитория № 218 Помещение для самостоятельной работы обучающихся Оборудование: рабочие места обучающихся (17); персональный компьютер с лицензионным ПО и возможностью выхода в Интернет (17); книжный шкаф (1); сплит-система (1); учебно-наглядные пособия; доступ в электронную информационно-образовательную среду Института.	350002, Краснодарский край, г. Краснодар, Центральный внутригородской округ, ул. им. Леваневского, д. 187/1