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.В.12 Кибербезопасность и защита информации в уголовном праве

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.В.12 «Кибербезопасность и защита информации в уголовном праве» 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.В.12 «Кибербезопасность и защита информации в уголовном праве» является формирование у обучающихся профессиональной компетенции ПК-11 (способность использовать в профессиональной деятельности методы защиты систем от кибератак), а также комплексного представления о правовых, организационных и технических аспектах обеспечения кибербезопасности в уголовно-правовой сфере, методах выявления, предупреждения и расследования киберпреступлений, особенностях защиты информации в деятельности правоохранительных органов, судов, следственных органов и иных участников уголовного судопроизводства.

1.2 Задачи дисциплины

1. Изучить правовые основы кибербезопасности и защиты информации в уголовно-правовой сфере (УК РФ, УПК РФ, ФЗ «О безопасности», ФЗ «Об информации», ФЗ «О персональных данных», Доктрина информационной безопасности РФ).
2. Сформировать понимание системы киберпреступлений (глава 28 УК РФ), их классификации, способов совершения, механизмов выявления и расследования.
3. Освоить методы и средства защиты информационных систем правоохранительных органов от кибератак: межсетевые экраны, системы обнаружения вторжений (IDS/IPS), антивирусная защита, криптографическая защита.
4. Научить применять методы расследования киберпреступлений: осмотр компьютерной техники, изъятие цифровых следов, анализ логов, восстановление удаленной информации.
5. Сформировать навыки работы со специализированным программно-аппаратным обеспечением для защиты информации и расследования инцидентов в правоохранительной сфере.
6. Изучить особенности обеспечения кибербезопасности в судебной системе, следственных органах, органах прокуратуры, МВД, ФСБ, ФСИН.

1.3 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Б1.В.12 «Кибербезопасность и защита информации в уголовном праве» относится к части, формируемой участниками образовательных отношений Блока 1 «Дисциплины (модули)» учебного плана.

В соответствии с рабочим учебным планом дисциплина изучается на 4 курсе по очной, очно-заочной и заочной формах обучения.

Вид промежуточной аттестации: экзамен.

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
ПК-11. Способен использовать в профессиональной деятельности методы защиты систем от кибератак	ПК-11.1. Знает: Основы кибербезопасности ПК-11.2. Умеет: Расследовать киберпреступления, (взломы,	**Знать:** правовые основы кибербезопасности в РФ (УК РФ глава 28, УПК РФ, ФЗ «О безопасности», ФЗ «Об

Код и наименование компетенции	Код и наименование индикаторов достижения результатов обучения по дисциплине	Планируемые результаты обучения
	мошенничество, распространение вредоносного ПО) ПК-11.3. Владеет: Методами защиты систем от кибератак	информации», Доктрина информационной безопасности РФ, приказы ФСТЭК, ФСБ, МВД); классификацию киберугроз и кибератак (DDoS, фишинг, вредоносное ПО, MITM, атаки на web-приложения, социальная инженерия); методы и средства защиты систем от кибератак: межсетевые экраны, IDS/IPS, антивирусные средства, средства криптографической защиты информации (СКЗИ); основы расследования киберпреступлений: порядок осмотра компьютерной техники, изъятия цифровых следов, анализа логов, восстановления удаленной информации; особенности обеспечения кибербезопасности в правоохранительных органах, судах, следственных органах. **Уметь:** выявлять признаки совершения киберпреступлений и фиксировать цифровые следы в соответствии с требованиями УПК РФ; проводить осмотр компьютерной техники, изымать электронные носители информации, копировать данные с соблюдением процессуальных норм; анализировать логи систем, сетевой трафик, метаданные файлов для установления обстоятельств совершения кибератаки; применять методы восстановления удаленной, зашифрованной, поврежденной информации; использовать специализированное ПО для расследования киберпреступлений (анализаторы трафика, криминалистические копировщики, инструменты для извлечения артефактов). **Владеть:** навыками настройки и эксплуатации средств защиты информации (межсетевые экраны, IDS/IPS, антивирусная защита); навыками выявления и анализа кибератак с использованием систем мониторинга и SIEM; навыками проведения мероприятий по локализации и ликвидации последствий кибератак; навыками применения методов криптографической защиты

Код и наименование компетенции	Код и наименование индикаторов достижения результатов обучения по дисциплине	Планируемые результаты обучения
		информации (шифрование, ЭП) в правоохранительной деятельности; навыками составления процессуальных документов по фактам киберпреступлений (протоколы осмотра, постановления о назначении экспертиз).

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 5 зачетных единиц (180 час.), их распределение по видам работ представлено в таблице

Виды работ		Всего часов		
		ОФО	ОЗФО	ЗФО
Контактная работа, в том числе:		**58**	**58**	10
Аудиторные занятия (всего):		**58**	**58**	10
занятия лекционного типа		22	22	4
практические занятия		36	36	6
Иная контактная работа:		**-**	**-**	**-**
Контрольная работа		**-**	**-**	**-**
Курсовая работа		**-**	**-**	**-**
Самостоятельная работа, в том числе:		**86**	**86**	**161**
Самоподготовка по темам (разделам) дисциплины		66	66	**141**
Подготовка к текущему контролю		20	20	**20**
Контроль:		**36**	**36**	**9**
Промежуточная аттестация (экзамен)		36	36	**9**
Общая трудоемкость	**час.**	**180**	**180**	**180**
	в том числе контактная работа	**58**	**58**	**10**
	зач. ед	**5**	**5**	**5**

2.2 Содержание дисциплины

Распределение видов учебной работы и их трудоемкости по разделам дисциплины.

Разделы (темы) дисциплины, изучаемые на 4 курсе (очная форма обучения)

№	Наименование темы/раздела	Количество часов

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

		Всего	В том числе в виде практической подготовки	Аудиторная работа		Внеаудиторная работа (СР)
				Л	ПЗ	
1	Раздел 1 **Правовые основы кибербезопасности в уголовно-правовой сфере РФ.** Доктрина информационной безопасности. УК РФ глава 28. УПК РФ. ФЗ «О безопасности», «Об информации».	18	-	4	4	10
2	Раздел 2. **Классификация киберугроз и кибератак.** Виды угроз, векторы атак. Вредоносное ПО. Социальная инженерия. Фишинг. DDoS. MITM.	18	-	4	4	10
3	Раздел 3. **Методы и средства защиты систем от кибератак.** Межсетевые экраны (фаерволы). IDS/IPS (системы обнаружения/предотвращения вторжений). Антивирусная защита. SIEM-системы.	18	-	4	4	10
4	Раздел 4. **Криптографическая защита информации в уголовном праве.** СКЗИ. Шифрование. Электронная подпись. Порядок применения в правоохранительных органах.	18	-	2	6	10
5	Раздел **5. Преступления в сфере компьютерной информации (глава 28 УК РФ).** Ст. 272, 273, 274, 274.1, 274.2. Составы, квалификация, судебная практика.	18	-	2	6	10
6	Раздел **6. Расследование киберпреступлений.** Осмотр компьютерной техники. Изъятие цифровых следов. Анализ логов. Восстановление удаленной информации.	18	-	2	4	12
7	Раздел 7. **Обеспечение кибербезопасности в правоохранительных органах.** Защита ИС МВД, ФСБ, СК, прокуратуры, ФСИН, судов. Требования ФСТЭК, ФСБ.	18	-	2	4	12
8	Раздел 8. **Судебная компьютерно-техническая экспертиза (СКТЭ).** Виды, вопросы, методики. Взаимодействие следователя с экспертом.	18	-	2	4	12
	ИТОГО по разделам дисциплины	144	-	22	36	86
	Контрольная работа	-	-	-	-	-
	Курсовая работа	-	-	-	-	-
	Промежуточная аттестация (экзамен)	36	-	-	-	-
	Общая трудоемкость по дисциплине	180	-	22	36	86

Разделы (темы) дисциплины, изучаемые на 4 курсе (очно-заочная форма обучения)

№	Наименование темы/раздела	Количество часов

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

		Всего	В том числе в виде практической подготовки	Аудиторная работа		Внеаудиторная работа (СР)
				Л	ПЗ	
1	Раздел 1 **Правовые основы кибербезопасности в уголовно-правовой сфере РФ.** Доктрина информационной безопасности. УК РФ глава 28. УПК РФ. ФЗ «О безопасности», «Об информации».	18	-	4	4	10
2	Раздел 2. **Классификация киберугроз и кибератак.** Виды угроз, векторы атак. Вредоносное ПО. Социальная инженерия. Фишинг. DDoS. MITM.	18	-	4	4	10
3	Раздел 3. **Методы и средства защиты систем от кибератак.** Межсетевые экраны (фаерволы). IDS/IPS (системы обнаружения/предотвращения вторжений). Антивирусная защита. SIEM-системы.	18	-	4	4	10
4	Раздел 4. **Криптографическая защита информации в уголовном праве.** СКЗИ. Шифрование. Электронная подпись. Порядок применения в правоохранительных органах.	18	-	2	6	10
5	Раздел **5. Преступления в сфере компьютерной информации (глава 28 УК РФ).** Ст. 272, 273, 274, 274.1, 274.2. Составы, квалификация, судебная практика.	18	-	2	6	10
6	Раздел **6. Расследование киберпреступлений.** Осмотр компьютерной техники. Изъятие цифровых следов. Анализ логов. Восстановление удаленной информации.	18	-	2	4	12
7	Раздел 7. **Обеспечение кибербезопасности в правоохранительных органах.** Защита ИС МВД, ФСБ, СК, прокуратуры, ФСИН, судов. Требования ФСТЭК, ФСБ.	18	-	2	4	12
8	Раздел 8. **Судебная компьютерно-техническая экспертиза (СКТЭ).** Виды, вопросы, методики. Взаимодействие следователя с экспертом.	18	-	2	4	12
	ИТОГО по разделам дисциплины	144	-	22	36	86
	Контрольная работа	-	-	-	-	-
	Курсовая работа	-	-	-	-	-
	Промежуточная аттестация (экзамен)	36	-	-	-	-
	Общая трудоемкость по дисциплине	180	-	22	36	86

Разделы (темы) дисциплины, изучаемые на 4 курсе (заочная форма обучения)

№	Наименование темы/раздела	Количество часов

ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ В ПРАВОВОЙ ДЕЯТЕЛЬНОСТИ

09.03.02 Информационные системы и технологии

2026 год набора

		Всего	В том числе в виде практической подготовки	Аудиторная работа		Внеаудиторная работа (СР)
				Л	ПЗ	
1	Раздел 1 **Правовые основы кибербезопасности в уголовно-правовой сфере РФ.** Доктрина информационной безопасности. УК РФ глава 28. УПК РФ. ФЗ «О безопасности», «Об информации».	22	-	1	-	21
2	Раздел 2. **Классификация киберугроз и кибератак.** Виды угроз, векторы атак. Вредоносное ПО. Социальная инженерия. Фишинг. DDoS. MITM.	21	-	1	-	20
3	Раздел 3. **Методы и средства защиты систем от кибератак.** Межсетевые экраны (фаерволы). IDS/IPS (системы обнаружения/предотвращения вторжений). Антивирусная защита. SIEM-системы.	21	-	1	-	20
4	Раздел 4. **Криптографическая защита информации в уголовном праве.** СКЗИ. Шифрование. Электронная подпись. Порядок применения в правоохранительных органах.	21	-	1	-	20
5	Раздел **5. Преступления в сфере компьютерной информации (глава 28 УК РФ).** Ст. 272, 273, 274, 274.1, 274.2. Составы, квалификация, судебная практика.	22	-	-	2	20
6	Раздел **6. Расследование киберпреступлений.** Осмотр компьютерной техники. Изъятие цифровых следов. Анализ логов. Восстановление удаленной информации.	21	-	-	1	20
7	Раздел 7. **Обеспечение кибербезопасности в правоохранительных органах.** Защита ИС МВД, ФСБ, СК, прокуратуры, ФСИН, судов. Требования ФСТЭК, ФСБ.	21	-	-	1	20
8	Раздел 8. **Судебная компьютерно-техническая экспертиза (СКТЭ).** Виды, вопросы, методики. Взаимодействие следователя с экспертом.	22	-	-	2	20
	ИТОГО по разделам дисциплины	171	-	4	6	161
	Контрольная работа	-	-	-	-	-
	Курсовая работа	-	-	-	-	-
	Промежуточная аттестация (экзамен)	9	-	-	-	-
	Общая трудоемкость по дисциплине	180	-	4	6	161

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 и т.д.

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.В.12 Кибербезопасность и защита информации в уголовном праве» 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)

Оценочные средства предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины Б1.В.12 «Кибербезопасность и защита информации в уголовном праве». Материалы для проведения текущего контроля успеваемости и промежуточной аттестации размещены в фонде оценочных средств по дисциплине Б1.В.12 «Кибербезопасность и защита информации в уголовном праве».

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	ПК-11.1. Знает: Основы кибербезопасности	**Знать:** правовые основы кибербезопасности в РФ (УК РФ глава 28, УПК РФ, ФЗ «О безопасности», ФЗ «Об информации», Доктрина информационной безопасности	Подготовка докладов/сообщений, вопросы для обсуждения по темам, задания открытого и закрытого типа	Вопросы на экзамене

2	ПК-11.2. Умеет: Расследовать киберпреступления, (взломы, мошенничество, распространение вредоносного ПО)	РФ, приказы ФСТЭК, ФСБ, МВД); классификацию киберугроз и кибератак (DDoS, фишинг, вредоносное ПО, MITM, атаки на web-приложения, социальная инженерия); методы и средства защиты систем от кибератак: межсетевые экраны, IDS/IPS, антивирусные средства, средства криптографической защиты информации (СКЗИ); основы расследования киберпреступлений: порядок осмотра компьютерной техники, изъятия цифровых следов, анализа логов, восстановления удаленной информации; особенности обеспечения кибербезопасности в правоохранительных органах, судах, следственных органах. **Уметь:** выявлять признаки совершения киберпреступлений и фиксировать цифровые следы в соответствии с требованиями УПК РФ; проводить осмотр компьютерной техники, изымать электронные носители информации, копировать данные с соблюдением процессуальных норм; анализировать логи систем, сетевой трафик, метаданные файлов для установления обстоятельств совершения кибератаки; применять методы восстановления удаленной, зашифрованной, поврежденной информации; использовать специализированное ПО для расследования киберпреступлений (анализаторы трафика, криминалистические копировщики, инструменты для извлечения артефактов). **Владеть:** навыками настройки и эксплуатации средств защиты информации (межсетевые экраны, IDS/IPS, антивирусная защита); навыками выявления и анализа кибератак с использованием систем мониторинга и SIEM; навыками проведения мероприятий по локализации и	Подготовка докладов/сообщений, вопросы для обсуждения по темам, задания открытого и закрытого типа	Вопросы на экзамене
3	ПК-11.3. Владеет: Методами защиты систем от кибератак		Подготовка докладов/сообщений, вопросы для обсуждения по темам, задания открытого и закрытого типа	Вопросы на экзамене

		ликвидации последствий кибератак; навыками применения методов криптографической защиты информации (шифрование, ЭП) в правоохранительной деятельности; навыками составления процессуальных документов по фактам киберпреступлений (протоколы осмотра, постановления о назначении экспертиз).		

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. Доктрина информационной безопасности РФ: основные угрозы и направления защиты.
2. Сравнительный анализ составов преступлений, предусмотренных ст. 272, 273, 274 УК РФ.
3. Методы выявления и предупреждения фишинговых атак.
4. Особенности осмотра компьютерной техники при расследовании киберпреступлений (ст. 176.1, 177 УПК РФ).
5. Средства криптографической защиты информации в деятельности правоохранительных органов.
6. Системы обнаружения вторжений (IDS/IPS): классификация, принципы работы, применение.
7. Судебная компьютерно-техническая экспертиза: виды и методики.
8. Особенности обеспечения кибербезопасности в судебной системе (ГАС «Правосудие»).
9. Анализ логов как метод расследования кибератак.
10. Проблемы доказывания по делам о преступлениях в сфере компьютерной информации.

Тестовые задания (открытого типа)

1. Совокупность правовых, организационных и технических мер, направленных на защиту информационных систем, сетей и данных от кибератак, называется _____.

Ответ: «кибербезопасность».

2. Вид вредоносного ПО, которое блокирует доступ к данным пользователя и требует выкуп за их расшифровку, называется _____.

Ответ: «программа-шифровальщик (ransomware)».

3. Система, осуществляющая централизованный сбор, корреляцию и анализ событий информационной безопасности, называется _____.

Ответ: «SIEM (Security Information and Event Management)».

Кейс-задача

Кейс «Анализ кибератаки на сервер суда»

В районном суде был осуществлен несанкционированный доступ к серверу с базами данных. Злоумышленник скопировал персональные данные участников судебных процессов. Обнаружено, что атака была проведена через уязвимость в веб-интерфейсе системы, без использования вредоносного ПО, в ночное время с IP-адреса, зарегистрированного на подставное лицо.

Вопросы:

1. Какой состав преступления усматривается? Квалифицируйте по ст. 272 УК РФ.
2. Каков порядок осмотра компьютерной техники (ст. 176.1, 177 УПК РФ)?
3. Какие цифровые следы необходимо зафиксировать?
4. Какие вопросы следует поставить перед компьютерно-технической экспертизой?

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 (экзамен)

Теоретические вопросы к экзамену

1. Доктрина информационной безопасности РФ: структура, основные угрозы, направления защиты.
2. Понятие и виды киберпреступлений в уголовном праве РФ (общая характеристика главы 28 УК РФ).
3. Неправомерный доступ к компьютерной информации (ст. 272 УК РФ): объект, объективная сторона, субъект, субъективная сторона.
4. Квалифицирующие признаки ст. 272 УК РФ. Отграничение от смежных составов.
5. Создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ).
6. Понятие и классификация вредоносного ПО (вирусы, трояны, программы-шпионы, шифровальщики).
7. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации (ст. 274 УК РФ).
8. Неправомерное воздействие на критическую информационную инфраструктуру РФ (ст. 274.1 УК РФ).
9. Проблемы квалификации преступлений в сфере компьютерной информации. Судебная практика.
10. Особенности собирания электронных доказательств по УПК РФ (ст. 164.1, 164.2, 176.1, 177, 204).
11. Порядок осмотра компьютерной техники: участники, технические средства, фиксация.
12. Порядок изъятия цифровых следов: копирование, создание образов, упаковка.
13. Анализ логов как метод расследования кибератак.
14. Восстановление удаленной, зашифрованной, поврежденной информации: методы и средства.
15. Понятие и виды судебной компьютерно-технической экспертизы (СКТЭ).
16. Вопросы, разрешаемые судебной компьютерно-технической экспертизой.

17. Взаимодействие следователя с экспертом: постановка вопросов, предоставление объектов, оценка заключения.
18. Межсетевые экраны (фаерволы): виды, правила фильтрации, топологии развертывания.
19. Системы обнаружения и предотвращения вторжений (IDS/IPS): классификация, принципы работы.
20. Антивирусная защита: сигнатурный и эвристический анализ, поведенческие детекторы, песочницы.
21. SIEM-системы: назначение, архитектура, функции.
22. Средства криптографической защиты информации (СКЗИ): классификация, требования ФСБ России.
23. Правовое регулирование кибербезопасности в правоохранительных органах (требования ФСТЭК, ФСБ, МВД).
24. Обеспечение кибербезопасности в судебной системе: ГАС «Правосудие», электронное правосудие.
25. Обеспечение кибербезопасности в учреждениях ФСИН, прокуратуре, Следственном комитете.

Практические задания к экзамену

Задача 1. Квалификация кибератаки

Гражданин Иванов, используя вредоносную программу, полученную через фишинговое письмо, получил несанкционированный доступ к базе данных персональных пациентов частной клиники. Он скопировал информацию (ФИО, адреса, диагнозы) и передал третьим лицам за вознаграждение. Действия Иванова повлекли крупный ущерб (свыше 1 млн руб.) и нарушение прав более 500 граждан.

Вопросы:

1. Квалифицируйте действия Иванова по УК РФ (ст. 272, 137, 183, 272?).
2. Какие последствия подлежат доказыванию?
3. Каков порядок назначения компьютерно-технической экспертизы?
4. Какие вопросы следует поставить перед экспертом?

Задача 2. Осмотр компьютерной техники

В ходе расследования уголовного дела по ст. 272 УК РФ следователь прибыл для осмотра системного блока компьютера, с которого предположительно осуществлялся неправомерный доступ. Системный блок находится в рабочем состоянии, включен. Следователь не имеет специалиста.

Вопросы:

1. Допустим ли осмотр без специалиста?
2. Каков порядок осмотра компьютерной техники (ст. 176.1, 177 УПК РФ)?
3. Кто должен участвовать в осмотре?
4. В каком порядке следует изымать информацию?
5. Какие процессуальные документы составляются?

Задача 3. Анализ логов сервера

Вам предоставлен фрагмент логов веб-сервера суда, где зафиксирована подозрительная активность: множественные попытки авторизации с различных IP-адресов, переходы к несуществующим страницам, передача больших объемов данных.

Вопросы:

1. Какой тип атаки наиболее вероятен?
2. Какие признаки (индикаторы компрометации) усматриваются?
3. Каким образом можно установить источник атаки?

4. Как оформить результаты анализа в качестве доказательства?

Задача 4. Назначение компьютерно-технической экспертизы

По уголовному делу о распространении вредоносного ПО изъят жесткий диск с компьютера обвиняемого. На диске могут находиться исходные коды вредоносной программы, переписка с соучастниками, следы компиляции.

Вопросы:

1. Какой вид компьютерно-технической экспертизы следует назначить (программно-компьютерная, информационно-компьютерная)?
2. Какие вопросы следует поставить перед экспертом?
3. Какие образцы (сравнительные материалы) необходимо предоставить?
4. Каков порядок назначения экспертизы (постановление, выбор экспертного учреждения)?

Задача 5. Настройка межсетевого экрана

Для информационной системы районного суда необходимо настроить межсетевой экран. ИС имеет выход в Интернет, подключена к ведомственной сети, содержит персональные данные участников процессов. Разработайте:

Вопросы:

1. Класс защищенности ИСПДн для данной системы.
2. Требования к межсетевому экрану (сертификация ФСТЭК).
3. Правила фильтрации для входящего и исходящего трафика.
4. Меры по защите от DDoS-атак.

Задача 6. Восстановление удаленных данных

При осмотре компьютера обвиняемого по ст. 273 УК РФ обнаружено, что важные файлы (исходные коды вредоносной программы, переписка) были удалены с использованием штатных средств ОС, а также программами-уничтожителями.

Вопросы:

1. Какие методы восстановления удаленной информации могут быть применены?
2. Какова вероятность восстановления при использовании программ-уничтожителей?
3. Какие программные средства используются для восстановления?
4. Как обеспечить процессуальную допустимость восстановленных данных?

Задача 7. Реагирование на инцидент ИБ

В судебной информационной системе обнаружены признаки компрометации: медленная работа, подозрительные сетевые соединения, появление неизвестных файлов.

Вопросы:

1. Каков алгоритм реагирования на инцидент (шаги, ответственные)?
2. Кто должен быть уведомлен (руководство, ФСТЭК, прокуратура)?
3. Какие меры по локализации и ликвидации последствий необходимо принять?
4. Какие изменения в регламентах информационной безопасности следует внести после инцидента?

Задача 8. Судебная практика по киберпреступлениям

Проанализируйте предложенный приговор суда по делу о совершении преступления, предусмотренного ч. 2 ст. 272 УК РФ (приговор предоставляется). Выполните:

Вопросы:

1. Квалифицируйте содеянное (объект, объективная сторона, субъект, субъективная сторона).
2. Какие доказательства были положены в основу приговора (электронные, вещественные, свидетельские показания)?
3. Какие нарушения уголовно-процессуального закона допущены (если есть)?
4. Согласны ли вы с решением суда? Аргументируйте.

Критерии оценивания промежуточной аттестации: экзамен

Оценка	Критерии оценивания по экзамену
Высокий уровень «5» (отлично)	Обучающийся полностью освоил компетенцию ПК-11. Дает развернутые ответы на теоретические вопросы со ссылками на конкретные статьи УК РФ, УПК РФ, нормативные акты; правильно квалифицирует киберпреступления; демонстрирует умение проводить осмотр компьютерной техники, анализировать логи, восстанавливать данные; обосновывает выбор средств защиты информации; правильно решает практические задачи.
Средний уровень «4» (хорошо)	Обучающийся в основном освоил компетенцию ПК-11. Дает достаточно полные ответы на теоретические вопросы, решает практические задачи с незначительными ошибками, умеет квалифицировать киберпреступления, но испытывает трудности при анализе логов или восстановлении данных.
Пороговый уровень «3» (удовлетворительно)	Обучающийся частично освоил компетенцию ПК-11. Допускает существенные ошибки в теоретических вопросах, испытывает значительные трудности при решении практических задач, слабо ориентируется в методах защиты и расследования кибератак.
Минимальный уровень «2» (неудовлетворительно)	Обучающийся не освоил компетенцию ПК-11. Не может ответить на теоретические вопросы, не квалифицирует киберпреступления, не владеет методами защиты и расследования, не решает практические задачи.

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. *Зенков, А. В.* 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]. — URL: https://urait.ru/bcode/530927.

2. Корабельников, С. М. Преступления в сфере информационной безопасности: учебное пособие для вузов / С. М. Корабельников. — Москва: Издательство Юрайт, 2026. — 111 с. — (Высшее образование). — ISBN 978-5-534-12769-0. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/588094.

3. Бабаш, А. В. Криптографические методы защиты информации: учебник / А. В. Бабаш, Е. К. Баранова. — Москва: КноРус, 2026. — 189 с. — ISBN 978-5-406-14904-1. — URL: https://book.ru/book/959208.

4. 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.

5. Внуков, А. А. Защита информации в банковских системах: учебник для вузов / А. А. Внуков. — 2-е изд., испр. и доп. — Москва: Издательство Юрайт, 2026. — 246 с. — (Высшее образование). — ISBN 978-5-534-01679-6. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/584051.

6. Васильева, И. Н. Криптографические методы защиты информации: учебник и практикум для вузов / И. Н. Васильева. — Москва: Издательство Юрайт, 2026. — 310 с. — (Высшее образование). — ISBN 978-5-534-02883-6. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/583783.

Дополнительная литература

1. Смушкин, А. Б. Криминалистические аспекты использования киберпространства и обеспечения кибербезопасности: монография / А. Б. Смушкин; под ред. В. Б. Вехова. — Москва: Русайнс, 2024. — 195 с. — ISBN 978-5-466-08332-3. — URL: https://book.ru/book/956551.

2. Ковалева, Н. Н. Информационное обеспечение органов власти: учебник для вузов / Н. Н. Ковалева. — 2-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2026. — 245 с. — (Высшее образование). — ISBN 978-5-534-13291-5. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/587992.

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

Нормативные правовые акты

1. Уголовный кодекс Российской Федерации (глава 28 «Преступления в сфере компьютерной информации»).
2. Уголовно-процессуальный кодекс Российской Федерации (ст. 164.1, 164.2, 176.1, 177, 204).
3. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 05.12.2016 № 646).
4. Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности».
5. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
6. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
7. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
8. Федеральный закон от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг».
9. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации...».
10. Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по защите информации...».

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
6. Официальный сайт ФСТЭК России — https://fstec.ru (требования к защите информации)
7. Официальный сайт ФСБ России — https://www.fsb.ru (сертификация СКЗИ, криптозащита)

8. Официальный сайт МВД России — https://мвд.рф (отчеты о киберпреступности)
9. Государственная автоматизированная система «Правосудие» — https://sudrf.ru (судебная практика)
10. Портал «Мой арбитр» — https://my.arbitr.ru (электронное правосудие)

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 № 215 (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 сеть "Интернет" (26); мультимедийное оборудование (1); доска учебная (1); книжный шкаф (1); сплит-система(1); учебно-наглядные пособия; доступ в электронную информационно-образовательную среду Института. Программное обеспечение: LibreOffice - офисный пакет PDFedit – программа для работы с pdf Yandex Browser – браузер Менеджер архивов	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