**КАЗАНСКИЙ КООПЕРАТИВНЫЙ ИНСТИТУТ (ФИЛИАЛ)
АВТОНОМНОЙ НЕКОММЕРЧЕСКОЙ ОБРАЗОВАТЕЛЬНОЙ
ОРГАНИЗАЦИИ ВЫСШЕГО ОБРАЗОВАНИЯ
ЦЕНТРОСОЮЗА РОССИЙСКОЙ ФЕДЕРАЦИИ
«РОССИЙСКИЙ УНИВЕРСИТЕТ КООПЕРАЦИИ»**

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ В КОМПЬЮТЕРНЫХ СИСТЕМАХ И СЕТЯХ

Специальность: 10.05.01 Компьютерная безопасность
Специализация: «Разработка защищенного программного обеспечения»
Формы обучения: очная
Объем дисциплины:
в зачетных единицах: 3 з.е.
в академических часах: 108 ак.ч.

Форма промежуточной аттестации: зачет

2025

Рабочая программа по дисциплине «Компьютерные преступления в компьютерных системах и сетях» по специальности 10.05.01 Компьютерная безопасность, специализации «Разработка защищенного программного обеспечения», составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования – специалитет по специальности 10.05.01 Компьютерная безопасность, утвержденного приказом Министерства науки и высшего образования Российской Федерации от «26» ноября 2020 г. № 1459, профессионального стандарта 06.032 «Специалист по безопасности компьютерных систем и сетей», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 г. № 533н, профессионального стандарта 06.033 «Специалист по защите информации в автоматизированных системах», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 г. №525н.

Рабочая программа:

обсуждена и рекомендована к утверждению решением кафедры гуманитарных дисциплин и иностранных языков от 21 марта 2025 г., протокол № 7

одобрена Научно-методическим советом Казанского кооперативного института (филиала) от «2» апреля 2025 г., протокол № 3.

СОДЕРЖАНИЕ

1. Цель и задачи освоения дисциплины

Цели определены государственным образовательным стандартом высшего профессионального образования и соотнесены с общими целями ООП ВО по специальности 10.05.01 Компьютерная безопасность, в рамках которой преподается дисциплина «Компьютерные преступления в компьютерных системах и сетях».

Целью освоения учебной дисциплины «Компьютерные преступления в компьютерных системах и сетях» является формирование у студентов современных знаний, навыков и компетенций в области уголовного права, посвященного компьютерным преступлениям, обеспечение усвоения поведенческих мотивов, целей, условий и механизмов совершения компьютерных преступлений, а также законодательных основ их предотвращения, предупреждения и расследования.

Задачи: привить навыки формирования требований по защите информации в различных КС, ознакомить с требованиями к защите автоматизированных информационных систем (ИС) от несанкционированного доступа (НСД) на территории Российской Федерации.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Компьютерные преступления в компьютерных системах и сетях» относится к части, формируемой участниками образовательных отношений Блока 1 «Дисциплины (модули)» основной образовательной программы – программы специалитета по специальности 10.05.01 Компьютерная безопасность специализация «Разработка защищенного программного обеспечения».

Код компетенции	Предшествующие дисциплины (модули), практики	Изучаемые в текущем семестре дисциплины (модули), практики	Последующие дисциплины (модули), практики
ПК-3.3 ПК-3.6	Основы облачных технологий Функциональное и логическое программирование Производственная практика, технологическая практика	**Компьютерные преступления в компьютерных системах и сетях** Проектирование организационно-распорядительных и эксплуатационно-технических документов в системах обеспечения информационной безопасности	Производственная практика, преддипломная практика

3. Перечень планируемых результатов обучения по дисциплине

Изучение дисциплины направлено на формирование у обучающихся компетенций.

Формируемые компетенции (код и наименование компетенции)	Индикаторы достижения компетенций	Планируемые результаты обучения
ПК-3.3 Способен участвовать в проведении экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов	ПК-3.3.1 Реализует технологии поиска и анализа следов компьютерных преступлений, правонарушений и инцидентов	Знать: методы анализа защищенности компьютерных систем и сетей с использованием сканеров безопасности с целью противодействия компьютерным преступлениям, осуществляемым с использованием вредоносного программного обеспечения Уметь: реализовывать анализ защищенности сетевых сервисов автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей Владеть: навыками структуризации аналитической информации для составления отчётов по результатам проверок качества противодействия информационным атакам и операциям, реализуемым в компьютерных системах и сетях
	ПК-3.3.2 Применяет методы и средства прогнозирования возможных путей развития новых видов компьютерных преступлений	Знать: методы анализа защищенности компьютерных систем и сетей с использованием сканеров безопасности с целью противодействия компьютерным преступлениям, осуществляемым с использованием вредоносного программного обеспечения Уметь: реализовывать анализ защищенности сетевых сервисов автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей Владеть: навыками структуризации аналитической информации для составления отчётов по результатам проверок качества противодействия информационным атакам и операциям, реализуемым в компьютерных системах и сетях
	ПК-3.3.3 выявление индивидуальных признаков программы, позволяющих впоследствии идентифицировать ее автора, а также взаимосвязи с информационным обеспечением исследуемой компьютерной системы	Знать: методы анализа защищенности компьютерных систем и сетей с использованием сканеров безопасности с целью противодействия компьютерным преступлениям, осуществляемым с использованием вредоносного программного обеспечения Уметь: реализовывать анализ защищенности сетевых сервисов автоматического

Формируемые компетенции (код и наименование компетенции)	Индикаторы достижения компетенций	Планируемые результаты обучения
		реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей Владеть: навыками структуризации аналитической информации для составления отчётов по результатам проверок качества противодействия информационным атакам и операциям, реализуемым в компьютерных системах и сетях
ПК-3.6 Способен участвовать в работах по противодействию информационным атакам и операциям, реализуемым в компьютерных системах и сетях	ПК-3.6.1 Выполняет анализ защищенности компьютерных систем и сетей с использованием сканеров безопасности	Знать: технологии поиска и анализа следов компьютерных преступлений, правонарушений и инцидентов Уметь: применять методы и средства прогнозирования возможных путей развития новых видов компьютерных преступлений Владеть: навыками выявления индивидуальных признаков программы, позволяющих впоследствии идентифицировать ее автора, а также взаимосвязи с информационным обеспечением исследуемой компьютерной системы с информационным обеспечением исследуемой компьютерной системы
	ПК-3.6.2 Реализует анализ защищенности сетевых сервисов автоматического реагирования на попытки несанкционированного доступа к ресурсам	Знать: технологии поиска и анализа следов компьютерных преступлений, правонарушений и инцидентов Уметь: применять методы и средства прогнозирования возможных путей развития новых видов компьютерных преступлений Владеть: навыками выявления индивидуальных признаков программы, позволяющих впоследствии идентифицировать ее автора, а также взаимосвязи с информационным обеспечением исследуемой компьютерной системы с информационным обеспечением исследуемой компьютерной системы
	ПК-3.6.3 Структурирует аналитическую информацию для составления отчётов по результатам проверок качества противодействия информационным атакам и операциям, реализуемым в компьютерных системах и сетях	Знать: технологии поиска и анализа следов компьютерных преступлений, правонарушений и инцидентов Уметь: применять методы и средства прогнозирования возможных путей развития новых видов компьютерных преступлений Владеть: навыками выявления индивидуальных признаков программы, позволяющих впоследствии идентифицировать ее автора, а также взаимосвязи с информационным обеспечением исследуемой

Формируемые компетенции (код и наименование компетенции)	Индикаторы достижения компетенций	Планируемые результаты обучения
		компьютерной системы с информационным обеспечением исследуемой компьютерной системы

4. Объем дисциплины и виды учебной работы

Объем дисциплины и виды учебной работы в академических часах с выделением объема контактной работы обучающихся с преподавателем и самостоятельной работы обучающихся

очная форма обучения

Вид учебной деятельности		ак.часов	
		Всего	По семестрам
			А
1. Контактная работа обучающихся с преподавателем:		51	51
Аудиторные занятия, часов всего, в том числе:		50	50
• занятия лекционного типа		34	34
• занятия семинарского типа:		16	16
практические занятия		-	-
лабораторные занятия		16	16
в том числе занятия в форме практической подготовки		-	-
Консультации		0,5	0,5
Контактные часы на аттестацию в период экзаменационных сессий		0,5	0,5
2. Самостоятельная работа студентов всего, в том числе		57	57
- подготовка курсовой работы		-	-
- проработка учебного (теоретического) материала		20	20
- выполнение домашних заданий по практическим занятиям		20	20
- подготовка к зачету с оценкой		17	17
Промежуточная аттестация: зачет с оценкой		-	-
ИТОГО:	часов	108	108
общая трудоемкость	зач. ед.	3	3

5. Содержание дисциплины, структурированное по темам (разделам) с указанием количества академических часов и видов учебных занятий

5.1. Содержание дисциплины

Тема 1. Основы компьютерных преступлений.

Понятие и виды компьютерных преступлений. Признаки, основные характеристики.

Тема 2. Расследование компьютерных преступлений

Обзор угроз безопасности компьютерных систем. Раскрытие и расследование компьютерных преступлений.

Тема 3. Противодействие компьютерным преступлениям, осуществляемым с использованием вредоносного программного обеспечения

Детальный анализ вредоносного программного обеспечения. Классификация ВПО. Эвристический анализ

Тема 4. Противодействие компьютерным преступлениям, реализуемым в ходе проведения компьютерных сетевых атак

Компьютерные сетевые атаки. Удаленные компьютерные сетевые атаки. Системы обнаружения вторжения и межсетевого экранирования.

Тема 5. Противодействие компьютерным преступлениям путем реализации политики безопасности

Анализ разрушающих воздействий. Методы обнаружения и борьбы. Политики безопасности. Организация сетевой политики безопасности.

Тема 6. Преступления в сфере компьютерной информации

Несанкционированный доступ к компьютерной информации. Незаконные использование и (или) передача, сбор и (или) хранение компьютерной информации, содержащей персональные данные.

Создание, использование и распространение вредоносных компьютерных программ. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и ИТКС. Неправомерное воздействие на КИИ РФ. Нарушение правил централизованного управления ТС противодействия угрозам устойчивости, безопасности и целостности функционирования на территории РФ ИТКС "Интернет" и сети связи общего пользования.

Тема 7. Компьютерные преступления, направленные на воздействие на критическую информационную инфраструктуру РФ

Создание, распространение и (или) использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на КИИ РФ. Неправомерный доступ к охраняемой компьютерной информации, содержащейся в КИИ РФ. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в КИИ РФ.

Тема 8. Судебная практика по компьютерным преступлениям

Приговоры, апелляционные, кассационные и надзорные судебные акты по рассмотренным преступлениям.

Тема 9. Предотвращение компьютерных преступлений

Превентивные методы. Способы предотвращения компьютерных преступлений.

5.2. Разделы, темы дисциплины и виды занятий

очная форма обучения

№ п/п	Наименование раздела, темы дисциплины	Виды занятий, включая самостоятельную работу студентов (в часах)			Индикаторы достижения компетенций
		занятия лекционного типа	занятия семинарского типа / из них в форме практической подготовки (лабораторные работы)	самостоятельная работа	
1	Тема 1. Основы компьютерных преступлений	4	2/2	6	ПК-3.3, ПК-3.3.1, ПК-3.3.2, ПК-3.3.3 ПК-3.6, ПК-3.6.1, ПК_3.6.2, ПК-3.6.3
2	Тема 2. Расследование компьютерных преступлений	4	2/2	6	ПК-3.3, ПК-3.3.1, ПК-3.3.2, ПК-3.3.3 ПК-3.6, ПК-3.6.1, ПК_3.6.2, ПК-3.6.3
3	Тема 3. Противодействие компьютерным преступлениям, осуществляемым с использованием вредоносного программного обеспечения	4	2/2	6	ПК-3.3, ПК-3.3.1, ПК-3.3.2, ПК-3.3.3 ПК-3.6, ПК-3.6.1, ПК_3.6.2, ПК-3.6.3
4	Тема 4. Противодействие компьютерным преступлениям, реализуемым в ходе проведения компьютерных сетевых атак	4	2/2	6	ПК-3.3, ПК-3.3.1, ПК-3.3.2, ПК-3.3.3 ПК-3.6, ПК-3.6.1, ПК_3.6.2, ПК-3.6.3
5	Тема 5. Противодействие компьютерным преступлениям путем реализации политики безопасности	4	2/2	6	ПК-3.3, ПК-3.3.1, ПК-3.3.2, ПК-3.3.3 ПК-3.6, ПК-3.6.1, ПК_3.6.2, ПК-3.6.3
6	Тема 6. Преступления в сфере компьютерной информации	4	2/2	6	ПК-3.3, ПК-3.3.1, ПК-3.3.2, ПК-3.3.3

№ п/п	Наименование раздела, темы дисциплины	Виды занятий, включая самостоятельную работу студентов (в часах)			Индикаторы достижения компетенций
		занятия лекционного типа	занятия семинарского типа / из них в форме практической подготовки (лабораторные работы)	самос-тоятельная работа	
7	Тема 7. Компьютерные преступления, направленные на воздействие на критическую информационную инфраструктуру РФ	4	2/2	6	ПК-3.6, ПК-3.6.1, ПК_3.6.2, ПК-3.6.3
8	Тема 8. Судебная практика по компьютерным преступлениям	4	2/2	6	ПК-3.3, ПК-3.3.1, ПК-3.3.2, ПК-3.3.3 ПК-3.6, ПК-3.6.1, ПК_3.6.2, ПК-3.6.3
9	Тема 9. Предотвращение компьютерных преступлений	2	-	9	ПК-3.3, ПК-3.3.1, ПК-3.3.2, ПК-3.3.3 ПК-3.6, ПК-3.6.1, ПК_3.6.2, ПК-3.6.3
	Всего	**34**	**16/16**	**57**	

6. Практические занятия

Практические занятия не предусмотрены.

7. Лабораторные работы

№ п/п	Наименование раздела, темы дисциплины	Содержание лабораторных работ	Объем (час.)
			Очная форма обучения
1.	Тема 1. Основы компьютерных преступлений	Классификация видов компьютерных преступлений: изучение основных категорий и типов компьютерных преступлений согласно законодательству РФ. Методы взлома компьютерных сетей и защита от них: практическое освоение методов выявления уязвимостей сетевых инфраструктур и способы защиты. Анализ вредоносного программного обеспечения: исследование структуры и функций вирусов, троянов, шпионских программ и других угроз информационной безопасности. Сбор цифровых доказательств компьютерного преступления: общие принципы и методы сбора электронных следов и цифровой информации.	2
2.	Тема 2. Расследование	Определение признаков состава преступления в сфере	2

№ п/п	Наименование раздела, темы дисциплины	Содержание лабораторных работ	Объем (час.)
			Очная форма обучения
	компьютерных преступлений	высоких технологий: определение квалификации уголовных деяний в области ИТ-правонарушений. Методология документирования и фиксации цифровых доказательств: порядок изъятия и закрепления доказательственных материалов при совершении киберпреступлений. Выявление следовых элементов при исследовании компьютерной техники подозреваемого лица: сбор цифровых следов, оставленных злоумышленником на устройстве жертвы	
3.	Тема 3. Противодействие компьютерным преступлениям, осуществляемым с использованием вредоносного программного обеспечения	Изучение классификации вредоносного ПО: анализ различных видов вредоносного программного обеспечения (вирусы, черви, трояны, руткиты). Методы обнаружения и идентификации вредоносного ПО: использование антивирусных сканеров и сигнатурных подходов для выявления зараженных объектов. Исследование механизмов распространения вредоносного ПО: изучение путей распространения вредоносных программ через электронную почту, веб-сайты, социальные сети и съемные носители.	2
4.	Тема 4. Противодействие компьютерным преступлениям, реализуемым в ходе проведения компьютерных сетевых атак	Работа с системами анализа трафика (IDS/IPS): применение межсетевых экранов и систем обнаружения вторжений для блокировки подозрительных пакетов данных. Подготовка отчетности по инцидентам информационной безопасности: составление отчетов о выявленных случаях нарушения информационной безопасности предприятия. Моделируемые сценарии противодействия вредоносному ПО: отработка практических приемов реагирования на обнаружение вредоносных программ.	2
5.	Тема 5. Противодействие компьютерным преступлениям путем реализации политики безопасности	Разработка политики безопасности в организации: основные этапы формирования и внедрения документационной политики информационной безопасности. Формулировка требований к защите данных и контроль исполнения: установление стандартов управления доступом и контроля над ресурсами предприятия. Регистрация и учет нарушений информационной безопасности: организация процедуры регистрации и учёта фактов несоблюдения установленных норм и правил.	2
6.	Тема 6. Преступления в сфере компьютерной информации	Осуществление внутреннего аудита информационной безопасности: оценка соответствия текущих процессов стандартам и требованиям внутренней политики безопасности. Проведение тренингов сотрудников по вопросам информационной безопасности: осуществление регулярного информирования персонала относительно вопросов сохранения конфиденциальности и целостности данных. Организация и проведение проверок оборудования и каналов связи: проверка работоспособности защитного программного обеспечения и отсутствие неавторизованных подключений.	2
7.	Тема 7.	Критическая информационная инфраструктура (КИИ):	2

№ п/п	Наименование раздела, темы дисциплины	Содержание лабораторных работ	Объем (час.)
			Очная форма обучения
	Компьютерные преступления, направленные на воздействие на критическую информационную инфраструктуру РФ	определение и состав КИИ, роль КИИ в национальной безопасности, примеры объектов КИИ в России Типы угроз для КИИ: вредоносное ПО (вирусы, черви, трояны), атаки на отказ в обслуживании (DDoS), социальная инженерия и фишинг Методы и инструменты атак на КИИ: анализ уязвимостей систем, использование эксплойтов, примеры успешных атак на КИИ	
8.	Тема 8. Судебная практика по компьютерным преступлениям	Методы расследования компьютерных преступлений: сбор и анализ цифровых доказательств, использование экспертиз в судебном процессе, применение технологий для выявления и преследования преступников Роль прокурора и адвоката в делах о компьютерных преступлениях: обязанности и функции прокурора, защита прав обвиняемого и потерпевшего, стратегии защиты и обвинения Судебные процессы: этапы и особенности: подготовка к судебному разбирательству, проведение судебного заседания, принятие решений и вынесение приговоров	2
9	Тема 9. Предотвращение компьютерных преступлений	Политики безопасности информационных систем: разработка и внедрение политик безопасности, обучение сотрудников основам кибербезопасности, регулярные аудиты и тестирование систем. Социальная инженерия и методы защиты от нее: понятие социальной инженерии, примеры атак и способы защиты, обучение персонала	-
	Всего		**16**

8. Примерная тематика курсовых работ (проектов)

Курсовые работы (проекты) не предусмотрены.

9. Самостоятельная работа студента

Самостоятельная работа студента при изучении дисциплины «Компьютерные преступления в компьютерных системах и сетях» направлена на:

– освоение нормативных правовых актов и учебной литературы, необходимых для освоения дисциплины;

– самостоятельный поиск информации в Интернете и других источниках;

– выполнение домашних заданий по практическим занятиям;

– подготовку к зачету с оценкой.

Краткие рекомендации по выполнению самостоятельной работы:

Успешное усвоение дисциплины предполагает большой, упорный, серьезный, систематический труд студентов. Важнейшая его составная часть – выполнение разных видов самостоятельной работы.

1. **Составление тематического конспекта** на основе изученной основной и дополнительной учебной литературы. В тематическом конспекте за основу берется содержание темы, вопросы для обсуждения.

Этапы работы.

1.1 Конспектирование делается только после того, как прочитан или усвоен материал для конспектирования.

1.2. Необходимо мысленно или письменно составить план конспекта. По этому плану и будет строиться конспект далее.

1.3. Составление самого конспекта. Можно сказать, что конспект – это расширенные тезисы, дополненные рассуждениями и доказательствами, содержащимися в материалах для конспекта, а также собственными мыслями и положениями составителя конспекта.

Писать конспект рекомендуется четко и разборчиво. В конспекте можно выделять места текста в зависимости от их значимости. Для этого применяются различного размера буквы, подчеркивания, замечания на полях.

Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Зачетно-экзаменационные материалыдля промежуточной аттестации (зачет)

1. Понятие и виды компьютерных преступлений.
2. Признаки, основные характеристики компьютерных преступлений
3. Обзор угроз безопасности компьютерных систем.
4. Раскрытие и расследование компьютерных преступлений.
5. Детальный анализ вредоносного программного обеспечения.
6. Классификация ВПО. Эвристический анализ.
7. Компьютерные сетевые атаки. Удаленные компьютерные сетевые атаки.
8. Системы обнаружения вторжения и межсетевого экранирования.
9. Анализ разрушающих воздействий. Методы обнаружения и борьбы.
10. Политики безопасности. Организация сетевой политики безопасности.
11. Несанкционированный доступ к компьютерной информации.
12. Незаконные использование и (или) передача, сбор и (или) хранение компьютерной информации, содержащей персональные данные.
13. Создание, использование и распространение вредоносных компьютерных программ.
14. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и ИТКС.
15. Неправомерное воздействие на КИИ РФ.
16. Нарушение правил централизованного управления ТС противодействия угрозам устойчивости, безопасности и целостности функционирования на территории РФ ИТКС "Интернет" и сети связи общего

пользования.

17. Компьютерные преступления, направленные на воздействие на критическую информационную инфраструктуру РФ.

18. Приговоры по компьютерным преступлениям.

19. Апелляционные судебные акты по компьютерным преступлениям.

20. Кассационные и надзорные судебные акты по компьютерным преступлениям.

21. Превентивные методы. Способы предотвращения компьютерных преступлений.

10. Оценивание результатов обучения и уровня сформированности компетенций

Оценивание результатов обучения по дисциплине и уровня сформированности компетенций (части компетенции) осуществляется в рамках текущего контроля успеваемости и промежуточной аттестации в соответствии с оценочными материалами.

11. Учебно-методическое обеспечение дисциплины

Основная литература:

1. Расследование преступлений в сфере компьютерной информации и электронных средств платежа : учебник для вузов / ответственные редакторы С. В. Зуев, В. Б. Вехов. — Москва : Издательство Юрайт, 2025. — 243 с. — (Высшее образование). — ISBN 978-5-534- 13898-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/567677 (дата обращения: 03.03.2025).

2. Преступления в сфере высоких технологий и информационной безопасности : учебное пособие / В. Ф. Васюков, А. Г. Волеводз, М. М. Долгиева, В. Н. Чаплыгина ; под науч. ред. А. Г. Волеводза. - Москва : Прометей, 2023. - 1086 с. - ISBN 978-5-00172-447-6. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2124867 (дата обращения: 03.03.2025). – Режим доступа: по подписке.

3. Корноухов, В. Е. Методика расследования преступлений: теоретические основы : монография / В.Е. Корноухов. — Москва : Норма : ИНФРА-М, 2024. — 224 с. - ISBN 978- 5-91768-263-1. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2132533 (дата обращения: 03.03.2025). – Режим доступа: по подписке.

4. Петров, А. А. Компьютерная безопасность. Криптографические методы защиты : практическое руководство / А. А. Петров. - 2-е изд. - Москва : ДМК Пресс, 2023. - 451 с. - ISBN 978-5-89818-453-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/2106222 (дата обращения: 03.03.2025). – Режим доступа: по подписке.

5. Преступления против общественной безопасности и общественного порядка : учебник для вузов / ответственные редакторы А. В. Наумов, А. Г. Кибальник. — 6-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 158 с. — (Высшее образование). — ISBN 978-5-534-18589-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/563347 (дата обращения: 03.03.2025).

Электронные библиотечные системы (ЭБС) и электронные образовательные ресурсы

1. Электронно-библиотечная система ZNANIUM https:// www.znanium.com
2. Универсальная справочно-информационная полнотекстовая база данных периодических изданий «East View» (ИВИС) https://dlib.eastview.com/
3. Электронно-библиотечная система «BOOK.ru» www.book.ru
4. Электронно-библиотечная система «IPRbooks» http://www.iprbookshop.ru/
5. ЭБС «Национальный цифровой ресурс «Руконт» https://lib.rucont.ru/search
6. Образовательная платформа ЮРАЙТ http://www.urait.ru

Электронный каталог Университета – Автоматизированная информационная библиотечная система (АИБС «МегаПро»)

12. Перечень программного обеспечения, профессиональных баз данных и информационных справочных систем, необходимых для освоения дисциплины

Лицензионное программное обеспечение, в том числе отечественного производства:

– DsktpEdu ALNG LicSARk OLV F1 1Y Acdmc Ent (MS Windows) (подписка на ПО).

Свободно распространяемое программное обеспечение, в том числе отечественного производства:

– 7-Zip (свободный файловый архиватор с высокой степенью сжатия данных) (отечественное ПО).

– FastStone Image Viewer (программа для просмотра изображений в Microsoft Windows (лицензия бесплатного программного обеспечения)).

– Foxit Reader (Бесплатное прикладное программное обеспечение для просмотра электронных документов в стандарте PDF (лицензия бесплатного программного обеспечения)).

– Indigo (система программ для создания и проведения компьютерного тестирования знаний).

– Google Crome, ЯндексБраузер (браузер).

– Adobe Acrobat Reader DC (• ПО для просмотра, печати и комментирования документов в формате PDF)

– Visual Studio Code (интегрированная среда разработки программного обеспечения)

Профессиональные базы данных не используются.

Информационные справочные системы:

– СПС КонсультантПлюс. Компьютерная справочная правовая система, широко используется учеными, студентами и преподавателями (подписка на ПО)

Каждый обучающийся в течение всего периода обучения обеспечивается индивидуальным неограниченным доступом к электронно-библиотечной

13. Материально–техническое обеспечение дисциплины

Образовательный процесс обеспечен учебными аудиториями для проведения учебных занятий, а именно для проведения занятий лекционного типа, лабораторных занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, помещениями для

Учебная аудитория для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Рабочее место преподавателя (стол, стул), рабочие места обучающихся, доска для написания мелом, кафедра.

Технические средства обучения: персональный компьютер-1, мультимедийное оборудование (проектор, проекционный экран) - 1

Учебная аудитория для проведения лабораторных занятий. Учебная аудитория для проведения лабораторных занятий. Лаборатория сетей и систем передачи информации, безопасности компьютерных сетей

Рабочее место преподавателя (стол, стул), рабочие места обучающихся:

Технические средства обучения: персональный компьютер с подключением к сети «Интернет» - - 15, сетевое оборудование; стенды; коммутаторы, маршрутизаторы, средства анализа сетевого трафика, межсетевые экраны, средства обнаружения компьютерных атак, средства анализа защищенности компьютерных сетей

Учебная аудитория для проведения лабораторных занятий. Аудитория информационных технологий

Рабочее место преподавателя (стол, стул), рабочие места обучающихся:

Технические средства обучения:

персональный компьютер с подключением к сети «Интернет» - 15, сетевое оборудование.

Помещение для самостоятельной работы обучающихся, оснащенное компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду института.

Рабочие места обучающихся.

Технические средства обучения: персональный компьютер - 13.

Учебные аудитории соответствуют действующим противопожарным правилам и нормам, укомплектованы учебной мебелью.

Обновление рабочей программы дисциплины (модуля)

Наименование раздела рабочей программы, в который внесены изменения

(измененное содержание раздела)

обсуждено и рекомендовано к утверждению решением кафедры наименование кафедры
от ___ _____ 20_ г., протокол № ___

одобрено Научно-методическим советом _____ от ___ _____ 20__ г., протокол №____