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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

МОДЕЛИ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ

Специальность: 10.05.01 Компьютерная безопасность
Специализация: «Разработка защищенного программного обеспечения»
Формы обучения: очная
Объем дисциплины:
в зачетных единицах: 4 з.е.
в академических часах: 144 ак.ч.

Форма промежуточной аттестации: экзамен

2025

Рабочая программа по дисциплине «Модели безопасности компьютерных систем» 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 естественных дисциплин, сервиса и туризма от 25 марта 2025 г., протокол № 6

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

СОДЕРЖАНИЕ

1. Цель и задачи освоения дисциплины

Целью изучения дисциплины «Модели безопасности компьютерных систем» является подготовка обучающихся к решению задач профессиональной деятельности в области защиты информации по направлению подготовки 10.05.01 Компьютерная безопасность посредством обеспечения этапов формирования компетенций, предусмотренных ФГОС и установленных программой специалитета на основе профессиональных стандартов, в части представленных ниже знаний, умений и навыков.

Изучить понятийный аппарат дисциплины, основные теоретические положения и методы обеспечения безопасности компьютерных систем и сетей; дать представление об уязвимости компьютерных сетей, технических каналах "утечки" информации в компьютерных сетях, основных характеристиках технических средств защиты информации от утечек по техническим каналам в компьютерных сетях, категориях сетевых атак, технологиях обнаружения сетевых вторжений, организационных мерах по защите информации; рассмотреть вопросы информационной безопасности IP-сетей, технологий виртуальных защищенных сетей, защиты беспроводных каналов связи; ознакомить обучающихся с национальными, межгосударственными и международными стандартами в области защиты информации, стандартами по защите сетей промышленных систем автоматизации, видами политик безопасности компьютерных сетей, архитектурой системы управления средствами информационной безопасности сети, основными средствами, способами и принципами построения сетевой инфраструктуры систем защиты информации автоматизированных систем, программно-аппаратными средствами обеспечения защиты информации в компьютерных сетях, особенностями защиты промышленных сетей; сформировать умения и привить навыки применения теоретических знаний для решения профессиональных задач, таких как определение уровня защищенности компьютерных сетей, оценка соответствия механизмов безопасности компьютерной сети требованиям существующих стандартов и нормативных документов, формулировка предложений по устранению выявленных уязвимостей, формирование политики безопасности компьютерных сетей, задание требований к защите информации в компьютерной сети, выбор средств защиты в соответствии с выявленными угрозами по критерию соответствия их стандартам информационной безопасности, разработка моделей сетевой инфраструктуры автоматизированных систем и подсистем безопасности сетевой инфраструктуры автоматизированных систем, проектирование защищенных виртуальных локальных сетей, проектирование защищенных каналов корпоративных сетей, тестирование систем защиты сетевой инфраструктуры автоматизированных систем, документирование технических средств компьютерных сетей с учетом требований по обеспечению защиты информации, настройка средств защиты сетевого трафика активного сетевого

оборудования, конфигурирование безопасной сетевой инфраструктуры IoT, конфигурирование и настройка защищенного беспроводного канала связи.

2. Место дисциплины в структуре образовательной программы

Дисциплина «Модели безопасности компьютерных систем» 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
ОПК-11	-	**Модели безопасности компьютерных систем**	-

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
ОПК-11. Способен разрабатывать политики безопасности, политики управления доступом и информационными потоками в компьютерных системах с учетом угроз безопасности информации и требований по защите информации	ОПК-11.1. Имеет практический опыт оценивания уровня безопасности компьютерных систем и сетей, разработки требований по защите, формирования политик безопасности компьютерных систем и сетей, проведения анализа безопасности компьютерных систем, разработки требований к программно-аппаратным средствам защиты информации компьютерных систем и сетей	Знать: методы оценки уровня защищенности компьютерных систем и сетей, требования по защите компьютерной инфраструктуры и методологии их разработки, основные принципы построения эффективных политик безопасности компьютерных систем и сетей; методики анализа безопасности информационных систем. Уметь: оценивать уровень безопасности существующих компьютерных систем и сетей; разрабатывать требования по защите компьютерных систем и сетей; формулировать политику безопасности и управлять её реализацией; проводить анализ уязвимости компьютерных систем и определять меры противодействия угрозам. Владеть: навыком проектирования и реализации политик безопасности компьютеризированных инфраструктур; инструментами оценки соответствия требованиям информационной безопасности; практическими методами мониторинга состояния защищённости компьютерных систем и сетей.

Формируемые компетенции (код и наименование компетенции)	Индикаторы достижения компетенций	Планируемые результаты обучения
	ОПК-11.2. Демонстрирует умение проводить исследование вредоносного программного обеспечения, выявлять аномальную активность в компьютерных системах и сетях, выбирать программно-аппаратные средства защиты информации	Знать: типологию и характеристики современных вредоносных программ; способы выявления аномальной активности в компьютерных системах и сетях; классификацию методов выбора аппаратных и программных средств защиты информации. Уметь: анализировать вредоносное программное обеспечение и выявлять признаки подозрительной активности в сети; определять необходимые средства защиты для нейтрализации конкретных типов атак; выбирать оптимальные решения для защиты информации исходя из особенностей организации. Владеть: техниками исследования поведения вредоносного ПО; способами обнаружения аномалий в работе компьютерных систем и сетевых взаимодействиях; мением подбирать и внедрять современные программно-технические средства защиты.
	ОПК-11.3. Применяет знания моделей без- опасности и правил разработки документов предприятия по информационной безопасности для разработки политики управления доступом и информационными потоками в компьютерных системах	Знать: современные модели информационной безопасности и правила документирования политики безопасности организаций; принципы управления доступом пользователей и контроль информационных потоков внутри корпоративных ИТ-инфраструктур; нормативно-правовые основы информационной безопасности предприятий. Уметь: создавать политики управления доступом и регулирующими информационными потоками в рамках корпоративной системы; проектировать эффективные схемы контроля над распространением конфиденциальной информации; документально оформлять стандарты и процедуры по обеспечению информационной безопасности. Владеть: умениями анализировать угрозы информационной безопасности и проектировать соответствующие защитные мероприятия; правилами составления регламентов и инструкций по управлению доступом и обеспечением конфиденциальности информации.
	ОПК-11.4. Демонстрирует умение разрабатывать модель угроз и нарушителя информационной безопасности компьютерных сетей	Знать: структуру и содержание типовых моделей угроз информационной безопасности; основы моделирования нарушителей информационной безопасности; алгоритмы оценки вероятности возникновения угроз и рисков для ИТ-инфраструктуры. Уметь: разрабатывать модели угроз и

Формируемые компетенции (код и наименование компетенции)	Индикаторы достижения компетенций	Планируемые результаты обучения
		нарушителей применительно к конкретной корпоративной среде; оценивать степень риска потенциальных угроз и планировать контрмеры; использовать полученные модели для повышения общей устойчивости информационно-технологической среды. Владеть: компетенциями по созданию и применению профилей угроз и характеристик потенциального злоумышленника; механизмами прогнозирования последствий угроз и разработки мер по минимизации возможных потерь.

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
			9
1. Контактная работа обучающихся с преподавателем:		69	69
Аудиторные занятия, часов всего, в том числе:		68	68
• занятия лекционного типа		34	34
• занятия семинарского типа:		34	34
практические занятия		-	-
лабораторные занятия		34	34
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		39	39
- подготовка курсовой работы		-	-
- проработка учебного (теоретического) материала		15	15
- выполнение домашних заданий по практическим занятиям		15	15
- подготовка к зачету		9	9
Промежуточная аттестация: экзамен		36	36
ИТОГО:	часов	144	144
общая трудоемкость	зач. ед.	4	4

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

5.1. Содержание дисциплины

Раздел 1. Проблемы и угрозы информационной безопасности сетей. Стандарты информационной безопасности компьютерных сетей.

1.1. Введение в дисциплину. Основные понятия и определения.

1.2. Проблемы и угрозы информационной безопасности сетей.

1.3. Управление безопасностью компьютерных сетей.

1.4. Отечественные и зарубежные стандарты информационной безопасности компьютерных сетей.

Раздел 2. Межсетевые экраны. Схемы сетевой защиты на базе МЭ.

2.1. Введение в сетевой информационный обмен.

2.2. Межсетевые экраны. Схемы сетевой защиты на базе МЭ.

Раздел 3. Категории сетевых атак. Технологии обнаружения сетевых вторжений.

3.1. Категории сетевых атак.

3.2. Технологии обнаружения сетевых вторжений.

Раздел 4. Виртуальные защищенные сети, VPN.

4.1. Виртуальные локальные сети.

4.2. Конфигурирование виртуальных локальных сетей.

4.3. Виртуальные защищенные сети VPN.

4.4. Технологии и протоколы VPN.

4.5. Построение VPN на основе маршрутизаторов

Раздел 5. Защита информационных сетей на промышленных предприятиях и объектах критической инфраструктуры. Защищенные системы беспроводной связи.

5.1. Понятие и разновидности промышленных информационных сетей.

5.2. Промышленный Ethernet. Интегрированные системы промышленной автоматизации.

5.3. Защита информационных сетей на промышленных предприятиях и объектах критической инфраструктуры.

5.4. Защищенные системы беспроводной связи. Беспроводные виртуальные сети.

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)	самос-тоятельная работа	
1	Раздел 1. Проблемы и угрозы информационной безопасности сетей. Стандарты информационной безопасности компьютерных сетей	8	8/8	8	ОПК-11, ОПК-11.1, ОПК-11.2, ОПК_11.3 ОПК-11.4
2	Раздел 2. Межсетевые экраны. Схемы сетевой защиты на базе МЭ.	8	8/8	8	ОПК-11, ОПК-11.1, ОПК-11.2, ОПК_11.3 ОПК-11.4
3	Раздел 3. Категории сетевых атак. Технологии обнаружения сетевых вторжений.	8	8/8	8	ОПК-11, ОПК-11.1, ОПК-11.2, ОПК_11.3 ОПК-11.4
4	Раздел 4. Виртуальные защищенные сети VPN	6	6/6	6	ОПК-11, ОПК-11.1, ОПК-11.2, ОПК_11.3 ОПК-11.4
5	Раздел 5. Защита информационных сетей на промышленных предприятиях и объектах критической инфраструктуры. Защищенные системы беспроводной связи.	4	4/4	9	ОПК-11, ОПК-11.1, ОПК-11.2, ОПК_11.3 ОПК-11.4
	Всего	**34**	**34/34**	**39**	

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.	Раздел 1. Проблемы и угрозы	Вводное занятие. Настройка необходимого ПО и среды разработки.	8

№ п/п	Наименование раздела, темы дисциплины	Содержание лабораторных работ	Объем (час.)
			Очная форма обучения
	информационной безопасности сетей. Стандарты информационной безопасности компьютерных сетей		
2.	Раздел 2. Межсетевые экраны. Схемы сетевой защиты на базе МЭ.	Формирование политики безопасности компьютерных сетей. Формирование политики информационной безопасности компании. Разработка требований по защите компьютерных сетей на основе стандартов информационной безопасности компьютерных сетей и сетей связи.	8
3.	Раздел 3. Категории сетевых атак. Технологии обнаружения сетевых вторжений.	Проектирование защищенной виртуальной локальной сети. Защита канальной инфраструктуры сети. Исследование методов защиты сетевого трафика. Сетевая защита на базе межсетевых экранов. Управление трафиком межсетевого взаимодействия.	8
4.	Раздел 4. Виртуальные защищенные сети VPN	Разработка требований по защите промышленных компьютерных сетей на основе стандартов информационной безопасности промышленных систем и сетей. Проектирование защищенной корпоративной сети. Разработка модели сети.	6
5.	Раздел 5. Защита информационных сетей на промышленных предприятиях и объектах критической инфраструктуры. Защищенные системы беспроводной связи.	Конфигурирование безопасной сетевой инфраструктуры IoT. Конфигурирование и настройка беспроводного канала связи в соответствии с требованиями информационной безопасности.	4
	Всего		**34**

8. Примерная тематика курсовых работ (проектов)

Курсовые работы (проекты) не предусмотрены.

9. Самостоятельная работа студента

Самостоятельная работа студента при изучении дисциплины «Модели безопасности компьютерных систем» 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.

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 (экзамен)

Примеры экзаменационных билетов:

Экзаменационный билет №

Примеры практических заданий, выносимых на экзамен, для проверки практических

умений и навыков студентов по дисциплине

Задача 1.

По заданному IP адресу устройства и маске подсети определить:

- адрес широковещательной рассылки;
- первый и последний доступные IP адреса для этой сети.

IP-адрес устройства: 113.83.34.54. Маска подсети: 255.254.0.0

Построить модель сети из двух компьютеров, соединенных через

коммутатор. Задать компьютерам первый и последний доступные IP адреса рассчитанной сети. Проверить работоспособность сети.

Задача 2.

В сети заданной конфигурации настроить сеть vlan. Задача 3.

В сети заданной конфигурации настроить защищенный маршрут из сети 172.16.10.0 к серверу.

Перечень вопросов, которые выносятся на экзамен

1. Основные понятия и составляющие информационной безопасности компьютерных сетей.
2. Актуальность проблемы обеспечения информационной безопасности современных сетей.
3. Проблемы информационной безопасности сетей.
4. Угрозы информационной безопасности сетей.
5. Классификация методов защиты информации.
6. Общие вопросы формирования политики безопасности.
7. Задачи управления безопасностью компьютерных сетей.
8. Политика безопасности компьютерных сетей.
9. Архитектура системы управления средствами информационной безопасности сети.
10. Отечественные стандарты информационной безопасности компьютерных сетей.
11. Зарубежные стандарты информационной безопасности.
12. Сетевые стандарты и технологии.
13. Модель взаимодействия открытых систем (OSI).
14. Набор протоколов TCP/IP. Межсетевой протокол IP.
15. Функции и особенности функционирования МЭ на различных уровнях модели OSI.
16. Схемы сетевой защиты на базе МЭ.
17. Категории сетевых атак.
18. Средства анализа защищенности сетевых протоков и сервисов.
19. Системы обнаружения атак IDS. Компоненты и архитектура.
20. Методы реагирования на сетевые атаки.
21. Виртуальные локальные сети. Типы виртуальных сетей.
22. Идентификация сетей VLAN. Протокол VTP.
23. Конфигурирование виртуальных локальных сетей.
24. Основные понятия и функции сети VPN.
25. Варианты построения виртуальных защищенных каналов.
26. Средства обеспечения безопасности VPN.
27. Классификация VPN.
28. Основные варианты архитектуры VPN.
29. Сетевые защищенные протоколы.
30. Маршрутизация и автономные системы.
31. Принципы маршрутизации.

32.Статическая и динамическая маршрутизация.

33.Технология организации VPN-туннеля.

34.Промышленные информационные сети: понятие, особенности, разновидности.

35Сетевая информационная структура предприятия.

36Информационные сети технологического и полевого уровней.

37.Промышленный Ethernet.

38.Интегрированные системы промышленной автоматизации.

39.Особенности защиты информации на промышленных предприятиях и критически важных объектах.

40.Угрозы безопасности промышленных предприятий.

41.Вопросы безопасности сетевой инфраструктуры в концепции ИБ предприятия.

42.Защита промышленных систем автоматизации от вредоносного ПО.

43.Управление безопасностью на производстве согласно ISA S99.

44.Техническая архитектура безопасности на основе IEC 62443.

45.Методы защиты промышленных сетей.

46.Интегрированные системы безопасности.

47.Механизмы аутентификации беспроводных клиентов по стандарту IEEE 802.11.

48.Комплексная система обеспечения безопасности беспроводных сетей по стандарту IEEE 802.11i.

49.Стандарты безопасности WPA/WPA2.

50.Стандарт IEEE 802.1x/EAP.

51.Развертывание беспроводных виртуальных сетей.

52.Системы обнаружения вторжений в беспроводных сетях.

53.Какими правовыми актами и нормативными документами регулируются вопросы обеспечения безопасности объектов критической инфраструктуры?

54.В каких стандартах сформулированы требования, предъявляемые к информационной безопасности промышленных систем автоматизации и промышленных сетей?

55.Какой российский стандарт описывает безопасность оборудования с ограниченными возможностями с точки зрения применения информационных технологий в домашних сетях?

56.Какие методы защиты каналов связи применяются на промышленных предприятиях?

57.Назовите основные положения стандарта ISA-99.

58.Назовите основные положения семейства стандартов IEC 62443.

59.В каких национальных стандартах РФ рассматриваются вопросы защиты промышленных систем и сетей?

60.Какие требования к составлению программы обеспечения защищенности (кибербезопасности) системы управления и промышленной автоматики предъявляет стандарт ГОСТ Р МЭК 62443-2-1-2015?

61.Каковы основные требования к системной безопасности ГОСТ Р

МЭК 62443-3-3-2016?

62.Сформулируйте требования по защите промышленной сети организации (по вариантам)? Какими стандартами вы при этом руководствовались

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. Костин В. Н. Методы и средства защиты компьютерной информации: информационная безопасность компьютерных сетей [Электронный ресурс]: учебное пособие / В. Н. Костин. – Москва: МИСИС, 2018. – 31 с. – Режим доступа: https://e.lanbook.com/book/116743.
2. Прохорова О. В. Информационная безопасность и защита информации [Электронный ресурс]: учебник / О. В. Прохорова. – 2-е изд., испр. – Санкт-Петербург: Лань, 2020. – 124 с. Режим доступа: https://e.lanbook.com/book/133924.
3. Сидак, А. А. Информационная безопасность. Физические основы технических каналов утечки информации : учебное пособие : [16+] / А. А. Сидак, В. В. Василенко, С. В. Рыженко ; Технологический университет им. А. А. Леонова. – Москва : Директ-Медиа, 2022. – 128 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=694670 (дата обращения: 22.02.2025). – Библиогр.: с. 117-118. – ISBN 978-5-4499-3327-0. – DOI 10.23681/694670. – Текст :электронный.
4. Ларионова, С. Л. Информационная безопасность дистанционного банковского обслуживания : учебное пособие : [16+] / С. Л. Ларионова ; Финансовый университет при Правительстве Российской Федерации. – Москва : Прометей, 2022. – 296 с. : ил., табл., схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=701063 (дата обращения: 22.02.2025). – Библиогр. в кн. – ISBN 978-5-00172-343-1. – Текст : электронный.

Дополнительная литература:

1. Технологии защиты информации в компьютерных сетях [Электронный ресурс] / Н.А. Руденков, А.В. Пролетарский, Е.В. Смирнова, А.М. Суровов.– 2-е изд., испр. – Москва : Национальный Открытый

Университет «ИНТУИТ», 2016. – 369 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=428820.

2. Голиков А.М. Защита информации в инфокоммуникационных системах и сетях [Электронный ресурс]: учебное пособие – Томск: Томский государственный университет систем управления и радиоэлектроники, 2015. – 284 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=480637.

3. Сердюк В.А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий [Электронный ресурс]: учебное пособие. – Москва: Издательский дом Высшей школы экономики, 2015 574 с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=440285.

4. Голиков А.М. Защита информации от утечки по техническим каналам [Электронный ресурс]: учебное пособие. – Томск: Томский государственный университет систем управления и радиоэлектроники, 2015. - 256с. – Режим доступа: http://biblioclub.ru/index.php?page=book&id=480636.

5. Аверченков В.И. Аудит информационной безопасности [Электронный ресурс]: учебное пособие для вузов / В.И. Аверченков. – 3-е изд., стереотип. - Москва: Флинта, 2016 Режим доступа: Режим доступа: http://biblioclub.ru/index.php?page=book&id=93245.

6. Лапонина О.Р. Межсетевые экраны [Электронный ресурс]: учебное пособие /О.Р. Лапонина. – 2-е изд., исправ. – Москва: Национальный Открытый Университет «ИНТУИТ», 2016. – 466 с.: Режим доступа: https://biblioclub.ru/index.php?page=book&id=429093.

Для освоения дисциплины инвалидами и лицами с ограниченными возможностями здоровьяимеются издания в электронном виде в электронно-библиотечных системах «Лань» и «Юрайт».

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 самостоятельной работы студентов.

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. 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 №____