Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
"Амурский государственный университет"

УТВЕРЖДАЮ
Проректор по учебной и научной работе
Лейфа А.В. Лейфа
27 июня 2024 г.

РАБОЧАЯ ПРОГРАММА
«КОНТРОЛЬ ЗАЩИЩЕННОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ»

Направление подготовки 10.03.01 Информационная безопасность

Направленность (профиль) образовательной программы – Безопасность автоматизированных систем (по отраслям или в сфере профессиональной деятельности)

Квалификация выпускника – Бакалавр

Год набора – 2024

Форма обучения – Очная

Курс 4 Семестр 8

Зачет с оценкой 8 сем

Общая трудоемкость дисциплины 144.0 (академ. час), 4.00 (з.е)

Составитель Д.В. Фомин, старший преподаватель,
Институт компьютерных и инженерных наук
Кафедра информационной безопасности

2024

Рабочая программа составлена на основании Федерального государственного образовательного стандарта ВО для направления подготовки 10.03.01 Информационная безопасность, утвержденного приказом Министерства науки и высшего образования Российской Федерации от 17.11.20 № 1427

Рабочая программа обсуждена на заседании кафедры информационной безопасности

01.02.2024 г. , протокол № 8

Заведующий кафедрой Никифорова Л.В. Никифорова

СОГЛАСОВАНО	СОГЛАСОВАНО
Учебно-методическое управление	Выпускающая кафедра
Чалкина Н.А. Чалкина	Никифорова Л.В. Никифорова
27 июня 2024 г.	27 июня 2024 г.
СОГЛАСОВАНО	СОГЛАСОВАНО
Научная библиотека	Центр цифровой трансформации и технического обеспечения
Петрович О.В. Петрович	Тодосейчук А.А. Тодосейчук
27 июня 2024 г.	27 июня 2024 г.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель дисциплины:

Целями освоения учебной дисциплины «Контроль защищенности автоматизированных систем» является обеспечение требуемого уровня знаний, умений и навыков у студентов для организации и проведения работ в области выбора и применения методов и средств контроля эффективности защиты информации в АС от несанкционированного доступа.

Задачи дисциплины:

Дать основы правовых, организационно- распорядительных, нормативных и информационных документов в области технической защиты информации (ТЗИ); физических основ реализации угроз безопасности информации на ОИ и порядка их выявления; практической отработки методик проведения контроля технических средств обработки информации (ТСОИ) в соответствии с методологией исследований защищенности средств и систем на соответствие требованиям по безопасности информации; организации и порядка проведения аттестации ОИ и отработки технических документов по результатам испытаний.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Контроль защищенности автоматизированных систем» относится к числу Элективных дисциплин. Для успешного усвоения данной дисциплины необходимо, чтобы студент владел хорошей физико- математической подготовкой, знаниями, умениями и навыками смежных дисциплин "Безопасность систем баз данных", "Безопасность вычислительных сетей", "Стандарты информационных информационной безопасности", "Защита информации от утечки по техническим каналам".

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ И ИНДИКАТОРЫ ИХ ДОСТИЖЕНИЯ

3.1 Профессиональные компетенции и индикаторы их достижения

Код и наименование профессиональной компетенции	Код и наименование индикатора достижения профессиональной компетенции
ПК-3 Способен выполнять комплекс задач администрирования систем защиты информации автоматизированных систем	ИД-1ПК-3- знать: принципы формирования политики информационной безопасности в автоматизированных системах, программно-аппаратные средства защиты информации автоматизированных систем ИД-2ПК-3- уметь: создавать, удалять и изменять учетные записи пользователей автоматизированной системы, устанавливать и настраивать операционные системы, системы управления базами данных, компьютерные сети и программные системы с учетом требований по обеспечению защиты информации ИД-3ПК-3 — иметь навык установки и настройки операционных систем, систем управления базами данных, компьютерных сетей и программных систем с учетом требований по обеспечению защиты информации, управления полномочиями пользователей автоматизированной системы

4. СТРУКТУРА ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 4.00 зачетных единицы, 144.0 академических часов.

1 – № п/п

2 – Тема (раздел) дисциплины, курсовая работа (проект), промежуточная аттестация

3 – Семестр

4 – Виды контактной работы и трудоемкость (в академических часах)

4.1 – Л (Лекции)

4.2 – Лекции в виде практической подготовки

4.3 – ПЗ (Практические занятия)

4.4 – Практические занятия в виде практической подготовки

4.5 – ЛР (Лабораторные работы)

4.6 – Лабораторные работы в виде практической подготовки

4.7 – ИКР (Иная контактная работа)

4.8 – КТО (Контроль теоретического обучения)

4.9 – КЭ (Контроль на экзамене)

5 – Контроль (в академических часах)

6 – Самостоятельная работа (в академических часах)

7 – Формы текущего контроля успеваемости

1	2	3	4									5	6	7
			4.1	4.2	4.3	4.4	4.5	4.6	4.7	4.8	4.9			
1	Раздел 1. Основные рекомендации по защите информации ограниченного доступа от НСД.	8	6				6						40	Опрос. Защита лабораторных работ.
2	Раздел 2. Организация контроля прав доступа к объекту.	8	6				6						40	Опрос. Защита лабораторных работ.
3	Раздел 3. Особенности аттестационных испытаний АС на соответствие требованиям по защите информации от НСД.	8	6				6						27.8	Опрос. Защита лабораторных работ.
4	Зачёт с оценкой	8								0.2				
	Итого		18.0		0.0		18.0		0.0	0.2	0.0	0.0	107.8	

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

5.1. Лекции

№ п/п	Наименование темы (раздела)	Содержание темы (раздела)
1	Раздел 1. Основные рекомендации по защите информации ограниченного доступа от НСД.	Тема 1. Основные предпосылки реализации угроз безопасности информации ограниченного доступа, обрабатываемой с использованием автоматизированных систем различного уровня и назначения, обусловленных несанкционированным доступом (НСД) к ней и специальными воздействиями на нее. Классификация угроз безопасности информации по результатам реализации НСД и специальных воздействий на нее. Принципы выявления угроз НСД к информации и специальных воздействий на нее в системах обработки информации. Анализ опасности угроз. Тема 2. Нормативные документы ФСТЭК России по аттестации объектов информатизации и защите информации. Основные руководящие документы ФСТЭК России по критериям защищенности средств вычислительной техники и автоматизированных систем. Основные зарубежные стандарты по критериям защищенности информационных технологий. Средства контроля защищенности от НСД. Тема 3. Защита автоматизированных систем от несанкционированного доступа к обрабатываемой информации. Классификация автоматизированных систем и требования по защите информации. Методы оценки защищенности автоматизированных систем от НСД к обрабатываемой информации. Методики оценки защищенности подсистемы управления доступом в автоматизированных системах (АС), подсистемы регистрации и учета в АС, криптографической подсистемы защиты информации, обрабатываемой в АС, подсистемы обеспечения целостности информации, обрабатываемой в АС.
2	Раздел 2. Организация контроля прав доступа к объекту.	Тема 1. Понятие программно- математического воздействия и вредоносной программы. Классификация вредоносных программ. Деструктивные функции вредоносных программ и способы их реализации. Особенности программно-математического воздействия в сетях общего пользования. Тема 2. Требования к подсистемам в зависимости от типов АС (АРМ, ЛВС). Классы защищенности и требования к подсистемам, в зависимости от класса защищенности. Руководящий документ: Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа. Характеристики автоматизированных систем (в отличие от СВТ). Классификация нарушителей по уровню

		возможностей, представляемых им штатными средствами АС и СВТ. Тема 3. Понятия: Уязвимость, эксплойт, полезная нагрузка. Уязвимости переполнения буфера. Уязвимости форматных строк. Межсайтовое выполнение вредоносного программного кода. Внедрение в запросы к базам данных. Размещение вредоносного программного кода по предсказуемому адресу. Уязвимости использования памяти после ее освобождения. Методы поиска уязвимостей. Контроль уязвимостей на уровне сети. Контроль уязвимостей на уровне операционных систем и прикладного ПО. Контроль уязвимостей на уровне системы управления базами данных. Контроль настроек механизмов обновления системного и прикладного. Контроль механизмов идентификации и аутентификации пользователей» при работе со средствами защиты информации (СЗИ).
3	Раздел 3. Особенности аттестационных испытаний АС на соответствие требованиям по защите информации от НСД.	Тема 1. Программные средства создания и редактирования модели системы разграничения доступа (СРД). Структура ресурсов АРМ и ЛВС. Установленные права доступа файловой системы NTFS. Списки локальных и доменных пользователей системы. Информация о разрешительной системе. Разграничение доступа с помощью стандартных средств ОС Windows. Предотвращение попыток НСД. Изучение программ «Ревизор 1 XP», «Ревизор 2 XP». Разграничение доступа к объектам АРМ. Тема 2. Проверка настроек мандатного и дискреционного механизмов доступа, а также прав пользователей, работающих в системе. Реализация дискреционного механизма разграничения доступа. Активизация подсистемы управления доступом. Проверка настроек дискреционного механизма разграничения доступа с помощью программ «Ревизор 1 XP» и «Ревизор 2 XP». Реализация мандатного механизма разграничения доступа. Проверка настроек мандатного механизма разграничения доступа с помощью программ «Ревизор 1 XP» и «Ревизор 2 XP». Работа с сетевыми ресурсами. Тема 3. Контроль целостности программного обеспечения и специализированных средств защиты информации от НСД с помощью программ фиксации и контроля исходного состояния программными комплексами «ФИКС». Настройка средств контроля целостности на основе операций контрольного суммирования: • фиксация исходного состояния файлов программного комплекса; • контроль исходного состояния программного комплекса; • фиксация и контроль

		каталогов; • контроль различий в заданных файлах; • контроль целостности файлов программного комплекса.

5.2. Лабораторные занятия

Наименование темы	Содержание темы
Лабораторная работа № 1	Инвентаризация актуального состава технических и программных средств объекта информатизации с использованием штатных средств операционной системы и программного обеспечения.
Лабораторная работа № 2	Поиск отличий реально полученной информации от информации, заявленной в исходных данных на объекте информатизации.
Лабораторная работа № 3	Контроль уязвимостей на уровне сети и на уровне операционных систем и прикладного ПО.
Лабораторная работа № 4	Контроль механизмов идентификации и аутентификации пользователей» при работе со средствами защиты информации (СЗИ) от НСД.
Лабораторная работа № 5	Проверка организации контроля доступа к объекту с использованием специализированных средств доверенной загрузки.
Лабораторная работа № 6	Проверка настроек разрешительной системы доступа к файловым системам с использованием специализированных тестирующих средств и штатных средств из состава ОС.
Лабораторная работа № 7	Настройка средств контроля целостности на основе операций контрольного суммирования.

6. САМОСТОЯТЕЛЬНАЯ РАБОТА

№ п/п	Наименование темы (раздела)	Содержание темы (раздела)	Трудоемкость в академических часах
1	Раздел 1. Основные рекомендации по защите информации ограниченного доступа от НСД.	Подготовка к опросу. Подготовка к защите лабораторных работ	40
2	Раздел 2. Организация контроля прав доступа к объекту.	Подготовка к опросу. Подготовка к защите лабораторных работ	40
3	Раздел 3. Особенности аттестационных испытаний АС на соответствие требованиям по защите информации	Подготовка к опросу. Подготовка к защите лабораторных работ	27.8

	от НСД.		

7. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В процессе изучения данной дисциплины необходимо использовать действующие правовые акты в области защиты информации, организационно- распорядительные, нормативные и информационные документы ФСТЭК России, других уполномоченных органов государственной власти, а также соответствующие учебно- методические пособия, иллюстративный материал (презентации). На лекционных занятиях излагаются наиболее важные и сложные вопросы, являющиеся теоретической основой нормативных документов и практических действий по защите информации и аттестации объектов информатизации по требованиям безопасности информации. Часть лекций может излагаться проблемным методом с привлечением студентов для решения сформулированной преподавателем проблемы. С целью текущего контроля знаний в ходе лекций могут использоваться различные приёмы тестирования. На лабораторные работы выносятся вопросы, усвоение которых требуется на уровне навыков и умений. Цикл лабораторных работ по отработке программно-аппаратных средств выявления угроз безопасности информации, обусловленных несанкционированным доступом к ней, проводится в специализированной лаборатории с предварительной установкой необходимого программного обеспечения в компьютерной сети. Для проведения цикла лабораторных работ выделяются два преподавателя: ведущий преподаватель (лектор) и преподаватель для привития практических навыков. При проведении лабораторных работ необходимо отрабатывать задания, в том числе с проведением деловых игр (эпизодов). Лабораторные работы по контролю эффективности защиты информации от несанкционированного доступа проводятся на автоматизированных рабочих местах в специализированных лабораториях. На каждом рабочем месте должен быть преподаватель, развёрнуто необходимое ПО контроля и средства защиты информации. Результаты, полученные в ходе лабораторных работ, используются студентами в качестве исходных данных при отработке итоговых пакетов документов.

8. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Вопросы к зачёту с оценкой:

1. Общие вопросы технической защиты информации. Понятие информация, конфиденциальная информация, злоумышленник.
2. Цели защиты информации
3. Разделение мер защиты информации по способам осуществления. Опишите каждую из перечисленных Вами мер.
4. Базовые организационные меры по защите информации
5. Техническая защита информацию. Объекты технической защиты информации
6. Основные принципы, которым должна удовлетворять система защиты информации с позиции системного подхода.
7. Концептуальные основы защиты информации
8. Доктрина информационной безопасности
9. Законодательные и иные правовые акты в области технической защиты информации
10. Государственные органы в области защиты информации
11. ФСТЭК России
12. Основные задачи ФСТЭК России
13. Общий порядок лицензирования
14. Лицензирование деятельности в области технической защиты информации
15. Контроль за соблюдением лицензионных требований и условий
16. Общий порядок сертификации средств защиты информации
17. Функции федерального органа по сертификации
18. Процедура сертификации
19. Основные схемы проведения сертификации средств защиты информации

20. Порядок сертификации во ФСТЭК России
21. Заключение договора с испытательной лабораторией
22. Аттестация объектов информатизации
23. Структура системы аттестации
24. Функции ФСТЭК в рамках системы аттестации
25. Документы и данные, которые предоставляет заявитель органу по аттестации для проведения испытаний
26. Порядок проведения аттестации объектов информатизации по требованиям безопасности информации
27. Протокол аттестационных испытаний
28. Аттестат соответствия
29. Структура, источники сигнала технического канала утечки информации
30. Классификация технических каналов утечки информации (ТКУИ).
31. Классификация акустических каналов УИ.
32. Показатели и свойства акустических волн. Достоинства и недостатки акустических каналов.
33. Прямой акустический и акустовибрационный КУИ.
34. Структура прямого акустического и акустовибрационного каналов. ФЭ в прямом акустическом канале. Используемые технические средства. Средства противодействия перехвату по каналам. 35. Акустоэлектрический и акусторадиоэлектронный КУИ.
36. Структура каналов. ФЭ в каналах. Используемые технические средства. Средства противодействия перехвату по каналам.
37. Акустопараметрический и акустооптический КУИ.
38. Структура каналов. ФЭ в каналах. Используемые технические средства. Средства противодействия перехвату по каналам.
39. Анализ образования каналов утечки информации на примерах бытовой техники, оргтехники и систем жизнеобеспечения.
40. Изучение технических средств обнаружения и подавления утечки информации по параметрическому каналу
41. Изучение технических средств обнаружения утечки информации по акустооптическому каналу.
42. Классификация электрических каналов УИ.
43. Классификация электрических каналов утечки информации. Причины возникновения утечки информации по электрическим каналам.
44. Канал утечки информации по телефонной линии.
45. Контактные способы подключения. Бесконтактные способы подключения.
46. Способы перехвата речевой информации из телефонной линии. Предотвращение утечки информации по телефонной линии. Методы выявления утечки информации по телефонной линии.
47. Каналы утечки информации по цепям электропитания и заземления.
48. Предотвращение утечки информации по цепям электропитания и заземления. Средства контроля цепей для предотвращения утечки информации.
49. Изучение принципа работы скремблеров.
50. Изучение принципа работы устройств выявления утечки информации по телефонной линии.
51. Классификация оптических КУИ.
52. Визуально-оптический канал. Фототелеканалы. Канал инфракрасного излучения. Волоконно-оптический канал. Системы обнаружения оптических устройств.
53. Классификация электромагнитных КУИ.
54. Назначение ЭМВ. Достоинства перехвата по радиоканалу. Классификация радиоканалов утечки информации.
55. Способы перехвата сигналов. Защита от перехвата.
56. Перехват сигналов связных радиостанций. Перехват радиотелефонных сигналов. Радиомаяки. Радиозакладки. Методы и средства предотвращения утечки информации по радиотехническим каналам. Методы и средства контроля утечки информации по

радиоканалам.
57. Источники электромагнитных излучений и наводок.
58. Причины появления и разновидности электромагнитных излучений и наводок. Источники электромагнитных излучений. Классификация источников электромагнитных излучений и наводок.
59. Использование различных эффектов.
60. Использование эффектов паразитных связей. Использование эффектов электромагнитных наводок. Использование эффектов для образования случайных антенн.
61. Методы защиты информации от утечки через ПЭМИН.
62. Группы технических методов защиты информации от утечки через ПЭМИН. Методы пассивной защиты. Методы активной защиты. Методы и средства контроля ПЭМИН.
63. Изучение принципов действия радиозакладных устройств
64. Сокращения и основные термины. Общие вопросы организации и обеспечения информационной безопасности в техническом аспекте ее защиты.
65. Организационные вопросы обеспечения информационной безопасности
66. Структура технического канала утечки информации
67. Классификация технических каналов утечки информации. Информационный сигнал и его характеристики
68. Понятие информационного сигнала. Аналоговый и цифровой сигналы
69. Модуляция сигналов.
70. Опасные сигналы и их источники
71. Основные показатели технического канала утечки информации
72. Технические каналы утечки акустической информации
73. Основные понятия в области акустики.
74. Классификация акустических каналов утечки информации
75. Средства акустической разведки. Радиозакладки
76. Защита акустической (речевой) информации
77. Звукоизоляция. Зашумление. Средства создания акустических помех
78. Требования и рекомендации по защите речевой информации. Основные требования и рекомендации по защите речевой информации, циркулирующей в защищаемых помещениях
79. Защита информации, циркулирующей в системах звукоусиления и звукового сопровождения кинофильмов. Защита информации при проведении звукозаписи
80. Побочные электромагнитные излучения и наводки
81. Виды паразитной связи. Средства перехвата радиосигналов
82. Упрощенная схема комплекса для перехвата радиосигналов
83. Средства предотвращения утечки информации через ПЭМИН
84. Методы защиты информации в отходах производства
85. Средства инженерной защиты
86. Ограждения территории. Ограждения зданий и помещений. Металлические шкафы, сейфы и хранилища
87. Средства систем контроля и управления доступом
88. Средства технической охраны объектов
89. Средства телевизионной охраны. Средства освещения
90. Средства противодействия наблюдению.
91. Структурное скрытие объектов радиолокационного наблюдения
92. Средства противодействия подслушиванию
93. Средства предотвращения утечки информации с помощью закладных подслушивающих устройств
94. Индикаторы электромагнитных излучений. Радиочастотометры. Автоматизированные поисковые комплексы
95. Досмотровая техника. Металлодетекторы. Эндоскоп
96. Генераторы помех. Рентгеновские комплексы

97. Методы поиска электронных устройств перехвата информации

9. УЧЕБНО- МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) литература

1. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https:// urait.ru/ bcode/537247 (дата обращения: 21.03.2024).

2. Иванов, А. В. Защита речевой информации от утечки по акустоэлектрическим каналам : учебное пособие / А. В. Иванов, В. А. Трушин. — Новосибирск : Новосибирский государственный технический университет, 2012. — 43 с. — ISBN 978-5-7782-1888-8. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https:// www.iprbookshop.ru/44919.html (дата обращения: 21.03.2024). — Режим доступа: для авторизир. пользователей

3. Сагдеев, К. М. Физические основы защиты информации : учебное пособие / К. М. Сагдеев, В. И. Петренко, А. Ф. Чипига. — Ставрополь : Северо- Кавказский федеральный университет, 2015. — 394 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https:// www.iprbookshop.ru/63152.html (дата обращения: 21.03.2024). — Режим доступа: для авторизир. пользователей

4. Никитин, В. Н. Проведение анализа защищённости информации в информационной системе : учебное пособие / В. Н. Никитин. — Хабаровск : ДВГУПС, 2020. — 79 с. — Текст : электронный // Лань : электронно- библиотечная система. — URL: https:// e.lanbook.com/ book/179382 (дата обращения: 21.03.2024). — Режим доступа: для авториз. пользователей.

5. Голиков, А. М. Защита информации в инфокоммуникационных системах и сетях : учебное пособие / А. М. Голиков. — Москва : ТУСУР, 2015. — 284 с. — Текст : электронный // Лань : электронно- библиотечная система. — URL: https:// e.lanbook.com/ book/110336 (дата обращения: 21.03.2024). — Режим доступа: для авториз. пользователей.

б) программное обеспечение и Интернет-ресурсы

№	Наименование	Описание
1	VirtualBox	Бесплатное распространение по лицензии GNU GPL https://www.virtualbox.org/wiki/GPL
2	LibreOffice	Бесплатное распространение по лицензии GNU LGPL https://ru.libreoffice.org/about-us/license/
3	7-Zip	Бесплатное распространение по лицензии GNU LGPL http://www.7-zip.org/license.txt.
4	Fedora Workstation 27	Бесплатное распространение по лицензии GNU GPL http://www.gnu.org/licenses/old-licenses/gpl-2.0.htm.
5	Ubuntu Desktop	Бесплатное распространение по лицензии GNU GPL http://www.gnu.org/licenses/old-licenses/gpl-2.0.html.
6	Debian	Бесплатное распространение по лицензии GNU GPL https://www.debian.org/legal/licenses/
7	Secret Net 6	Сублицензионный договор №34/02/ ИБиИТ/697 от 09.08.2013.
8	Max Patrol Education	Лицензионный договор № 003-17/ЕМ.
9	Positive Technologies Application Firewall Education	Лицензионный договор № 004-17/EAF.

10	amursu.ru	Сайт ФГБОУ ВПО АмГУ
11	http:// www.iprbookshop.ru/	Электронно-библиотечная система IPRbooks - научно-образовательный ресурс для решения задач обучения в России и за рубежом. Уникальная платформа ЭБС IPRbooks объединяет новейшие информационные технологии и учебную лицензионную литературу. ЭБС IPRbooks в полном объеме соответствует требованиям законодательства РФ в сфере образования.
12	https://intuit.ru/	Интернет университет информационных технологи, содержит бесплатные учебные курсы, учебники и методические пособия по всем направлениям подготовки.
13	https://e.lanbook.com/	Электронно- библиотечная система Лань ресурс, включающий в себя как электронные версии книг ведущих издательств учебной и научной литературы (в том числе университетских издательств), так и электронные версии периодических изданий по различным областям знаний.
14	https://urait.ru/	Электронная библиотечная система «ЮРАЙТ», тематические пакеты: математика, физика, инженерно-технические науки, хи- мия. Фонд электронной библиотеки состав- ляет более 4000 наименований и постоянно пополняется новинками, в большинстве своем это учебники и учебные пособия для всех уровней профессионального образования от ведущих научных школ с соблюдением требований новых ФГОСов.

в) профессиональные базы данных и информационные справочные системы

№	Наименование	Описание
1	http://www.learner.org	Профессиональная база данных на английском языке свободного доступа с обучающими текстовыми, аудио, видеоматериалами, тестами.
2	http:// www.ict.edu.ru/	Портал «информационно- коммуникационные технологии в образовании» входит в систему федеральных образовательных порталов и нацелен на обеспечение комплексной информационной поддержки образования в области современных информационных и телекоммуникационных технологий, а также деятельности по применению икт в сфере образования
3	https://fstec.ru	Профессиональная база данных нормативных правовых актов, организационно- распорядительных документов, нормативных и методических документов по технической защите информации. Содержит банк данных угроз безопасности информации
4	https://reestr.minsvyaz.ru	Единый реестр российских программ для электронных вычислительных машин и баз данных. Реестр создан в соответствии со статьей 12.1 федерального закона «об информации, информационных технологиях и о защите информации» в целях расширения использования российских программ для электронных вычислительных машин и баз данных, подтверждения

		их происхождения из Российской федерации, а также в целях оказания правообладателям программ для электронных вычислительных машин или баз данных мер государственной поддержки
5	https:// www.gost.ru/	Каталог международных, межгосударственных и национальных стандартов, действующих технических регламентов.
6	http://www.informika.ru	Сайт ФГАУ, ГНИИиТТ, «ИНФОРМИКА». Институявляется государственным научным предприятием, созданным для обеспечения всестороннего развития и продвижения новых информационных технологий в сферах образования и науки России. Институт создан для осуществления комплексной поддержки развития и использования новых информационных технологий и телекоммуникаций в сфере образования и науки России
7	www.elibrary.ru	Крупнейший российский информационный портал в области науки, технологии, медицины и образования.
8	www.iop.org	В свободном доступе представлены все оглавления и все рефераты. Полные тексты всех статей во всех журналах находятся в свободном доступе в течение 30 дней после даты их онлайновой публикации.
9	www.nature.com archive.neicon.ru	Один из самых старых и авторитетных общенаучных журналов. Публикует исследования, посвящённые широкому кругу вопросов, в основном естественнонаучной тематики. С 2005 года журнал публикует подкасты, где вкратце обсуждаются достижения науки и публикации за последнюю неделю – две.
10	https://www.scopus.com	Международная реферативная база данных научных из-даний scopus.
11	https:// webofknowledge.com	Международная реферативная база данных научных из-даний webofscience.

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Учебные аудитории для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, укомплектованные специализированной мебелью и техническими средствами обучения (ноутбук, проектор, экран), служащими для представления учебной информации большой аудитории. Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой, подключенной к информационно-телекоммуникационной сети «Интернет», и обеспечены доступом в электронную информационно- образовательную среду АмГУ. Помещения для самостоятельной работы обучающихся:

– читальные залы;

– учебные залы вычислительной техники.