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
«ПРОЕКТИРОВАНИЕ ЗАЩИЩЕННЫХ 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

Экзамен 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:

Основной целью освоения дисциплины "Проектирование защищенных автоматизированных систем" является формирование у студентов знаний о защищенных автоматизированных системах, их проектированию, разработке и эксплуатации. Кроме того, целью дисциплины является развитие в процессе обучения системного мышления, необходимого для решения задач по обеспечению необходимого уровня информационной безопасности автоматизированных систем

Задачи дисциплины:

-изучение принципов эксплуатации защищенных автоматизированных систем;
- овладение средствами и методами проектирования и разработки защищенных автоматизированных систем;
- овладение средствами и методами выявления и нейтрализации попыток нарушения безопасности в компьютерных сетях.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина "Проектирование защищенных автоматизированных систем" изучается в 8 семестре и относится к обязательной части дисциплин Блока 1, специальности 10.03.01 "Информационная безопасность", профиля "Безопасность автоматизированных систем (по отраслям или в сфере профессиональной деятельности). Курс учебной дисциплины тесно увязан с другими учебными дисциплинами, в первую очередь с курсами "Физика", "Электротехника, электроника и схемотехника", "Сети и системы передачи информации", "Комплексное обеспечение информационной безопасности автоматизированных систем", "Программно-аппаратные средства защиты информации", "Защита информации от утечки по техническим каналам", позволяющим понять физическую сущность разработки и эксплуатации защищенных автоматизированных систем. Для освоения дисциплины студент должен иметь следующие «входные» знания, умения, навыки и компетенции: - знание базовых понятий в области физики, вычислительной техники, электроники и схемотехники; - способность использовать нормативные правовые документы; - способность анализировать проблемы и процессы; - способность использовать основные законы естественно- научных дисциплин, применять методы математического анализа и моделирования.

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

3.1. Универсальные компетенции и индикаторы их достижения

Категория (группа) универсальных компетенций	Код и наименование универсальной компетенции	Код и наименование индикатора достижения универсальной компетенции
Системное и критическое мышление	УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	ИД-1УК-1- знает принципы сбора, отбора и обобщения информации ИД-2УК-1- умеет соотносить разнородные явления и систематизировать их в рамках избранных видов профессиональной деятельности ИД-3УК-1- имеет практический опыт работы с информационными источниками, опыт научного поиска, создания научных текстов

3.2 Общепрофессиональные компетенции и индикаторы их достижения

Код и наименование общепрофессиональной компетенции	Код и наименование индикатора достижения общепрофессиональной компетенции
ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	ИД-1ОПК-6 знает: систему стандартов и нормативных правовых актов уполномоченных федеральных органов исполнительной власти по лицензированию в области обеспечения з ащиты государственной тайны, технической защиты конфиденциальной информации, систему нормативных правовых актов уполномоченных федеральных органов исполнительной власти по аттестации объектов информатизации и сертификации средств защиты информации, систему правовых и организационных мер, направленных на защиту документальных материалов ограниченного доступа; ИД-2 ОПК-6 умеет: определить политику контроля доступа работников к информации ограниченного доступа, формулировать основные требования, предъявляемы е к физической защите объекта и пропускному режиму в организации; ИД-3 ОПК-6 владеет: действиями (навыками) по применению нормативных правовых актов, нормативных и методических документов, регламентирующие деятельность по защите информации ограниченного доступа в сфере профессиональной деятельности, используя нормативные и методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;
ОПК-10. Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты;	ИД-1ОПК-10- знать: цели и задачи управления информационной безопасностью, основные документы по стандартизации в сфере управления информационной безопасностью, принципы формирования политики информационно й безопасности объекта информатизации, принципы организации информационных систем в соответствии с требованиями по защите информации, особенности комплексного подхода к обеспечению информационной безопасности организации ИД-2ОПК-10- уметь: разрабатывать модели угроз и модели нарушителя объекта информатизации, оценивать информационные риски объекта информатизации, определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите, разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации ИД-3ОПК-10- иметь навыки: участие в

	формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты;
ОПК-12. Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений;	ИД-1ОПК-12- знать: жизненные циклы управляемых процессов: жизненный цикл изделия, жизненный цикл программного продукта, реализуемого в информационной системе, требования Единой системы конструкторской документации и Единой системы программной документации в части разработки технической документации, методы, показатели и критерии технико- экономического обоснования проектных решений при разработке систем и средств обеспечения защиты информации с учетом действующих нормативных и методических документов, ИД-2ОПК-12- уметь: разрабатывать основные показатели технико- экономического обоснования соответствующих проектных решений; ИД-3ОПК-12- иметь навыки: владения подготовки исходных данных для проектирования подсистем, средствами обеспечения защиты информации и для технико- экономического обоснования соответствующих проектных решений

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	Понятия и сущность защищённых автоматизированных систем	8	8				16						50	Опрос, защита лабораторных работ.
2	Общие принципы проектирования и разработки защищённых автоматизированных систем	8	10				18						41.8	Опрос, защита лабораторных работ.
3	Экзамен	8								0.2				
	Итого		18.0		0.0		34.0		0.0	0.2	0.0	0.0	91.8	

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

5.1. Лекции

№ п/п	Наименование темы (раздела)	Содержание темы (раздела)
1	Понятия и сущность защищённых автоматизированных систем	Тема 1: Классификация автоматизированных систем (АС). Информационные технологии, используемые в АС. Жизненный цикл АС. Основные угрозы безопасности информации в автоматизированных системах. Отказоустойчивость АС. Тема 2: Понятия информации и информационных ресурсов. Предмет защиты информации. Объект защиты информации. Понятие информационной безопасности. Понятие политики информационной безопасности. Понятие системы защиты информации. Основные положения безопасности автоматизированных систем. Трехэтапная разработка мер по обеспечению безопасности автоматизированных систем. Стадия выработки требований. Стадия определения способов защиты. Стадия определения функций, процедур и средств безопасности, реализуемых в виде некоторых механизмов защиты. Основные принципы обеспечения информационной безопасности в автоматизированной системе (АС). Принципы, позволяющие реализовать положения по защите АС. Принцип системности. Принцип комплексности. Принцип непрерывной защиты. Тема 3: Понятие угрозы безопасности. Понятие атаки. Понятие злоумышленника.Источники угроз. Окно опасности. Базовые признаки угроз информационной безопасности. Классификация угроз. Доступность информации. Угроза доступности. Целостность информации. Угроза нарушения целостности. Конфиденциальность информации. Угроза нарушения конфиденциальности. Угроза раскрытия параметров АС.

		Методы обеспечения информационной безопасност и. Структуризация методов обеспечения информационной безопасности. Уровни доступа к защищаемой информации. Основные направления и методы реализации угроз информационной безопасности. Классификация злоумышленников. Тема 4: Подходы к обеспечению защиты информации. Сервисы безопасности. Основные и вспомогательные сервисы безопасности. Виды сервисов безопасности. Понятия идентификации, аутентификации и авторизации пользователей. Виды аутентификации. Проблема надежной аутентификации и пути ее решения. Средства и методы хранения эталонных копий аутентификационной информации . Протоколы передачи аутентификационной информации по каналам авто матизированных сетей. Криптографическое обеспечение аутентификации п пользователей. Парольная аутентификация. Виды парольной аутентификации. Преимущества и недостатки парольной аутентификации. Повышение надежности парольной аутентификации. Средства и методы защиты от компрометации и подбора паролей. Биометрическая аутентификация. Общая схема биометрической аутентификации. Преимущества и недостатки биометрической аутентификации. Достоинства и недостатки различных схем биометрической аутентификации. Требования к защите компьютерной информации. Общие положения. Характеристики подходов к защите компьютерной информации. Классификация требований к системам защиты. Формализованные требования к набору и параметрам механизмов защиты. Необходимые требования. Дополнительные требования. Формализованные требования к защите информации от несанкционированного доступа.
2	Общие принципы проектирования и разработки защищённых автоматизированных систем	Тема 5: Последовательность и содержание этапов разработки АС. Методы и средства разработки автоматизированных систем и подсистем безопасности автоматизированных систем. Методы и средства обеспечения отказоустойчивости автоматизированных систем. Критерии оценки защищенности АС. Методы обеспечения информационной безопасности АС. Организация коллективной разработки программного обеспечения АС. Тема 6: Проектирование защищенных АС. Методы проектирования. Содержание этапов проектирования. Основы ведения конструкторской документации. Структура и содержание технического задания. Построение комплексной

		защиты АС. Основы проектирования комплексной защиты информационной безопасности от НСД. Средства обеспечения надежности защищенных АС. Организация хранения информации в защищенных АС. Тема 7: Аттестация АС по требованиям безопасности. Содержание основных документов, определяющих цели, задачи, порядок проведения аттестации. Особенности эксплуатации АС на объекте защиты. Требования и рекомендации по защите государственной тайны и персональных данных при работе АС. Порядок обеспечения защиты информации при эксплуатации АС. Организация технического обслуживания защищенных АС. Средства диагностирования защищенных АС. Аппаратно-программные средства диагностики АС. Аппаратно- программные средства контроля функционирования отдельных элементов, узлов, блоков. Тема 8: Протоколы аутентификации на прикладном уровне. Протокол Kerberos. Протоколы аутентификации на транспортном уровне. Протокол SSL/ TLS. Достоинства и недостатки аутентификации на различных уровнях модели ISO/ OSI. Тема 9: Задачи администрирования подсистем АС. Взаимодействие подсистем АС. Средства администрирования АС. Настройка сетевой подсистемы защищенной АС. Принципы функционирования информационных сервисов АС. Установка и настройка работы информационных сервисов АС. Удаленное администрирование компонентов АС.

5.2. Лабораторные занятия

Наименование темы	Содержание темы
Тема 1: Основные понятия и классификация защищенных автоматизированных систем. Тема 2: Программно-технический уровень защиты автоматизированных систем.	Тема 1: Лабораторная работа № 1. «Анализ сетевого трафика (Wireshark)». Тема 2: Лабораторная работа № 2. «Получение информации о устройстве в сети». Тема 2: Лабораторная работа № 3. «Получение информации о домене (WHOIS)»
Тема 1: Основы эксплуатации защищенных АС. Тема 2: Криптографические протоколы обеспечения безопасности. Тема 3: Основы администрирования АС.	Тема 1: Лабораторная работа № 4. «Основы маршрутизации». Тема 2: Лабораторная работа № 5. «Знакомство с аппаратными маршрутизаторами». Тема 3: Лабораторная работа № 6. «Изучение технологии NAT». Тема 3: Лабораторная работа № 7. «Основы работы IP сетей».

6. САМОСТОЯТЕЛЬНАЯ РАБОТА

№	Наименование темы	Содержание темы (раздела)	Трудоемкость

п/п	(раздела)		в академических часах
1	Понятия и сущность защищённых автоматизированных систем	Подготовка к опросу. Подготовка к защите лабораторных работ.	50
2	Общие принципы проектирования и разработки защищённых автоматизированных систем	Подготовка к опросу. Подготовка к защите лабораторных работ.	41.8

7. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Интегральную модель образовательного процесса по дисциплине формируют технологии методологического уровня: модульно- рейтинговое обучение, технология поэтапного формирования умственных действий, технология развивающего обучения, элементы технологии развития критического мышления. Реализация данной модели предполагает использование следующих технологий стратегического уровня (задающих организационные формы взаимодействия субъектов образовательного процесса), осуществляемых с использованием определенных тактических процедур: – лекционные (вводная лекция, информационная лекция, обзорная лекция, лекцияконсультация, проблемная лекция); – лабораторные (углубление знаний, полученных на теоретических занятиях, решение задач, практическое применение некоторых теоретических знаний); – тренинговые (формирование определенных умений и навыков, формирование алгоритмического мышления); – активизации познавательной деятельности (приемы технологии развития критического мышления через чтение и письмо, работа с литературой, подготовка презентаций по темам домашних работ); – самоуправления (самостоятельная работа студентов, самостоятельное изучение материала). Информационные технологии используются при организации коммуникации со студентами для представления информации, выдачи рекомендаций и консультирования по оперативным вопросам (электронная почта), использование мультимедиа- средств при проведении лекционных и практических занятий. В качестве образовательных технологий при изучении дисциплины используются мультимедийные лекции, на лабораторных занятиях используются современные пакеты программных продуктов, лабораторные стенды. С целью текущего контроля знаний студентов на лабораторных работах проводится контроль выполнения работы. Студентам предлагается обсудить полученные результаты и высказать свое мнение по применению возможных приемов для улучшения показателей либо результатов работы.

8. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Вопросы к экзамену:

1. Классификация автоматизированных систем (АС)
2. Информационные технологии, используемые в АС
3. Жизненный цикл АС
4. Основные угрозы безопасности информации в автоматизированных системах
5. Отказоустойчивость АС
6. Основные понятия и классификация защищенных автоматизированных систем
7. Понятия информации и информационных ресурсов. Предмет защиты информации
8. Понятие информационной безопасности
9. Понятие политики информационной безопасности
10. Понятие системы защиты информации. Основные положения безопасности автоматизированных систем

11. Трехэтапная разработка мер по обеспечению безопасности автоматизированных систем
12. Стадия выработки требований
13. Стадия определения способов защиты
14. Стадия определения функций, процедур и средств безопасности, реализуемых в виде некоторых механизмов защиты
15. Основные принципы обеспечения информационной безопасности в автоматизированной системе
16. Принципы, позволяющие реализовать положения по защите АС
17. Угрозы безопасности информации в защищенных автоматизированных системах
18. Базовые признаки угроз информационной безопасности. Классификация угроз
19. Уровни доступа к защищаемой информации
20. Подходы к обеспечению защиты информации. Сервисы безопасности
21. Виды аутентификации. Проблема надежной аутентификации и пути ее решения
22. Средства и методы хранения эталонных копий аутентификационной информации
23. Средства и методы защиты от компрометации и подбора паролей
24. Требования к защите компьютерной информации
25. Нормативные документы ФСТЭК, регламентирующие защиту информации от несанкционированного доступа
26. Основные подсистемы и группы механизмов защиты АС
27. Последовательность и содержание этапов разработки АС
28. Методы и средства разработки автоматизированных систем и подсистем безопасности автоматизированных систем
29. Методы и средства обеспечения отказоустойчивости автоматизированных систем. Критерии оценки защищенности АС
30. Методы обеспечения информационной безопасности АС. Организация коллективной разработки программного обеспечения АС
31. Проектирование защищенных АС. Основные методы проектирования
32. Основы ведения конструкторской документации
33. Структура и содержание технического задания
34. Построение комплексной защиты АС. Основы проектирования комплексной защиты информационной безопасности от НСД
35. Аттестация АС по требованиям безопасности. Содержание основных документов, определяющих цели, задачи, порядок проведения аттестации
36. Особенности эксплуатации АС на объекте защиты
37. Организация технического обслуживания защищенных АС
38. Аппаратно-программные средства диагностики АС
39. Протоколы аутентификации на прикладном уровне
40. Протоколы аутентификации на транспортном уровне
41. Достоинства и недостатки аутентификации на различных уровнях модели ISO/OSI
42. Задачи администрирования подсистем АС. Средства администрирования АС
43. Настройка сетевой подсистемы защищенной АС
44. Принципы функционирования информационных сервисов АС
45. Установка и настройка работы информационных сервисов АС
46. Удаленное администрирование компонентов АС

9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) литература

1. Карпов, В. В. Технология построения защищенных автоматизированных систем : учебное пособие / В. В. Карпов, В. А. Мельник. — Москва : Российский новый университет, 2009. — 232 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https:// www.iprbookshop.ru/21326.html (дата обращения: 22.03.2024). — Режим доступа: для авторизир. пользователей
2. Гутгарц, Р. Д. Проектирование автоматизированных систем обработки

информации и управления : учебное пособие для вузов / Р. Д. Гутгарц. — 2- е изд., перераб. и доп. — Москва : Издательство Юрайт, 2024. — 351 с. — (Высшее образование). — ISBN 978-5-534-15761-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https:// urait.ru/ bcode/541196 (дата обращения: 22.03.2024).
3. Волкова, Т. В. Основы проектирования компонентов автоматизированных систем : учебное пособие / Т. В. Волкова. — Оренбург : Оренбургский государственный университет, ЭБС АСВ, 2016. — 226 с. — ISBN 978-5-7410-1560-5. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/69921.html (дата обращения: 22.03.2024). — Режим доступа: для авторизир. пользователей
Астапчук, В. А. Корпоративные информационные системы: требования при проектировании : учебное пособие для вузов / В. А. Астапчук, П. В. Терещенко. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2023. — 113 с. — (Высшее образование). — ISBN 978-5-534-08546-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https:// urait.ru/ bcode/514213 (дата обращения: 22.03.2024).

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	Fedora Workstation 27	Бесплатное распространение по лицензии GNU GPL http://www.gnu.org/licenses/old-licenses/gpl-2.0.htm.
4	Ubuntu Desktop	Бесплатное распространение по лицензии GNU GPL http://www.gnu.org/licenses/old-licenses/gpl-2.0.html.
5	Secret Net 6	Сублицензионный договор №34/02/ ИБиИТ/697 от 09.08.2013.
6	Max Patrol Education	Лицензионный договор № 003-17/ЕМ.
7	amursu.ru	Сайт ФГБОУ ВПО АмГУ
8	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.
9	https://intuit.ru/	Интернет университет информационных технологи, содержит бесплатные учебные курсы, учебники и методические пособия по всем направлениям подготовки.
10	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.
11	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.