ФГБОУ ВО «Санкт-Петербургский университет ГПС МЧС России»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Специалитет по специальности
10.05.03 – Информационная безопасность автоматизированных систем

Специализация «Анализ безопасности информационных систем»

Санкт-Петербург

1. Цель и задачи дисциплины

Цель освоения дисциплины::

•раскрытие сущности и значения информационной безопасности и защиты информации, их места в системе национальной безопасности, определение теоретических, концептуальных, методологических и организационных основ обеспечения безопасности информации, классификация и характеристики составляющих информационной безопасности и защиты информации, установление взаимосвязи и логической организации входящих в них компонентов.

Перечень компетенций, формируемых в процессе изучения дисциплины «Основы информационной безопасности»

Компетенции	Содержание
ОПК-1	Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства
ОПК-5	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации

Задачи дисциплины

- сформировать у обучающихся целостной системы знаний в области информационной безопасности как фундаментальной базы информационной культуры высокообразованной личности;
- сформировать у обучающихся практических навыков по защите информации, необходимых для формирования и развития ряда профессионально важных качеств.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

Индикаторы достижения компетенции	Планируемые результаты обучения по дисциплине
ОПК-1.1. Использует современные достижения отечественной и зарубежной науки и техники в области информационных технологий и информационной безопасности	**Знает** сущность и понятие информационной безопасности, характеристику ее составляющих, место информационной безопасности в системе национальной безопасности страны, виды, источники и носители защищаемой информации, источники угроз безопасности информации и меры по их предотвращению; **Умеет** применять современные достижения отечественной и зарубежной науки и техники в области информационных технологий и информационной безопасности
ОПК-1.2. Определяет значение информационных технологий и информационной безопасности для целей государства и общества	**Знает** значение информационной безопасности для целей государства и общества **Умеет** классифицировать защищаемую информацию по видам тайны и секретности
ОПК-1.3. Оценивает и анализирует необходимость внедрения средств автоматизации и информационной безопасности в процессы профессиональной деятельности	**Знает** современные средства и способы обеспечения информационной безопасности **Умеет** классифицировать основные угрозы безопасности информации
ОПК-5.1. Использует основные нормативные правовые акты, стандарты и методические документы в области защиты информации и информационной безопасности	**Знает** перечень основных нормативных правовых актов, стандартов и методических документов в области защиты информации и информационной безопасности **Умеет** применять нормативные правовые акты, стандарты и методические документы в области защиты информации и информационной безопасности

3. Место дисциплины в структуре ОПОП

Дисциплина «Основы информационной безопасности» относится к обязательной части, образовательной программы специалитета по специальности **10.05.03 – Информационная безопасность автоматизированных систем**, специализация - **Анализ безопасности информационных систем**

4. Структура и содержание

Дисциплина «Основы информационной безопасности» реализуется:

Для очной формы обучения в рамках обязательной части образовательной программы в объеме 108 академических часов (3 зачетных единицы).

4.1 Распределение трудоемкости дисциплины по видам работ по семестрам для очной формы обучения

Вид учебной работы	Трудоемкость		
	з.е.	час.	по семестрам
			4
Общая трудоемкость дисциплины по учебному плану	**3**	**108**	**108**
Контактная работа, в том числе:		**54**	**54**
Аудиторные занятия		**54**	**54**
Лекции (Л)		20	20
Практические занятия (ПЗ)		34	34
Самостоятельная работа (СРС)		**54**	**54**
Зачет с оценкой		+	+

4.2 Разделы и темы дисциплины «Основы информационной безопасности» и виды занятий

№ п/п	Наименование разделов и тем	Всего часов	Количество часов по видам занятий, в том числе Практические занятия		Самостоятельная работа	Контроль
			Лекции	Практические занятия		
1	**2**	**3**	**4**	**5**	**7**	**8**
1.	Тема 1. Сущность и понятие информационной безопасности	16	6	4	6	
2.	Тема 2. Значение информационной безопасности и ее место в системе национальной безопасности	14	2	4	8	
3.	Тема 3. Сущность и понятие защиты информации	16	2	6	8	
4.	Тема 4. Состав и классификация носителей защищаемой информации	14	2	4	8	
5.	Тема 5. Понятие и структура угроз защищаемой информации	16	2	6	8	
6.	Тема 6. Объекты защиты информации	14	2	4	8	
7.	Тема 7. Классификация видов, методов и средств защиты информации	18	4	6	8	
8.	Зачет с оценкой	+				+
Итого		**108**	**20**	**34**	**54**	

4.3 Тематический план для обучающихся

Тема 1. Сущность и понятие информационной безопасности

Лекции. Предмет и задачи курса. Значение и место курса в, подготовке специалистов, по защите информации. Научная и учебная взаимосвязь курса с другими дисциплинами. Разделы и темы, их распределение по видам аудиторных занятий. Становление и развитие понятия "информационная безопасность". Современные подходы к определению понятия. Сущность информационной безопасности. Объекты информационной безопасности. Связь информационной безопасности с информатизацией общества. Структура информационной безопасности. Определение понятия информационная безопасность".

Практические занятия. Семантический анализ базовых понятий предметной области. Предметный анализ стандартов в области информационной безопасности и защиты информации.

Самостоятельная работа. Абстрактная модель системы защиты информации: основные понятия. Основы формальной теории защиты информации. Модели дискреционного доступа. Модели мандатного доступа. Ролевые модели доступа. Модели безопасности информационных потоков. Акты регуляторов в сфере защиты информации.

Рекомендуемая литература

основная: [1,2]

дополнительная: [1]

Тема 2. Значение информационной безопасности и ее место в системе национальной безопасности

Лекция. Значение информационной, безопасности для субъектов информационных отношений. Связь между информационной безопасностью и безопасностью информации. Понятие и современная концепция национальной безопасности. Место информационной, безопасности, в системе национальной безопасности.

Практическое занятие. Исследование генераторов паролей с заданными требованиями. Построение модели угроз информационной системы.

Самостоятельная работа. Краткая история защиты информации в России.

Рекомендуемая литература

основная: [1,2]

дополнительная: [1]

Тема 3. Сущность и понятие защиты информации

Лекция. Существующие подходы к содержательной части понятия "защита информации" и способы реализации содержательной части. Методологическая основа раскрытия сущности и определения понятия защиты информации. Формы выражения нарушения статуса информации. Обусловленность статуса информации ее уязвимостью. Понятие уязвимости информа-

ции. Формы проявления уязвимости информации. Виды уязвимости информации. Понятие "утечка информации". Соотношение форм и видов уязвимости информации. Содержательная часть понятия "защита информации". Способ реализации содержательной части защиты информации.

Практическое занятие. Построение модели утечки информационной безопасности.

Самостоятельная работа. Определение понятия "защита информации", его соотношение с понятием, сформулированным в ГОСТ Р 50922-96. "Защита информации. Основные термины и определения".

Рекомендуемая литература

основная: [1,2]

дополнительная: [1,2]

Тема 4. Состав и классификация носителей защищаемой информации

Лекция. Понятие носитель защищаемой информации". Соотношение между носителем и источником информации. Состав носителей защищаемой информации. Способы фиксирования информации в носителях. Виды отображения информации в носителях. Методы воспроизведения отображенной информации в носителях информации. Носители письменной, видовой, излучаемой информации. Опосредованные носители защищаемой информации. Свойства и значение типов носителей защищаемой информации.

Практическое занятие. Исследование уязвимости информации. Исследование видов уязвимости. Исследование форм уязвимости.

Самостоятельная работа. Средства обнаружения технических каналов утечки информации. Средства препятствования утечке информации по техническим каналам. Электронные устройства негласного получения информации: «жучки», записывающие устройства, подслушивающие устройства. Ответственность за незаконный оборот специальных технических средств, предназначенных для негласного получения информации.

Рекомендуемая литература

основная: [1,2]

дополнительная: [1,2]

Тема 5. Понятие и структура угроз защищаемой информации

Лекция. Современные подходы к понятию угрозы защищаемой информации. Связь угрозы защищаемой информации с уязвимостью информации. Признаки и составляющие угрозы: явления, факторы, условия. Понятие угрозы защищаемой информации. Структура явлений как сущностного выражения угрозы защищаемой информации. Структура факторов, создающих возможность дестабилизирующего воздействия на информацию.

Практическое занятие. Построение алгоритмов социальной инженерии и способы защиты от них. Построение алгоритмов принятия решения.

Самостоятельная работа. Методы сокрытия информации в сетевых пакетах. Методы сокрытия информации в исполняемых файлах

Рекомендуемая литература
основная: [1,2]
дополнительная: [1,3]

Тема 6. Объекты защиты информации

Лекция. Понятие объекта защиты. Носители информации как конечные объекты защиты. Особенности отдельных видов носителей как объектов защиты. Состав объектов хранения письменных и видовых носителей информации, подлежащих защите. Состав подлежащих защите технических средств отображения, обработки, хранения, воспроизведения передачи информации.

Практическое занятие. Анализ обрабатываемой информации с точки зрения видов тайн и формирование требований к ее защите. Анализ обрабатываемой информации с точки зрения ее защиты.

Самостоятельная работа. Другие объекты защиты информации. Виды и способы дестабилизирующего воздействия на объекты защиты.

Рекомендуемая литература
основная: [1,2]
дополнительная: [1,3]

Тема 7. Классификация видов, методов и средств защиты информации

Лекция. Виды защиты информации, сферы их действия. Классификация методов защиты информации. Универсальные методы защиты информации, область их применения. Области применения организационных, криптографических и инженерно-технических методов защиты информации. Понятие и классификация средств защиты информации.

Практическое занятие. Сравнение криптографических и технических средств защиты.

Самостоятельная работа. Назначение программных, криптографических и технических средств защиты.

Рекомендуемая литература
основная: [1,2]
дополнительная: [1,3]

5. Методические рекомендации по организации изучения дисциплины «Основы информационной безопасности»

При реализации программы дисциплины «Основы информационной безопасности» используются лекционные и практические занятия.

Общими целями занятий являются:

–обобщение, систематизация, углубление, закрепление теоретических знаний по конкретным темам дисциплины;

–формирование умений применять полученные знания на практике, реализация единства интеллектуальной и практической деятельности;

–выработка при решении поставленных задач профессионально значимых качеств: самостоятельности, ответственности, точности, творческой инициативы.

Целями лекции являются:

– систематизированные основы научных знаний по дисциплине, раскрывать состояние и перспективы развития соответствующей области науки и техники;

– концентрировать внимание обучающихся на наиболее сложных и узловых вопросах;

– стимулировать их активную познавательную деятельность и способствовать формированию творческого мышления.

В ходе практического занятия обеспечивается процесс активного взаимодействия обучающихся с преподавателем; приобретаются практические навыки и умения. Цели практического занятия: выработка практических умений и приобретение навыков, закрепление пройденного материала по соответствующей теме дисциплины.

Самостоятельная работа обучающихся направлена на углубление и закрепление знаний, полученных на лекциях и других занятиях, выработку навыков самостоятельного активного приобретения новых, дополнительных знаний, подготовку к предстоящим занятиям.

6. Оценочные материалы по дисциплине «Основы информационной безопасности»

Текущий контроль успеваемости обеспечивает оценивание хода освоения дисциплины, проводится в соответствии с содержанием дисциплины по видам занятий в форме опроса / тестирования.

Промежуточная аттестация обеспечивает оценивание промежуточных и окончательных результатов обучения по дисциплине, проводится в форме зачета с оценкой.

6.1. Примерные оценочные материалы:

6.1.1. Текущего контроля

Типовые вопросы для опроса

– дайте определение основным терминам в сфере информационной безопасности и защиты информации (угроза, уязвимость, конфиденциальность, целостность, доступность);

– назовите основные стандарты в области информационной безопасности и защиты информации;

– назовите регуляторов в сфере защиты информации и их основные нормативно-правовые акты;

– перечислите и дайте определение основным моделям доступа.

– назовите виды ответственности за нарушения в сфере информационной безопасности и защиты информации;

– перечислите статьи Уголовного кодекса РФ в части ответственности за преступления в сфере компьютерной информации;

– назовите статью Уголовного кодекса РФ, регламентирующую ответственность за незаконный оборот специальных технических средств, предназначенных для негласного получения информации.

– приведите права регуляторов в части наложения административных взысканий за нарушения в сфере информационной безопасности и защиты информации

Типовые задания для тестирования

Правильный вариант ответа отмечен знаком +

1) К правовым методам, обеспечивающим информационную безопасность, относятся:

- Разработка аппаратных средств обеспечения правовых данных

- Разработка и установка во всех компьютерных правовых сетях журналовучета действий

+ Разработка и конкретизация правовых нормативных актов обеспечениябезопасности

2) Основными источниками угроз информационной безопасности являются все указанное в списке:

- Хищение жестких дисков, подключение к сети, инсайдерство

+ Перехват данных, хищение данных, изменение архитектуры системы

- Хищение данных, подкуп системных администраторов, нарушение регламента работы

3) Виды информационной безопасности:

+ Персональная, корпоративная, государственная

- Клиентская, серверная, сетевая

- Локальная, глобальная, смешанная

4) Цели информационной безопасности – своевременное обнаружение, предупреждение:

+ несанкционированного доступа, воздействия в сети

- инсайдерства в организации

- чрезвычайных ситуаций

5) Основные объекты информационной безопасности:

+ Компьютерные сети, базы данных

- Информационные системы, психологическое состояние пользователей

- Бизнес-ориентированные, коммерческие системы

6) Основными рисками информационной безопасности являются:

- Искажение, уменьшение объема, перекодировка информации

- Техническое вмешательство, выведение из строя оборудования сети

+ Потеря, искажение, утечка информации

7) К основным принципам обеспечения информационной безопасности относится:

+ Экономической эффективности системы безопасности

- Многоплатформенной реализации системы

- Усиления защищенности всех звеньев системы

8) Основными субъектами информационной безопасности являются:

- руководители, менеджеры, администраторы компаний

+ органы права, государства, бизнеса

- сетевые базы данных, фаерволлы

9) К основным функциям системы безопасности можно отнести все перечисленное:

+ Установление регламента, аудит системы, выявление рисков

Установка новых офисных приложений, смена хостинг-компании

Внедрение аутентификации, проверки контактных данных пользователей

10) Принципом информационной безопасности является принцип недопущения:

+ Неоправданных ограничений при работе в сети (системе)

- Рисков безопасности сети, системы

- Презумпции секретности

11) Принципом политики информационной безопасности является принцип:

+ Невозможности миновать защитные средства сети (системы)

- Усиления основного звена сети, системы

- Полного блокирования доступа при риск-ситуациях

12) Принципом политики информационной безопасности является принцип:

+ Усиления защищенности самого незащищенного звена сети (системы)

- Перехода в безопасное состояние работы сети, системы

- Полного доступа пользователей ко всем ресурсам сети, системы

13) Принципом политики информационной безопасности является принцип:

+ Разделения доступа (обязанностей, привилегий) клиентам сети (системы)

- Одноуровневой защиты сети, системы

- Совместимых, однотипных программно-технических средств сети, системы

14) К основным типам средств воздействия на компьютерную сеть относится:

- Компьютерный сбой

+ Логические закладки («мины»)

- Аварийное отключение питания

15) Когда получен спам по e-mail с приложенным файлом, следует:

- Прочитать приложение, если оно не содержит ничего ценного – удалить

- Сохранить приложение в парке «Спам», выяснить затем IP-адрес гене-

ратора спама

+ Удалить письмо с приложением, не раскрывая (не читая) его

16) Принцип Кирхгофа:

- Секретность ключа определена секретностью открытого сообщения

- Секретность информации определена скоростью передачи данных

+ Секретность закрытого сообщения определяется секретностью ключа

17) ЭЦП – это:

- Электронно-цифровой преобразователь

+ Электронно-цифровая подпись

- Электронно-цифровой процессор

18) Наиболее распространены угрозы информационной безопасности корпоративной системы:

- Покупка нелицензионного ПО

+ Ошибки эксплуатации и неумышленного изменения режима работы системы

- Сознательного внедрения сетевых вирусов

19) Наиболее распространены угрозы информационной безопасности сети:

- Распределенный доступ клиент, отказ оборудования

- Моральный износ сети, инсайдерство

+ Сбой (отказ) оборудования, нелегальное копирование данных тест_20) Наиболее распространены средства воздействия на сеть офиса:

- Слабый трафик, информационный обман, вирусы в интернет

+ Вирусы в сети, логические мины (закладки), информационный перехват

- Компьютерные сбои, изменение администрирования, топологии

21) Утечкой информации в системе называется ситуация, характеризуемая:

+ Потерей данных в системе

- Изменением формы информации

- Изменением содержания информации

22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:

+ Целостность

- Доступность

- Актуальностьl

23) Угроза информационной системе (компьютерной сети) – это:

+ Вероятное событие

- Детерминированное (всегда определенное) событие

- Событие, происходящее периодически

24) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:

- Регламентированной

- Правовой

+ Защищаемой

25) Разновидностями угроз безопасности (сети, системы) являются все перчисленное в списке:

+ Программные, технические, организационные, технологические

- Серверные, клиентские, спутниковые, наземные

- Личные, корпоративные, социальные, национальные

26) Окончательно, ответственность за защищенность данных в компьютерной сети несет:

+ Владелец сети

- Администратор сети

- Пользователь сети

27) Политика безопасности в системе (сети) – это комплекс:

+ Руководств, требований обеспечения необходимого уровня безопасности

- Инструкций, алгоритмов поведения пользователя в сети

- Нормы информационного права, соблюдаемые в сети

28) Наиболее важным при реализации защитных мер политики безопасности является:

- Аудит, анализ затрат на проведение защитных мер

- Аудит, анализ безопасности

+ Аудит, анализ уязвимостей, риск-ситуаций

6.1.2. Промежуточной аттестации

Примерный перечень вопросов, выносимых на зачет с оценкой

1. Значение и место курса в, подготовке специалистов, по защите информации
2. Анализ нормативных источников, научной и учебной литературы
3. Становление и развитие понятия "информационная безопасность". Современные подходы к определению понятия.
4. Сущность информационной безопасности. Объекты информационной безопасности
5. Связь информационной безопасности с информатизацией общества
6. Значение информационной, безопасности для субъектов информационных
7. Место информационной, безопасности, в системе национальной безопасности.
8. Существующие подходы к содержательной части понятия "защита информации" и способы реализации содержательной части
9. Понятие уязвимости информации
10. Методологическая основа раскрытия сущности и определения понятия защиты информации.
11. Понятие носитель защищаемой информации". Соотношение между носителем и источником информации.
12. Виды отображения информации в носителях
13. Современные подходы к понятию угрозы защищаемой информации

14. Понятие угрозы защищаемой информации. Понятие объекта защиты.

15. Состав объектов хранения письменных и видовых носителей информации, подлежащих защите.

16. Другие объекты защиты информации. Виды и способы дестабилизирующего воздействия на объекты защиты

17. Виды защиты информации, сферы их действия Классификация методов защиты информации

18. Понятие и классификация средств защиты информации.

19. Назначение программных, криптографических и технических средств защиты.

6.2. Шкала оценивания результатов промежуточной аттестации и критерии выставления оценок

Система оценивания включает:

Форма контроля	Показатели оценивания	Критерии выставления оценок	Шкала оценивания
зачет с оценкой	правильность и полнота ответа	дан правильный, полный ответ на поставленный вопрос, показана совокупность осознанных знаний по дисциплине, доказательно раскрыты основные положения вопросов; могут быть допущены недочеты, исправленные самостоятельно в процессе ответа.	отлично
		дан правильный, недостаточно полный ответ на поставленный вопрос, показано умение выделить существенные и несущественные признаки, причинно-следственные связи; могут быть допущены недочеты, исправленные с помощью преподавателя.	хорошо
		дан недостаточно правильный и полный ответ; логика и последовательность изложения имеют нарушения; в ответе отсутствуют выводы.	удовлетворительно
		ответ представляет собой разрозненные знания с существенными ошибками по вопросу; присутствуют фрагментарность, нелогичность изложения; дополнительные и уточняющие вопросы не приводят к коррекции ответа на вопрос.	неудовлетворительно

7. Ресурсное обеспечение дисциплины «Основы информационной безопасности»

7.1. Лицензионное и свободно распространяемое программное обеспечение

Перечень лицензионного и свободно распространяемого программного обеспечения:

- Статистическая диалоговая система STADIA [ПО-6FF-561] - Статистическая диалоговая система [Лицензионное. Номер в Едином реестре российских программ для электронных вычислительных машин и баз данных - 9064]

- SMath Studio [ПО-A68-516] - Программное обеспечение для вычисления математических выражений и построения графиков функций [Свободно распространяемое. Номер в Едином реестре российских программ для электронных вычислительных машин и баз данных - 12849]

- МойОфис Образование [ПО-41B-124] - Полный комплект редакторов текстовых документов и электронных таблиц, а также инструментарий для работы с графическими презентациями [Свободно распространяемое. Номер в Едином реестре российских программ для электронных вычислительных машин и баз данных - 4557]

- Astra Linux Common Edition релиз Орел [ПО-25B-603] - Операционная система общего назначения "Astra Linux Common Edition" [Коммерческая (Full Package Product). Номер в Едином реестре российских программ для электронных вычислительных машин и баз данных - 4433]

7.2. Профессиональные базы данных и информационные справочные системы

1. Информационная система «Единое окно доступа к образовательным ресурсам» [Электронный ресурс]. – Режим доступа: http://window.edu.ru/, доступ только после самостоятельной регистрации
2. Научная электронная библиотека «eLIBRARY.RU» [Электронный ресурс]. – Режим доступа: https://www.elibrary.ru/, доступ только после самостоятельной регистрации
3. Электронная библиотека Санкт-Петербургского университета ГПС МЧС России: http://elib.igps.ru
4. Электронно-библиотечная система IPRBOOK: http://www.iprbookshop.ru/
5. Электронно-библиотечная система ЛАНЬ: https://e.lanbook.com/

7.3. Литература

Основная литература:

1. Нестеров, С. А. Основы информационной безопасности / С. А. Нестеров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2023. — 324 с. —

ISBN 978-5-507-48149-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/341267 (дата обращения: 29.08.2023). — Режим доступа: для авториз. пользователей.

2. Петренко, В. И. Теоретические основы защиты информации : учебное пособие / В. И. Петренко. — Ставрополь : СКФУ, 2015. — 222 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/155247 (дата обращения: 29.08.2023). — Режим доступа: для авториз. пользователей.

Дополнительная литература:

1. Безопасность информационных систем и защита информации в МЧС России: учебное пособие: [гриф МЧС] / Ю.И. Синещук [и др.]; ред. В.С. Артамонов; С.-Петерб. гос. ун-т гос. противопож. службы МЧС России. – СПб.: СПбУ ГПС МЧС России, 2012. – 300 с. Режим доступа: http://elib.igps.ru/?4&type=card&cid=ALSFR-6d86bbe6-aeac-49db-bc2e-068c7a55cb8d&remote=false

2. Ерохин, В. В. Безопасность информационных систем : учебное пособие / В. В. Ерохин, Д. А. Погонышева, И. Г. Степченко. — 4-е изд., стер. — Москва : ФЛИНТА, 2022. — 184 с. — ISBN 978-5-9765-1904-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/232457 (дата обращения: 29.08.2023). — Режим доступа: для авториз. пользователей.

3. Мартынов А.П. Информационная безопасность и защита информации : учебное пособие / Мартынов А.П., Мартынова И.А., Русаков А.А.. — Москва : Ай Пи Ар Медиа, 2023. — 122 с. — ISBN 978-5-4497-2247-8. — Текст : электронный // IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/131797.html (дата обращения: 29.08.2023). — Режим доступа: для авторизир. пользователей. - DOI: https://doi.org/10.23682/131797

7.4 Материально-техническое обеспечение дисциплины «Основы информационной безопасности»

Для проведения и обеспечения занятий используются помещения, которые представляют собой учебные аудитории для проведения учебных занятий, предусмотренных программой специалитета, оснащенные оборудованием и техническими средствами обучения: автоматизированное рабочее место преподавателя, маркерная доска, мультимедийный проектор, документ-камера, посадочные места обучающихся.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде университета.

Автор: д.т.н., профессор Буйневич М.В., к.т.н., доцент Матвеев А.В.