МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Чувашский государственный университет имени И. Н. Ульянова»

Факультет информатики и вычислительной техники

Кафедра вычислительной техники

«УТВЕРЖДАЮ»
Проректор по учебной работе

_____ И.Е. Поверинов

31 августа 2017 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Специальность: 10.05.03 – Информационная безопасность автоматизированных систем

Квалификация выпускника: Специалист по защите информации

Специализация: Безопасность открытых информационных систем

Чебоксары – 2017

Рабочая программа основана на требованиях Федерального государственного образовательного стандарта высшего образования по специальности 10.05.03 Информационная безопасность автоматизированных систем, утвержденного приказом Министерства образования и науки 01.12.2016 г. №1509

СОСТАВИТЕЛЬ (СОСТАВИТЕЛИ):

старший преподаватель _____ О.А. Лобастова

доцент, к.т.н. _____ А.А. Андреева

ОБСУЖДЕНО:

на заседании кафедры вычислительной техники «30» августа 2017г., протокол № 1

заведующий кафедрой _____ А.В. Щипцова

СОГЛАСОВАНО:

Методическая комиссия факультета информатики и вычислительной техники «30» августа 2017г., протокол № 1

Декан факультета _____ А.В. Щипцова

Директор научной библиотеки _____ Н. Д. Никитина

Начальник управления информатизации _____ И. П. Пивоваров

Начальник учебно-методического управления _____ В. И. Маколов

Оглавление

1. Цель и задачи обучения по дисциплине

Целью преподавания дисциплины является подготовка студентов в области проектирования средств обеспечения информационной безопасности автоматизированных систем и привитие навыков разработки и анализа компонентов автоматизированных систем.

Задачи дисциплины:

- изучение моделей угроз и модели нарушителя информационной безопасности автоматизированной системы;
- изучение методов анализа проектных решений по обеспечению безопасности автоматизированных систем;
- получение практических навыков проектирования средств защиты информации автоматизированной системы;
- изучение методов анализа угроз и уязвимостей проектируемых и эксплуатируемых автоматизированных систем;
- получение навыков использования программно-аппаратных средств защиты информации.

2. Место дисциплины в структуре основной образовательной программы (ООП)

Дисциплина реализуется в рамках обязательных дисциплин базовой части образовательной программы.

Для успешного усвоения данной дисциплины необходимо, чтобы студент владел знаниями, умениями и навыками, сформированными в процессе изучения дисциплин:

«Языки программирования» – разрабатывать программы на языке программирования высокого уровня;

«Основы информационной безопасности» – основные средства и способы обеспечения информационной безопасности, подходы к построению систем защиты информации;

«Безопасность операционных систем» – использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем;

«Безопасность систем баз данных» – уметь применять средства обеспечения безопасности данных, реализовывать политику безопасности баз данных, владеть навыками эксплуатации и администрирования баз данных с учетом требований по обеспечению информационной безопасности;

«Организация ЭВМ и вычислительных систем» – знать архитектуру, принципы функционирования, элементную базу современных компьютеров, вычислительных и телекоммуникационных систем, уметь анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей информационной безопасности автоматизированных систем.

Дисциплина является предшествующей для преддипломной практики и государственной итоговой аттестации.

3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ООП

Процесс обучения по дисциплине направлен на формирование следующих профессиональных компетенций:

- способность к освоению новых образцов программных, технических средств и информационных технологий (ОПК-8);
- способность разрабатывать политику информационной безопасности автоматизированной системы (ПК-11);

- способность проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-14);
- способность обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций (ПК-25).

В результате обучения по дисциплине, обучающийся должен (ЗУН):

знать:

- программно-аппаратные средства защиты информации в типовых операционных системах (З1),
- программно-аппаратные средства защиты информации в системах управления базами данных (З2),
- программно-аппаратные средства защиты информации в компьютерных сетях (З3);
- нормативные правовые акты, используемые при программно-аппаратной защите информации (З4);
- угрозы безопасности информации (З5);

уметь:

- проводить выбор программно-аппаратных средств защиты информации для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы (У1);
- разрабатывать и исследовать аналитические и компьютерные модели автоматизированных систем и подсистем безопасности автоматизированных систем (У2);
- применять нормативные правовые акты при программно-аппаратной защите информации (У3);
- определять информационные ресурсы, подлежащие защите, угрозы безопасности информации (У4);

владеть навыками:

- применения нормативно-правовых актов при программно-аппаратной защите информации (Н1);
- определения информационных ресурсов, подлежащих защите (Н2);
- эксплуатации и администрирования (в части, касающейся разграничения доступа, аутентификации и аудита) баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности (Н3);
- использования программно-аппаратных средств обеспечения безопасности сетей ЭВМ (Н4).

4. Структура и содержание дисциплины

Образовательная деятельность по дисциплине проводится:

– в форме контактной работы обучающихся с педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях (далее – контактная работа);

– в форме самостоятельной работы.

Контактная работа включает в себя занятия лекционного типа, занятия семинарского типа (семинары, практические занятия, лабораторные работы, практикумы), групповые и (или) индивидуальные консультации, в том числе в электронной информационно-образовательной среде.

Обозначения:

Л – лекции, л/р – лабораторные работы, п/р – практические занятия, КСР – контроль самостоятельной работы, СРС – самостоятельная работа студента, ИФР – интерактивная форма работы, К – контроль.

4.1. Содержание дисциплины

Содержание	Формируемые компетенции	Формируемые ЗУН
Раздел 1. Защита от несанкционированного доступа	ОПК-8, ПК-11, ПК-14, ПК-25	З1, З2, З3,У1, У2, Н1, Н2
1.1. Назначение и функции программно-аппаратных средств защиты информации		
1.2. Средства авторизации и аутентификации пользователей автоматизированных систем		
1.3. Методы защиты информации от несанкционированного доступа		
1.4. Методы обеспечения целостности аппаратного обеспечения автоматизированных систем		
Раздел 2. Защита от вредоносных программ	ОПК-8, ПК-14, ПК-25	З1, У1, Н2
2.1. Анализ уязвимости программного обеспечения автоматизированных систем		
2.2. Методы защиты от вредоносных программ		
Расчетно-графическая работа	ОПК-8, ПК-11	У1, Н1
Зачет	ОПК-8, ПК-11, ПК-14, ПК-25	З1, З2, З3,У1, У2, Н1, Н2

4.2. Объем дисциплины, виды учебной работы обучающихся по очной форме обучения

Содержание	Всего, час	Контактная работа, час			СРС, час	ИФР, час	К, час
		Л	л/р	КСР			
Раздел 1. Защита от несанкционированного доступа							
1.1. Назначение и функции программно-аппаратных средств защиты информации	7	2			5	2	
1.2. Средства авторизации и аутентификации пользователей автоматизированных систем	23	6	8		9	6	
1.3. Методы защиты информации от несанкционированного доступа	23	6	8		9	6	
1.4. Методы обеспечения целостности аппаратного обеспечения автоматизированных систем	11	6			5	6	
Раздел 2. Защита от вредоносных программ							
2.1. Анализ уязвимости программного обеспечения автоматизированных систем	18	6	8		4	6	
2.2. Методы защиты от вредоносных программ	20	6	8		6	6	
РГР	4				4		
Зачет	2			2			
Итого	**108 3 з.е.**	**32**	**32**	**2**	**42**	**32**	

5. Содержание разделов дисциплины

5.1. Лекции и лабораторные работы

Раздел 1. Защита от несанкционированного доступа

Тема 1.1. Назначение и функции программно-аппаратных средств защиты информации.

Лекция 1. Цели и задачи курса. Содержание дисциплины. Рекомендуемая литература. Основные понятия и определения. Эскалация привилегий. Функции программно-аппаратных средств защиты информации. Содержание и задачи процесса обеспечения информационной безопасности с использованием программно-аппаратных средств.

Тема 1.2.Средства авторизации и аутентификации пользователей автоматизированных систем.

Лекция 2. Применение парольных систем. Аутентификация с помощью физических предметов хранящихся у пользователя. Электронные ключи. Пластиковые карты.

Лекция 3. Особенности идентификации и аутентификации с помощью биометрических характеристик пользователей. Использование криптографических методов в системах аутентификации.

Лекция 4. Протоколы и алгоритмы аутентификации и идентификации пользователей в современных операционных системах ОС.

Лабораторное занятие 1. Исследование систем идентификации на основе устройств Bluetooth.

Тема 1.3.Методы защиты информации от несанкционированного доступа

Лекция 5. Требования к специализированным средствам защиты информации от несанкционированного доступа.

Лекция 6. Контроль целостности системного программного обеспечения и аппаратных средств.

Лекция 7. Организация виртуальных логических дисков. Шифрование пользовательских виртуальных дисков. Формирование ключевой информации.

Лабораторное занятие 2. Создание шифрованных пользовательских виртуальных дисков.

Тема 1.4.Методы обеспечения целостности аппаратного обеспечения автоматизированных систем

Лекция 8. Средства обеспечения целостности составных частей компьютера. Защита узлов и блоков компьютеров от несанкционированного доступа.

Лекция 9. Средства контроля доступа к рабочему месту пользователя.

Лекция 10. Программные средства выявления фактов физического доступа к системному блоку и узлам автоматизированной системы.

Раздел 2. Защита от вредоносных программ

Тема 2.1.Анализ уязвимости программного обеспечения автоматизированных систем

Лекция 11. Понятие вредоносного кода. Программные закладки. Классификация программных закладок. Предпосылки к внедрению программных закладок.

Лекция 12. Уязвимости программного обеспечения. Принципы построения политики безопасности.

Лекция 13. Уязвимости политики безопасности. Человеческий фактор. Сокрытие программных закладок.

Лабораторное занятие 3. Настройка политики безопасности операционной системы.

Тема 2.2.Методы защиты от вредоносных программ

Лекция 14. Сигнатурное и эвристическое сканирование. Аппаратные средства противодействия вредоносному коду.

Лекция 15. Контроль целостности программного обеспечения. Мониторинг информационных потоков. Изолированная программная среда.

Лекция 16. Цифровая подпись исполняемого кода. Шифрование исполняемого кода. Средства анализа уязвимостей.

Лабораторное занятие 4. Анализ защищенности изолированной программной среды.

6. Образовательные технологии

В соответствии со структурой образовательного процесса по дисциплине применяются следующие технологии:

- диагностики;
- целеполагания;
- управления процессом освоения учебной информации;
- применения знаний на практике, поиска новой учебной информации;
- организации совместной и самостоятельной деятельности обучающихся (учебно-познавательной, научно-исследовательской, частично-поисковой, репродуктивной, творческой и пр.);
- контроля качества и оценивания результатов образовательной деятельности (технология оценивания качества знаний, рейтинговая технология оценки знаний и др.)

В соответствии с требованиями ФГОС ВО для реализации компетентностного подхода при обучении дисциплине предусмотрено широкое использование в учебном процессе активных и интерактивных методов проведения занятий:

При обучении дисциплине применяются следующие формы занятий:

- лекции, направленные на получение новых и углубление научно-теоретических знаний, в том числе вводная лекция, информационная лекция, обзорная лекция, лекция-консультация, проблемная лекция, лекции-дискуссии, лекции-беседы и др.;
- лабораторные занятия, проводимые под руководством преподавателя в учебной лаборатории с использованием компьютеров и учебного оборудования, направленные на закрепление и получение новых умений и навыков, применение знаний и умений, полученных на теоретических занятиях, при решении практических задач и др.

Все занятия обеспечены мультимедийными средствами (SMARTдоски, проекторы, экраны) для повышения качества восприятия изучаемого материала. В образовательном процессе широко используются информационно-коммуникационные технологии.

Самостоятельная работа студентов – это планируемая работа студентов, выполняемая по заданию при методическом руководстве преподавателя, но без его непосредственного участия. Формы самостоятельной работы студентов определяются содержанием учебной дисциплины, степенью подготовленности студентов. Они могут иметь учебный или учебно-исследовательский характер: анализ литературы по теме, подготовка к лабораторным работам, разработка проекта и др.

Формами контроля самостоятельной работы выступают проверка письменных отчётов по результатам выполненных заданий и лабораторных работ; проверка расчетно-графической работы. Результаты самостоятельной работы учитываются при оценке знаний на зачёте.

7. Формы аттестации и оценочные материалы

Текущий контроль предназначен для проверки хода и качества усвоения учебного материала, стимулирования учебной работы обучающихся и совершенствования методики проведения занятий. Он проводится в ходе всех видов занятий в форме, избранной преподавателем.

Промежуточная аттестация имеет целью определить степень достижения учебных целей по учебной дисциплине и проводится в форме зачета. Принимается зачет преподавателями, читающими лекции по данной учебной дисциплине в соответствии с перечнем основных вопросов, выносимых для контроля знаний обучающихся:

7.1. Вопросы к зачету

1) Актуальность проблемы защиты информации
2) Основные понятия и термины защиты информации
3) Классификация методов и средств защиты информации от несанкционированного доступа

4) Механизмы защиты информации от несанкционированного доступа
5) Классификация автоматизированных систем и требования по защите информации
6) Показатели защищенности средств вычислительной техники по защите информации от несанкционированного доступа
7) Политика безопасности
8) Разработка модели разграничения доступа к информации
9) Основные принципы функционирования аппаратных средств защиты информации
10) Основные принципы функционирования программных средств защиты
11) Угрозы перевода программной системы защиты в пассивное состояние
12) Разграничение доступа к информации
13) Основные подходы к защите данных от несанкционированного доступа
14) Модели управления доступом
15) Защита информации средствами операционных систем
16) Методы контроля доступа к ресурсам компьютерной системы
17) Способы фиксации факта доступа к файлам
18) Структура и функции подсистемы контроля доступа программ и пользователей
19) Средства ведения и анализа системных журналов
20) Средства контроля за процессами. Свойства процессов и управление ими
21) Средства поиска остаточной информации на машинных носителях информации
22) Средства гарантированного удаления информации
23) Модели взаимодействия прикладных программ и программы-злоумышленника
24) Классификация разрушающих программных средств и их воздействий
25) Методы внедрения разрушающих программных средств
26) Компьютерные вирусы как особый класс разрушающего программного воздействия
27) Принципы и методы защиты от разрушающих программных воздействий
28) Построение и принципы работы типовых антивирусных средств
29) Способы и средства обеспечения целостности информации
30) Защита файлов от изменений
31) Криптографические средства обеспечения целостности информации
32) Электронная подпись
33) Основные принципы криптографической защиты информации в автоматизированных системах
34) Программно-аппаратные средства шифрования
35) Методы распределения и хранения ключевой и парольной информации

7.2. Оценивание результатов зачета.

Зачет проводится по окончании занятий по дисциплине до начала экзаменационной сессии в период недели контроля самостоятельной работы.

Билет для проведения промежуточной аттестации в форме зачета включают вопросы и задачи для проверки сформированности знаний, умений и навыков.

Оценивание результатов зачета осуществляется в соответствии с полнотой и качеством выполнения задания на работу, качеством защиты работы (ответы на вопросы, и др.). Оценка работы отражает уровень сформированности соответствующих компетенций.

– «отлично» - работа выполнена в соответствии с утвержденным планом и заданием, полностью раскрыто содержание каждого вопроса; студентом сформулированы собственные аргументированные выводы по теме работы; оформление работы соответствует предъявляемым требованиям; при защите работы обучающийся демонстрирует свободное владение материалом и верно отвечает на поставленные вопросы;

– «хорошо» - работа выполнена в соответствии с утвержденным планом и заданием; полностью раскрыто содержание каждого вопроса; имеются незначительные замечания к оформлению работы; при защите работы обучающийся демонстрирует владение материалом, но отвечает на ряд поставленных вопросов не в достаточно полном объеме;

– «удовлетворительно» - работа выполнена в соответствии с утвержденным планом и заданием, но не полностью раскрыто содержание каждого вопроса; обучающимся не сделаны собственные выводы по теме работы; допущены существенные недостатки в оформлении работы; при защите работы обучающийся демонстрирует владение материалом, но отвечает не на все поставленные вопросы, либо не в достаточно полном объеме;

– «неудовлетворительно» - если работа не выполнена в соответствии с утвержденным планом и заданием, не раскрыто содержание каждого вопроса; обучающимся не сделаны выводы по теме работы, имеются существенные недостатки в оформлении работы; при защите работы обучающийся не демонстрирует владение материалом, не отвечает на поставленные вопросы.

Оценка «зачтено» проставляется студенту, выполнившему и защитившему в полном объеме практические задания и лабораторные работы в течение семестра, чей уровень знаний, умений и навыков соответствует уровню оценок «отлично», «хорошо» или «удовлетворительно». Оценка «не зачтено» проставляется студенту, не выполнившему и (или) не защитившему в полном объеме практические задания и лабораторные работы в течение семестра, либо чей уровень знаний, умений и навыков соответствует уровню оценки «неудовлетворительно».

7.3. Выполнение и примерные задания расчетно-графической работы

Расчетно-графическая работа выполняется в процессе изучения дисциплины. Общее руководство и контроль за ходом выполнения расчетно-графической работы осуществляет преподаватель соответствующей дисциплины. Расчетно-графическая работа выполняется в соответствии с методическими указаниями для обучающихся.

Основными функциями руководителя расчетно-графической работы являются:

– определение и формулирование задания расчетно-графической работы;

– консультирование по вопросам содержания и последовательности выполнения расчетно-графической работы;

– оказание помощи студенту в подборе необходимой литературы;

– контроль хода выполнения расчетно-графической работы.

Примерные задания для выполнения расчетно-графической работы: необходимо разработать политику безопасности предприятия.

7.4. Оценивание результатов расчетно-графической работы

Оценивание расчетно-графической работы осуществляется в соответствии с полнотой и качеством выполнения задания на работу, качеством защиты работы (ответы на вопросы, и др.). Оценка работы отражает уровень сформированности соответствующих (п. 1.2) компетенций.

– «отлично» - работа выполнена в соответствии с утвержденным планом и заданием, полностью раскрыто содержание каждого вопроса; студентом сформулированы собственные аргументированные выводы по теме работы; оформление работы соответствует предъявляемым требованиям; при защите работы обучающийся демонстрирует свободное владение материалом и верно отвечает на поставленные вопросы;

– «хорошо» - работа выполнена в соответствии с утвержденным планом и заданием; полностью раскрыто содержание каждого вопроса; имеются незначительные замечания к оформлению работы; при защите работы обучающийся демонстрирует владение материалом, но отвечает на ряд поставленных вопросов не в достаточно полном

объеме;

– «удовлетворительно» - работа выполнена в соответствии с утвержденным планом и заданием, но не полностью раскрыто содержание каждого вопроса; обучающимся не сделаны собственные выводы по теме работы; допущены существенные недостатки в оформлении работы; при защите работы обучающийся демонстрирует владение материалом, но отвечает не на все поставленные вопросы, либо не в достаточно полном объеме;

– «неудовлетворительно» - если работа не выполнена в соответствии с утвержденным планом и заданием, не раскрыто содержание каждого вопроса; обучающимся не сделаны выводы по теме работы, имеются существенные недостатки в оформлении работы; при защите работы обучающийся не демонстрирует владение материалом, не отвечает на поставленные вопросы.

Оценка «зачтено» по РГР проставляется студенту, чей уровень знаний, умений и навыков соответствует уровню оценок «отлично», «хорошо» или «удовлетворительно». В случае оценивания работы на «неудовлетворительно» работа направляется на дальнейшую доработку.

8. Учебно-методическое и информационное обеспечение дисциплины

Электронный каталог и электронные информационные ресурсы, предоставляемые научной библиотекой ФГБОУ ВО «Чувашский государственный университет имени И.Н. Ульянова» доступны по ссылке http://library.chuvsu.ru/

8.1. Рекомендуемая основная литература (ежегодное обновление перечня и условия доступа представлены в Приложениях к рабочей программе)

№ п/п	Наименование
1.	Методы и средства обеспечения программно-аппаратной защиты информации [Электронный ресурс]: научно-техническое издание / А.И. Астайкин [и др.]. — Электрон. текстовые данные. — Саров: Российский федеральный ядерный центр – ВНИИЭФ, 2015. — 224 c. — 978-5-9515-0305-3. — Режим доступа: http://www.iprbookshop.ru/60959.html
2.	Лабораторный практикум по дисциплине Программно-аппаратные средства защиты информации [Электронный ресурс]/. — Электрон. текстовые данные. — М.: Московский технический университет связи и информатики, 2016. — 31 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/61529.html

8.2. Рекомендуемая дополнительная литература (ежегодное обновление и условия доступа перечня представлены в Приложениях к рабочей программе)

№ п/п	Наименование
1.	Нестеров, С. А. Информационная безопасность: учебник и практикум для академического бакалавриата / С. А. Нестеров. — М.: ИздательствоЮрайт, 2017. — 321 с. — (Серия: Университеты России). — ISBN 978-5-534-00258-4. — Режим доступа: www.biblio-online.ru/book/836C32FD-678E-4B11-8BFC-F16354A8AFC7.

8.3. Программное обеспечение, профессиональные базы данных, информационно-справочные системы.

Программное обеспечение, профессиональные базы данных, информационно-справочные системы, предоставляемые управлением информатизации ФГБОУ ВО «Чувашский государственный университет имени И.Н. Ульянова» доступны по ссылке http://ui.chuvsu.ru//*

8.3.1 Программное обеспечение

№ п/п	Наименование	Условия доступа/скачивания
1.	MS Office/ LibreOffice	лицензия университета/ свободное лицензионное соглашение (https://ru.libreoffice.org/)
2.	MS Windows/Arch linux	лицензия университета/ свободное лицензионное соглашение (https://ru.libreoffice.org/)
3.	Visual Studio Community	http://www.visualstudio.com/ru/vs/community
4.	AVG AntiVirus Free	https://www.avg.com/ru-ru/homepage#pc
5.	Avast Free Antivirus	http://avast-anti-virus.ru/?yclid=5762528100398929218

6.	Kaspersky Free	https://www.kaspersky.ru/free-antivirus
7.	360 Total Security	https://www.360totalsecurity.com/ru/

8.3.2 Базы данных, информационно-справочные системы

№ п/п	Наименование программного обеспечения	Условия доступа/скачивания
1.	Гарант	из внутренней сети университета (договор)
2.	Консультант +	
3.	База данных угроз безопасности информации	https://bdu.fstec.ru/

8.4. Рекомендуемые интернет-ресурсы и открытые онлайн курсы.

№ п/п	Наименование	Условия доступа
1.	ISO 27000 Международные стандарты управления информационной безопасностью.	http://iso27000.ru
2.	SecurityLab. Информационный портал по безопасности.	http://www.securitylab.ru
3.	Xgu.ru.	http://xgu.ru/wiki/
4.	Российская Государственная Библиотека	http://www.rsl.ru
5.	Государственная публичная научно-техническая библиотека России	http://www.gpntb.ru
6.	Фундаментальная библиотека Нижегородского государственного университета	http://www.unn.ru/library
7.	Научная библиотека Казанского государственного университета	http://lsl.ksu.ru
8.	Научная электронная библиотека	http://elibrary.ru
9.	Полнотекстовая библиотека учебных и учебно-методических материалов	http://window.edu.ru
10.	Электронно-библиотечная система IPRbooks	http://www.iprbookshop.ru

9. Материально-техническое обеспечение дисциплины

Учебные аудитории для лекционных занятий по дисциплине оснащены автоматизированным рабочим местом (АРМ) преподавателя, обеспечивающим тематические иллюстрации и демонстрации, соответствующие программе дисциплины в составе:

– ПЭВМ с доступом в интернет (операционная система, офисные программы, антивирусные программы);
– мультимедийный проектор с дистанционным управлением;
– настенный экран;
– интерактивная доска SMART;
– телевизор SMART.

Учебные аудитории для практических, лабораторных и самостоятельных занятий по дисциплине оснащены АРМ преподавателя и пользовательскими АРМ по числу обучающихся, объединенных локальной сетью («компьютерный» класс), с возможностью подключения к сети Интернет и доступом к электронной информационно-образовательной среде ФГБОУ ВО «Чувашский государственный университет имени И.Н. Ульянова».

Для реализации программы обучения используется лаборатория оснащённая:

специализированным оборудованием по защите информации от утечки по акустическому каналу и по каналу побочных электромагнитных излучений и наводок (Система виброакустического зашумления "СонатаАВ мод.3М"в сост.виброизлучатель пьезоэлектрический ВИ-3М и ПИ-3М,аудиоизлучатель АИ-3М — 1; Устройство защиты

"МП-1А" — 1; Устройство защиты объектов информатизации от утечки информации за счет ПЭМИН "Соната-Р" - 1; Фильтр сетевой помехоподавляющий "ФСП-1Ф-7А" - 1);

техническими средствами контроля эффективности защиты информации от утечки по акустическому каналу и каналу побочных электромагнитных излучений и наводок (Устройство поисковое многофункциональное "ST 033" — 1; Комплекс проведения акустических и виброакустических измерений "Спрут-мини-А" - 1; Комплекс обнаружения радиоизлучающих средств и радиомониторинга "Крона" — 1; Имитатор многофункциональный "ИМФ-2" - 1; Прибор-приставка АСК-4106 комбинированный - 1).

10. Средства адаптации преподавания дисциплины к потребностям лиц с ограниченными возможностями

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося) могут предлагаться одни из следующих вариантов восприятия информации с учетом их индивидуальных психофизических особенностей, в том числе с применением электронного обучения и дистанционных технологий:

– для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат);в печатной форме на языке Брайля; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания и консультации.

– для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации.

– для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

11.Методические рекомендации по освоению дисциплины

В ходе лекционных занятий студенту рекомендуется вести конспектирование учебного материала. Следует обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации, положительный опыт в ораторском искусстве. При составлении конспекта желательно оставлять в рабочих конспектах поля, на которых в дальнейшем можно делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. В ходе лекционных занятий рекомендуется задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

В ходе подготовки к лабораторным работам рекомендуется изучить основную литературу, ознакомиться с дополнительной литературой, новыми публикациями в периодических изданиях. Основой для выполнения лабораторной работы являются разработанные кафедрой методические указания. Рекомендуется дорабатывать свой конспект лекций, делая в нем соответствующие записи из литературы, рекомендованной преподавателем и предусмотренной рабочей программой дисциплины. В процессе подготовки студент может дополнить список использованной литературы современными источниками, не представленными в списке рекомендованной литературы, и в дальнейшем использовать собственные подготовленные учебные материалы при написании расчетно-графической работы.

Формы организации студентов на лабораторных работах занятиях: фронтально-индивидуальная. Все студенты выполняют одновременно одну и ту же работу по индивидуальному заданию в соответствие с порядковым номером студента в списке группы.

В результате выполнения лабораторной работы запланирована подготовка письменного отчета о выполненной работе в соответствии с требованиями методических указаний. Качество выполнения лабораторных работ является важной составляющей оценки текущей успеваемости обучающегося.

Лист актуализации

№ п/п	Наименование документа	Решение кафедры		Подпись	Должность, ФИО
		Дата	протокол №		