ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«КАМЧАТСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «КамчатГТУ»)

ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ЭКОНОМИКИ И УПРАВЛЕНИЯ

Кафедра «Информационные системы»

УТВЕРЖДАЮ
Декан ФИТЭУ
_____ /И.А.Рычка/
«29» января 2024 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Кибербезопасность»

направление подготовки (специальность)
09.03.03 Прикладная информатика
(уровень подготовки – бакалавриат)

направленность (профиль):
«Прикладная информатика в цифровой экономике»

Петропавловск-Камчатский,
2023

Рабочая программа дисциплины составлена на основании ФГОС ВО направления подготовки 09.03.03 «Прикладная информатика».

Составитель рабочей программы
Заведующий кафедрой ИС, д.т.н., профессор _____ И.Г. Проценко

Рабочая программа рассмотрена на заседании кафедры «Информационные системы»
«16» декабря 2023 г., протокол №4

Заведующий кафедрой ИС, д.т.н., профессор _____ И.Г. Проценко
«16» декабря 2023 г.

1 Цель и задачи учебной дисциплины

Целью преподавания дисциплины является формирование у обучаемых знаний в области теоретических основ информационной безопасности и навыков практического обеспечения защиты информации и безопасного использования программных средств в вычислительных системах. Цели курса определяют структуру, содержание и рациональные формы организации обучения: лекции, семинары, практические занятия, различные виды самостоятельной работы.

Задачами изучения дисциплины являются:

– изучение основных теоретических положений и методов в области защиты информации;

– ознакомление с основными угрозами информационной безопасности, правилами их выявления, анализа и формирования требований к разным уровням обеспечения информационной безопасности;

– ознакомление с особенностями угроз, создаваемым вредоносным программным обеспечением, характерными чертами вирусов и средств борьбы с ними;

– формирование умений и привитие навыков применения теоретических знаний для решения прикладных задач, а также развитие новых подходов к обеспечению информационной безопасности в сфере экономики;

– учёт особенностей реализации технологий защиты данных в существующие инструменты поддержки и развития бизнес-процессов в экономической сфере и применения их в системах управления организацией;

– развитие новых подходов к обеспечению информационной безопасности в сфере экономики.

В результате изучения программы курса студенты должны:

Знать основы информационной безопасности и защиты информации, современные тенденции угроз информационной безопасности, нормативные правовые документы по защите информации, принципы криптографических преобразований, типовые программно-аппаратные средства и системы защиты информации от несанкционированного доступа в компьютерную среду; а также современные методы и средства обеспечения информационной безопасности в экономических информационных системах.

Уметь выявлять угрозы информационной безопасности, использовать нормативные правовые документы по защите информации, исследовать, использовать и развивать современные методы и средства обеспечения информационной безопасности; реализовывать мероприятия для обеспечения на предприятии (в организации) деятельности в области защиты информации, проводить анализ степени защищенности информации и осуществлять повышение уровня защиты с учетом развития математического и программного обеспечения вычислительных систем, разрабатывать средства и системы защиты информации.

Иметь представление о типовых разработанных средствах защиты информации, возможностях их использования в реальных задачах создания и внедрения информационных систем и **навыки** владения приемами разработки политики безопасности предприятия и навыки использования методов и средств обеспечения информационной безопасности в социально-экономических информационных системах.

2 Требования к результатам освоения дисциплины

В результате изучения дисциплины у студента должны быть сформированы следующие общепрофессиональные компетенции:

– способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-3);

– способность участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью (ОПК-4).

Планируемые результаты обучения при изучении дисциплины, соотнесенные с планируемыми результатами освоения образовательной программы, представлены в таблице 1.

Таблица 1.

Планируемые результаты обучения при изучении дисциплины, соотнесенные с планируемыми результатами освоения образовательной программы

Код компетенции	Планируемые результаты освоения образовательной программы	Код и наименование индикатора достижения	Планируемый результат обучения по дисциплине	Код показателя освоения
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**ИД-1** опк-3 **Знать** принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	**Знать:** – основы информационной безопасности и защиты информации, принципы криптографических преобразований; – виды угроз информационных систем и методы обеспечения информационной безопасности	**З(ОПК-3)1** **З(ОПК-3)2**
			Уметь: – выявлять угрозы информационной безопасности; – обосновывать организационно-технические мероприятия по защите информации в информационных системах	**У(ОПК-3)1** **У(ОПК-3)2**
			Владеть: – навыками разработки и применения систем информационной безопасности; – навыками разработки программного обеспечения и баз данных, которые обеспечивают приемлемый уровень информационной безопасности	**В(ОПК-3)1** **В(ОПК-3)2**

Код компетенции	Планируемые результаты освоения образовательной программы	Код и наименование индикатора достижения	Планируемый результат обучения по дисциплине	Код показателя освоения
ОПК-4	Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	**ИД-1** опк-4 **Знать** основные стандарты оформления технической документации на различных стадиях жизненного цикла информационной системы	**Знать:** – типовые средства и системы защиты информации от несанкционированного доступа в компьютерную среду и возможность их использования в реальных задачах создания и внедрения информационных систем	**З(ОПК-4)1**
			Уметь: - применять законы и другие нормативно-правовые акты в сфере информационной безопасности; - выявлять угрозы конфиденциальности, целостности, доступности информации; - проводить анализ информации с целью подготовки принятия решений по обеспечению информационной безопасности	**У(ОПК-4)1** **У(ОПК-4)2** **У(ОПК-4)3**
			Владеть: - приемами разработки политики безопасности предприятия и навыки использования методов и средств обеспечения информационной безопасности в социально-экономических информационных системах	**В(ОПК-4)1**

3 Место дисциплины в структуре образовательной программы

Дисциплина «Кибербезопасность» является базовой дисциплиной в структуре образовательной программы.

4 Содержание дисциплины

4.1 Тематический план дисциплины

Наименование разделов и тем	Всего часов	Аудиторные занятия	Контактная работа по видам учебных занятий			Самостоятельная работа	Формы текущего контроля	Итоговый контроль знаний по дисциплине
			Лекции	Семинары (практические)	Лабораторные работы			
Очная форма обучения								
Тема 1: Киберпространство и основы кибербезопасности	27	***12***	4,0	-	8.0	15.0	Опрос, ПЗ, Тест	
Тема 2: Векторы риска	27	***12***	4,0	-	8.0	15.0	Опрос, ПЗ, Тест	
Тема 3: Международные организации по кибербезопасности, принципы и стандарты	27	***12***	4,0	-	8.0	15.0	Опрос, ПЗ, Тест	
Тема 4: Менеджмент кибербезопасности в национальном контексте	27	***12***	4,0	-	8.0	15.0	Опрос, ПЗ, Тест	
Зачет с оценкой		-	-	-	-	-	-	
Всего	**108**	***48***	**16**		**32**	**60**		
Заочная форма обучения								
Тема 1: Киберпространство и основы кибербезопасности	**28**	***4***	**2**		**2**	**24**		
Тема 2: Векторы риска	**26**	***2***	**-**		**2**	**24**		
Тема 3: Международные организации по кибербезопасности, принципы и стандарты	**26**	***2***	**-**		**2**	**24**		
Тема 4: Менеджмент кибербезопасности в национальном контексте	**24**	***2***	**-**		**2**	**22**		
Зачет с оценкой	**4**							**4**
Всего	**108**	***10***	**2**		**8**	**94**		**4**

*ПЗ – практическое задание

4.2 Описание содержания дисциплины

Лекция 1.1. Кибербезопасность и киберпространство.

Рассматриваемые вопросы:

Основные понятия теории информационной безопасности; основные понятия и определения: уязвимость, угроза, атака, эксплойт; свойства информации: конфиденциальность, целостность, доступность; классификация угроз информационной безопасности; информационная безопасность и риски; структура информационного пространства: опорная сеть Интернета и сетевая инфраструктура государств; протоколы и платформы; архитектура сетевой безопасности и управление процессом обеспечения безопасности.

Лабораторная работа №1. Защита документов MS Office

Задание: на основе учебного материала по защите документов, созданных в формате MS Word, MS Excel, MS Access, подготовить соответствующие файлы, защитить их, подобранным для этой операции, паролем и проверить на чтение, редактирование, копирование.

Лабораторная работа № 2. Защита архивных файлов с помощью пароля

Задание: Изучить парольную защиту информации прикладного программного обеспечения и на основе этого материала создать архив из группы файлов и защитить его паролем от раскрытия и прочтения. Провести защиту архивных файлов формата.*.rar, *.zip. Попробовать распаковать архив произвольным паролем и паролем, который использовался при защите.

Лабораторная работа № 3. Защита кода HTML – страниц

Задание: Изучить защиту информации HTML-страниц (код HTML, JavaScript, VBScript, текст, ссылки и графику и т.д.) и на основе этого материала защитить текст от чтения. Блокировать щелчок правой кнопкой мыши, отображение ссылки в строке состояния, выделение текста, использование странички в оффлайн, распечатку страницы.

СРС по теме 1.

Подготовка к лекциям.

Изучение дополнительного теоретического материала.

Подготовка теоретического материала и данных для выполнения лабораторных работ.

Тема 2. Векторы риска

Лекция 2.1. Векторы риска

Рассматриваемые вопросы:

Классификация угроз и уязвимостей информационной безопасности в корпоративных системах; угроза безопасности объекта, источник угрозы, уязвимость объекта, атака; система поставок/поставщики, нападения из удаленного доступа и доступа по карточкам дистанционного считывания, вторжение в систему лицами, обладающими доступом (нападения при наличии локального доступа), риск, связанный с мобильностью, личные мобильные устройства и новые тенденции.

Лабораторная работа № 4. Открытые порты и запущенные службы

Задание: На основе учебного материала получить список открытых портов и запущенных служб используя утилиту Fport фирмы Foundstone. То же самое проделать с программой Netstat. и утилитой PortQry.

Лабораторная работа № 5. Открытые файлы и владеющие ими процессы

Задание: На основе учебного материала получить список открытых файлов и владеющих ими процессов используя программы handle и Program Explorer.

СРС по теме 2.

Подготовка к лекциям.

Изучение дополнительного теоретического материала.

Подготовка теоретического материала и данных для выполнения лабораторных работ.

Тема 3. Международные организации по кибербезопасности, принципы и стандарты

Лекция 3.1. Международные организации по КБ, принципы и стандарты

Рассматриваемые вопросы:

Правовое обеспечение информационной безопасности; понятие нормативности; международные организации по кибербезопасности, международные стандарты и требования — обзор структур и практических действий; национальные рамки кибербезопасности; кибербезопасность в национальном и международном законодательстве.

Лабораторная работа № 6. Вирусы и антивирусные системы

Задание: На основе учебного материала по компьютерным вирусам и антивирусным системам создать вакцину для вируса Autorun.inf (разными способами, в т.ч. антивирусной утилитой AntiAvtorun), написать программу антивирусного сканера в среде Borland Delphi.

Лабораторная работа № 7. Поиск и уничтожение вирусов-червей BugBear и Opasoft

Задание: На основе учебного материала по компьютерным вирусам и антивирусным системам воспользоваться программой clrav.exe, разработанной в Лаборатории Касперского, для поиска и уничтожения (в случае возможного обнаружения) червей BugBear и Opasoft.

Лабораторная работа № 8. Шпионское программное обеспечение

Задание: На основе учебного материала по компьютерным вирусам разработать алгоритм и написать программу клавиатурного шпиона в среде разработки Delphi

СРС по теме 3.

Подготовка к лекциям.

Изучение дополнительного теоретического материала.

Подготовка теоретического материала и данных для выполнения лабораторных работ.

Тема 4. Менеджмент кибербезопасности в национальном контексте

Лекция 4.1. Особенности национального менеджмента кибербезопасности

Рассматриваемые вопросы:

Национальные методы работы, принципы действия и организации по киберу- стойчивости, национальные структуры кибербезопасности, киберкриминалистика, аудит и оценка безопасности на национальном уровне.

Лабораторная работа № 9. Применение методов гаммирования файлов

Задание: На основе учебного материала по криптографическим методам шифрования данных изучить и воспользоваться программой E-CRYPT для шифрования и последующего дешифрования конкретного файла методом гаммирования.

Лабораторная работа №10. Криптографические методы защиты информации в корпоративных информационных системах

Задание: На основе учебного материала по криптографическим методам защиты информации изучить различные методы шифрования и их стандарты, изучить методы шифрования с открытыми и закрытыми ключами и применить при разработке алгоритма и программы, шифрование и дешифрования открытого текста. Программа реализуется в среде программирования Delphi.

Лабораторная работа № 11. Разработка алгоритма и написание программы определения частоты букв, и ее применение для дешифровки текста, зашифрованного методом подстановки

Задание: На основе учебного материала по криптоаналитическим методам дешифровки защищенных данных изучить метод подстановки и реализовать его, разработав алгоритм и написав соответствующую программу в среде программирования Delphi. Затем написать программу определения частоты букв и проанализировать результат.

Лабораторная работа № 12. Сокрытие файла в BMP-картинке

Задание: На основе учебного материала по криптографическим методам шифрование сообщений изучить метод стеганографии и реализовать его воспользовавшись программой bmpPacker.

СРС по теме 4

Подготовка к лекциям.

Изучение дополнительного теоретического материала.

Подготовка теоретического материала и данных для выполнения лабораторных работ.

Подготовка к зачету с оценкой.

5 Учебно-методическое обеспечение для самостоятельной работы обучающихся

В целом внеаудиторная самостоятельная работа обучающегося при изучении курса включает в себя следующие виды работ:

– проработка (изучение) материалов лекций;

– чтение и проработка рекомендованной основной и дополнительной литературы;

– подготовка к лабораторным работам;

– поиск и проработка материалов из Интернет-ресурсов, периодической печати;

– выполнение домашних заданий в форме творческих (проблемно-поисковых, групповых) заданий, кейс-стади, докладов;

– подготовка презентаций для иллюстрации докладов;

– выполнение тестовых заданий;

– подготовка к тестированию;

– подготовка к текущему и итоговому (промежуточная аттестация) контролю знаний по дисциплине.

Основная доля самостоятельной работы обучающихся приходится на подготовку к лабораторным работа и тестированию, тематика которых полностью охватывает содержание курса. Самостоятельная работа по подготовке к тестированию и лабораторным работам предполагает умение работать с первичной информацией.

Для проведения практических занятий, для самостоятельной работы используется учебно-методические пособия:

Проценко И.Г. Защита информации: конспект лекций. – Петропавловск-Камчатский: КамчатГТУ, 2019. – 64 с.

Проценко И.Г. Защита информации: лабораторный практикум. – Петропавловск-Камчатский: КамчатГТУ, 2019. – 50 с.

6 Рекомендуемая литература

6.1 Основная литература

1. Мельников В.П. Информационная безопасность и защита информации: учеб.пособие / В.П. Мельников, 2007г.

2. Щеглов А.Ю. Математические модели и методы формального проектирования систем защиты информационных систем 2015 г./ А.Ю. Щеглов, К.А. Щеглов – коллекция "Информатика – НИУ ИТМО (Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики)" ЭБС ЛАНЬ.

6.2 Дополнительная литература

1. Основы информационной безопасности / Галатенко В. А. — М.: Национальный Открытый Университет «ИНТУИТ», 2011. — Серия («Безопасность ») [Электронный ресурс] - Электрон.дан. — Режим доступа: https://www.intuit.ru/studies/courses/10/10/info. — Загл. с экрана.ISBN 978-5-9556-0053-6.

2. Куприянов А.И. Основы защиты информации: учеб. пособие / А.И. Куприянов, 2008г.

3. Кибербезопасность в условиях электронного банкинга : практическое пособие / А. А. Бердюгин, А. Б. Дудка, С. В. Конявская, В. А. Конявский, И. Г. Назаров. - Москва : Прометей, 2020. - 522 с. : ил. - Библиогр. в кн. - ISBN 978-5-907244-61-0 : Б. ц. - URL: https://biblioclub.ru/index.php?page=book&id=610688/ (дата обращения: 03.03.2021). - Режим доступа: ЭБС Университетская библиотека ONLINE. - Текст : электронный.

4. Анализ состояния защиты данных в информационных системах : учебно- методическое пособие. - Новосибирск : НГТУ, 2012. - 52 с. - ISBN 978-5-7782-1969-4: Б. ц. - URL: http://biblioclub.ru/index.php?page=book&id=228844/ (дата обращения: 03.03.2021). - Режим доступа: ЭБС Университетская библиотека ONLINE. - Текст : электронный.

5. Нестеров, С. А. Основы информационной безопасности : учебное пособие / С.А. Нестеров. - Санкт-Петербург : Издательство Политехнического университета, 2014. - 322 с. - ISBN 978-5-7422-4331-1: Б. ц. - URL: http://biblioclub.ru/index.php?page=book&id=363040/ (дата обращения: 03.03.2021). - Режим доступа: ЭБС Университетская библиотека ONLINE. - Текст : электронный.

6.3 Методические указания

1. Защита информации. Конспект лекций. / Проценко И.Г. – Петропавловск-Камчатский: КамчатГТУ, 2019. – 66 с.

2. Защита информации. Лабораторный практикум. / Проценко И.Г. – Петропавловск-Камчатский: КамчатГТУ, 2019. – 50 с.

7 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине «Кибербезопасность» представлен в приложении к рабочей программе дисциплины и включает в себя:

– перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы;

– описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания;

– типовые контрольные задания или материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций;

– методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций.

Вопросы для проведения промежуточной аттестации по дисциплине (экзамен)

1. Основные понятия и определения информационной безопасности.
2. Защита информации. Предмет и объект защиты.
3. Угроза безопасности. Уязвимость системы. Атака.
4. Несанкционированный доступ.
5. Особенности защиты информации в экономических информационных системах.
6. Основные методы и средства защиты информации, применяемые в ЭИС.
7. Уязвимость компьютера и сети. Виды угроз.
8. Угроза отказ в обслуживании.
9. Социальная инженерия и ИБ.
10. Правовые меры обеспечения информационной безопасности в ЭИС.
11. Законодательные и нормативные акты Российской Федерации в ИБ.
12. Компьютерные вирусы и черви.
13. Макровирусы.
14. Полиморфные вирусы.
15. Троянские кони (закладки).
16. Программы слежения за работой пользователя (клавиатурные шпионы).
17. Генераторы вирусов.
18. Методы защиты от вредоносных программ.
19. Системы обнаружения уязвимостей (сетевые сканеры).
20. Антивирусы и "антитроянцы".
21. Антивирусные программы в Интернете.
22. Политика безопасности. Ваш проект политики для компьютерной лаборатории.

23. Назначение и функции межсетевых экранов. Опыт работы с межсетевым экраном.

24. Виртуальные частные сети.

25. Отражение проблем ИБ в Интернете.

26. Парольная защита.

27. Обнаружение атак.

28. Защита информации в базах данных.

29. Анализаторы протоколов (снифферы).

30. Мандатный и дискреционный доступ.

31. Криптографические методы защиты информации. Математическое и алгоритмическое обеспечение криптографических методов защиты информации.

32. Шифрование. Метод подстановки.

33. Матрицы Вижинера.

34. Частотный анализ текстов.

35. Шифрование методом перестановки.

36. Криптосистема с открытым ключом.

37. Симметричные и асимметричные криптосистемы.

38. Электронная цифровая подпись.

39. Использование электронных ключей для организации ИБ.

40. Организационно-административные методы защиты, применяемые в ЭИС.

41. Формирование политики безопасности предприятия (организации).

42. Идентификация пользователей, аутентификация пользователей и авторизация пользователей (назначение и способы реализации).

43. Защита информации в компьютерных сетях. Объекты защиты информации в сети.

44. Потенциальные угрозы безопасности в сети Интернет. Методы защиты информации в сети Интернет.

45. Количественный подход к информационной безопасности. Оценка защищенности механизмов защиты.

46. Аудит информационной безопасности.

47. Управление информационными рисками.

8 Методические указания для обучающихся по освоению дисциплины

Методика преподавания данной дисциплины предполагает чтение лекций, проведение лабораторных работ, групповых и индивидуальных консультаций по отдельным (наиболее сложным) специфическим проблемам дисциплины. Предусмотрена самостоятельная работа студентов, а также прохождение аттестационных испытаний промежуточной аттестации (зачет).

Лекции посвящаются рассмотрению наиболее важных концептуальных вопросов: основным понятиям; теоретическим основам. В ходе лекций обучающимся следует подготовить конспекты лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины; проверять термины, понятия с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь; обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе.

На лекциях преподаватель знакомит слушателей с основными понятиями и положениями по текущей теме. На лекциях слушатель получает только основной объём информации по теме. Только посещение лекций является недостаточным для подготовки к лабораторным занятиям и зачету. Требуется также самостоятельная работа по изучению основной и дополнительной литературы и закрепление полученных на лабораторных занятиях навыков.

При изучении дисциплины используются интерактивные методы обучения:

– проблемная лекция, предполагающая изложение материала через неоднозначность трактовки материалов к вопросам, задачам или ситуациям. При этом процесс познания происходит в научном поиске, диалоге и сотрудничестве с преподавателем в процессе анализа и сравнения точек зрения;

– лекция-визуализация - подача материала осуществляется средствами технических средств обучения с кратким комментированием демонстрируемых визуальных материалов (презентаций).

Конкретные методики, модели, методы и инструменты рассматриваются преимущественно при подготовке и выполнении лабораторных работ.

Целью выполнения ***лабораторных работ*** является закрепление знаний обучающихся, полученных ими в ходе изучения дисциплины на лекциях и самостоятельно. Практические задания по темам выполняются на лабораторных занятиях в компьютерном классе. Если лабораторные занятия пропущены (по уважительной или неуважительной причине), то соответствующие задания необходимо выполнить самостоятельно и представить результаты преподавателю на очередном занятии. Самостоятельная работа студентов – способ активного, целенаправленного приобретения студентом новых для него знаний, умений и навыков без непосредственного участия в этом процесса преподавателя. Качество получаемых студентом знаний напрямую зависит от качества и количества необходимого доступного материала, а также от желания (мотивации) студента их получить. При обучении осуществляется целенаправленный процесс взаимодействия студента и преподавателя для формирования знаний, умений и навыков.

9 Курсовой проект/работа

В соответствии с учебным планом курсовое проектирование по дисциплине не предусмотрено.

10 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационно-справочных систем

При освоении дисциплины используются следующие информационные технологии:

– использование слайд-презентаций;

– изучение нормативных документов на официальном сайте федерального органа исполнительной власти, проработка документов;

– интерактивное общение с обучающимися и консультирование посредством электронной почты.

При освоении дисциплины используется лицензионное программное обеспечение:

– пакет Microsoft Office;

– текстовые редакторы (notepad++);

– Web-браузеры (Google chrome for Windows).

11 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

При освоении дисциплины используются следующие информационно-справочные системы:

– Введение в криптографию / Под. общ. ред. Ященко В. В. — Издание второе, исправленное. – М.: МЦНМО, 1999. – 272 с. [Электронный ресурс] – Режим доступа: https://www.twirpx.com/file/4220/

– Касперский Е.В. Компьютерные вирусы: что это такое и как с ними бороться. – М.: СК Пресс, 1998.- 288 с. [Электронный ресурс] – Режим доступа: https://www.twirpx.com/file/73531/

– Рябко Б.Я.,Фионов А.Н. Криптографические методы защиты информации: Учебное пособие для вузов. – 2-е издание, стереотип. – М.:Горячая линия – Телеком, 20113. – 229 с. [Электронный ресурс] – Режим доступа: https://docplayer.ru/27703084-Kriptograficheskie-metody-zashchity-informacii.html

– Электронная библиотека диссертаций РГБ [Электронный ресурс]. - Режим доступа: http://www.diss.rsl.ru

– справочно-правовая система Консультант-плюс [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/online

– справочно-правовая система Гарант [Электронный ресурс]. – Режим доступа: http://www.garant.ru/online

12 Материально-техническое обеспечение дисциплины

Лекционный материал изучается в специализированной аудитории, оснащенной проектором с видеотерминала персонального компьютера на настенный экран.

Лабораторные работы выполняются в специализированной лаборатории, оснащенной современными персональными компьютерами и программным обеспечением в соответствии с тематикой дисциплины.

Число рабочих мест в классах должно обеспечить индивидуальную работу студента на отдельном персональном компьютере.

В качестве материально-технического обеспечения дисциплины используются:

– для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации учебная аудитория № 7-405 с комплектом учебной мебели на 25 посадочных мест;

– для лабораторных работ - лабораторная аудитория № 7-402, оборудованная 10 рабочими станциями с доступом к сети «Интернет» и в электронную информационно-образовательную среду организации и комплектом учебной мебели на 15 посадочных мест;

– доска аудиторная;

– мультимедийное оборудование (ноутбук, проектор);

– презентации в Power Point по темам курса.

– информационная система «*КТест*», установленная на всех рабочих станциях.

13 Особенности реализации дисциплины (модуля) для обучающихся с ограниченными возможностями здоровья и инвалидов

Для инвалидов и лиц с ограниченными возможностями здоровья (далее – ОВЗ) при реализации дисциплины учитываются рекомендации медико-социальной экспертизы, отраженные в индивидуальной программе реабилитации и абилитации инвалида, относительно рекомендованных условий и видов труда, а также особенности психофизического развития, индивидуальные возможности и состояние здоровья таких обучающихся.

Подбор и разработка учебно-методических материалов производятся с учетом индивидуальных психофизических особенностей и предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Категории студентов	Формы
С нарушением слуха	- в печатной форме; - в форме электронного документа; - видеоматериалы.
С нарушением зрения	- в печатной форме увеличенным шрифтом; - в форме электронного документа; - в форме аудиофайла.
С нарушением опорно-двигательного аппарата	- в печатной форме; - в форме электронного документа; - в форме аудиофайла или видеоматериала

Для обучающихся инвалидов и с ОВЗ рекомендуется осуществление входного контроля, назначение которого состоит в определении его способностей, особенностей восприятия и готовности к освоению учебного материала. Форма входного контроля устанавливается с учетом индивидуальных психофизических особенностей данных обучающихся (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п.)

Для осуществления текущего контроля успеваемости и промежуточной аттестации обучающихся используются фонды оценочных средств, позволяющие оценить достижение ими запланированных результатов обучения и уровень сформированности компетенций.

Текущий контроль успеваемости осуществляется в целях получения информации о выполнении обучаемым требуемых действий в процессе учебной деятельности; правильности

выполнения требуемых действий; соответствии формы действия данному этапу усвоения учебного материала; формировании действия с должной мерой обобщения, освоения, быстроты выполнения.

Для студентов с ОВЗ и инвалидов предусмотрены следующие оценочные средства:

Категории студентов	Виды оценочных средств	Формы контроля и оценки результатов обучения
С нарушением слуха	тест	преимущественно письменная проверка
С нарушением зрения	собеседование	преимущественно устная проверка
С нарушением опорно-двигательного аппарата	решение тестов, контрольные вопросы	организация контроля с помощью электронной информационно-образовательной среды, письменная проверка, устная проверка

Студентам с ОВЗ и инвалидам предусматривается увеличение времени на подготовку ответов к зачету. Форма промежуточной аттестации устанавливается с учетом индивидуальных психофизических особенностей обучающихся (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п.).

Для освоения дисциплины инвалидами и лицами с ОВЗ предоставляются основная и дополнительная учебная литература в фонде библиотеки и/или в электронно-библиотечных системах.

Организация рабочего пространства, обучающегося с инвалидностью или ОВЗ, в ходе освоения дисциплины, осуществляется с использованием здоровьесберегающих технологий общего и специального назначения, помогающих компенсировать функциональные ограничения человека:

Лекционная аудитория – мультимедийное оборудование, акустический усилитель и колонки, стол для инвалидов-колясочников, источники питания для индивидуальных технических средств.

Аудитория для семинарских и практических занятий, групповых и индивидуальных консультаций; аудитория для текущего контроля и промежуточной аттестации; аудитория для курсового проектирования (выполнения курсовых работ):

– для слабослышащих обучающихся в процессе преподавания дисциплины возможно применение сурдотехнических средств, как собственных, так и предоставленных университетом, в целях оптимизации учебного процесса в качестве средства компенсации, утраченной или нарушенной слуховой функции. Учебная аудитория, в которой обучаются студенты с нарушением слуха оборудуется компьютерной техникой, аудиотехникой (акустический усилитель и колонки), видеотехникой (мультимедийный проектор, телевизор), мультимедийной системой.

– для слабовидящих обучающихся в процессе преподавания дисциплины могут применяться тифлотехнические средства, компьютерные тифлотехнологии, которые базируются на комплексе аппаратных и программных средств, обеспечивающих преобразование компьютерной информации в доступные для незрячих и слабовидящих обучающихся формы (звуковое воспроизведение, укрупненный текст), и позволяют им самостоятельно работать на обычном персональном компьютере с программами общего назначения. Для слабовидящих обучающихся в лекционных и учебных аудиториях предусмотрена возможность просмотра удаленных объектов (например, текста на доске или слайда на экране) при помощи вывода информации на монитор обучающегося.

– для обучающихся с нарушениями опорно-двигательного аппарата могут быть использованы альтернативные устройства ввода информации, в том числе специальные возможности операционных систем, таких как экранная клавиатура, с помощью которой можно вводить текст, настройка действий при вводе текста, изображения с помощью клавиатуры или мыши.

Аудитория для самостоятельной подготовки обучающихся (компьютерный класс) – стандартные рабочие места с персональными компьютерами; рабочее место с персональным

компьютером, с программным обеспечением экранного доступа.
Адаптация дисциплины предназначена для дополнительной индивидуализированной коррекции нарушений учебных и коммуникативных умений, профессиональной и социальной адаптации на этапе обучения обучающихся с ОВЗ и инвалидов.