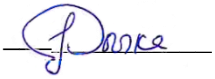
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«КАМЧАТСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «КамчатГТУ»)

Факультет информационных технологий

Кафедра «Информационные системы»

УТВЕРЖДАЮ
Декан ФИТ
 И.А. Рычка
«17» марта 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Защита информации»

направление подготовки
09.03.01 «Информатика и вычислительная техника»
(уровень бакалавриата)

направленность (профиль)
«Программное обеспечение средств вычислительной техники и автоматизированных систем»

Петропавловск-Камчатский
2021

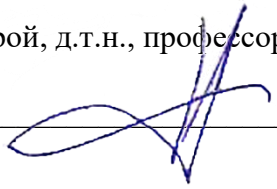
Рабочая программа разработана в соответствии с ФГОС ВО по направлению подготовки 09.03.01 «Информатика и вычислительная техника», профиль «Программное обеспечение средств вычислительной техники и автоматизированных систем», и учебного плана ФГБОУ ВО «КамчатГТУ».

Составители рабочей программы:

Заведующий кафедрой ИС  И.Г. Проценко

Рабочая программа рассмотрена на заседании кафедры «Информационные системы» Протокол № 7 от «05» марта 2021 года.

Заведующий кафедрой, д.т.н., профессор:

«05» марта 2021 г.  И.Г. Проценко

1. ЦЕЛИ И ЗАДАЧИ УЧЕБНОЙ ДИСЦИПЛИНЫ

Дисциплина «Защита информации» относится к базовой части основной профессиональной образовательной программы по направлению подготовки 09.03.01 «Информатика и вычислительная техника», профиль «Программное обеспечение средств вычислительной техники и автоматизированных систем», предусмотренной Учебным планом ФГБОУ ВО «КамчатГТУ».

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.

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, принципы криптографических преобразований, типовые программно-аппаратные средства и системы защиты информации от несанкционированного доступа в компьютерную среду; современные тенденции угроз информационной безопасности, нормативные правовые документы по защите информации, 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.

Требования к результатам освоения основных образовательных программ подготовки специалиста

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

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

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

Таблица - 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 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** способы решения 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; - 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-3)1** **З(ОПК-3)2** **З(ОПК-3)3**
			Уметь: – выявлять угрозы информационной безопасности; – обосновывать организационно-технические мероприятия по защите информации в информационных системах; – реализовывать мероприятия для обеспечения деятельности в области защиты информации на предприятии (в организации); – 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.	**У(ОПК-3)1** **У(ОПК-3)2** **У(ОПК-3)3** **У(ОПК-3)4**
			Владеть: – навыками разработки и применения систем	**В(ОПК-3)1**

Код компетенции	Планируемые результаты освоения образовательной программы	Код и наименование индикатора достижения	Планируемый результат обучения по дисциплине	Код показателя освоения
			информационной безопасности; – навыками разработки программного обеспечения и баз данных, которые обеспечивают приемлемый уровень информационной безопасности; – методами защиты компьютерной информации при проектировании информационных систем в различных предметных областях; – навыками работы с инструментальными средствами обеспечения информационной безопасности.	**В(ОПК-3)2** **В(ОПК-3)3** **В(ОПК-3)4**

1. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Курс «Защита информации» ориентирован на подготовку бакалавров по направлению 09.03.01 «Информатика и вычислительная техника». Дисциплина «Защита информации» является базовой дисциплиной в структуре образовательной программы. Курс позволяет дать будущим бакалаврам теоретические знания и сформировать у них практические навыки в создании и применении программно-технических средств для решения задач обеспечения информационной безопасности и защиты данных.

1.1. Связь с предшествующими и дисциплинами

В соответствии с учебным планом по направлению 09.03.01 «Информатика и вычислительная техника» дисциплина «Защита информации» базируется на дисциплинах «Информатика», «Программирование».

Теоретической основой для изучения материала по дисциплине «Защита информации» являются дисциплины: «Информатика», «Программирование», «Логические основы ЭВМ», «Арифметические основы ЭВМ», «Введение в направление».

1.2. Связь с последующими дисциплинами

Материал, изученный студентами в курсе «Защита информации» частично используется при изучении дисциплин «Операционные системы», «Функциональное и логическое программирование», «Структура и алгоритмы обработки данных», «Теория языков программирования и методы трансляции», «ЭВМ и периферийные устройства», «Программное обеспечение программируемых логических систем», а также является базой для курсов «Проектный практикум». Знания и умения, полученные в ходе изучения курса «Защита информации», могут быть использованы при подготовке студентами курсовых и дипломных работ и проектов.

2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1. 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 (практическ ие занятия)	Лабораторн ые работы			
Очная форма обучения								
Тема 1: Основы информационной безопасности	21	***11***	5,0	-	6.0	10.0	Опрос, ПЗ, Тест	
Тема 2: Стандарты и спецификации в области информационной безопасности	14	***7***	2,0	-	4.0	7.0	Опрос, ПЗ, Тест	
Тема 3: Вредоносное программное обеспечение	23	***11***	2,0	-	10.0	12.0	Опрос, ПЗ, Тест	
Тема 4: Криптография, шифрование и защита данных	26	***11***	2,0	-	8.0	15.0	Опрос, ПЗ, Тест	
Тема 5: Методы и средства обеспечения и информационной безопасности	24	***11***	6,0	-	6.0	13.0	Опрос, ПЗ, Тест	
Экзамен	-	-	-	-	-	-	-	-
Всего	**108**	***51***	**17**		**34**	**57**		

*ПЗ – практическое задание, РЗ – решение задач, КС – конкретная ситуация

2.2. Описание содержания дисциплины

Третий семестр

Дисциплинарный модуль 1

Продолжительность модуля 6 недель.

Тема 1: Основы информационной безопасности.

Лекция 1.1. Введение в информационную безопасность (2 часа)

Рассматриваемые вопросы:

Национальная безопасность: виды безопасности: государственная, экономическая, общественная, военная, экологическая, информационная; роль и место системы обеспечения информационной безопасности (ИБ) в системе национальной безопасности РФ; доктрина ИБ, история проблемы ИБ, угрозы ИБ; методы и средства обеспечения ИБ.

Лекция 1.2. Основные понятия информационной безопасности (2 часа)

Рассматриваемые вопросы:

Основные термины и определения дисциплины ИБ. Методологические и технологические основы комплексного обеспечения ИБ; модели, стратегии и системы обеспечения ИБ; методы управления, организации и обеспечения работ по обеспечению ИБ; обеспечение ИБ в нормальных и чрезвычайных ситуациях; проблемы информационной войны.

Лекция 1.3. Нормативно-правовое обеспечение информационной безопасности (2 часа)

Рассматриваемые вопросы:

Законодательство РФ в области информационной безопасности, защиты государственной тайны и конфиденциальной информации; конституционные гарантии прав граждан на информацию и механизм их реализации; понятие и виды защищаемой информации по законодательству РФ; защита интеллектуальной собственности средствами патентного и авторского права; правовая регламентация охранной деятельности; международное законодательство в области защиты информации.

Лекция 1.4. Персональные данные (2 часа)

Рассматриваемые вопросы:

Определение персональных данных. Конфиденциальность персональных данных. Конституция, закон №24-ФЗ о персональных данных. Принципы обработки персональных данных. Специальные категории. Обеспечения защиты и разграничение доступа к персональной информации. Биометрические персональные данные. Создание, использованием программ и баз данных персональных данных и их правовая охрана.

Лабораторная работа №1. Защита документов MS Office (2 часа)

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 (2 часа)

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 (2 часа)

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. (4 часа)

Подготовка к лекциям.

Изучение дополнительного теоретического материала.

Подготовка теоретического материала и данных для выполнения лабораторных работ.

Подготовка и прохождение тестирования (с использованием программы информационной системы «*КТест*»).

Примеры вопросов теста:

1. Что такое конфиденциальность информации?

- гарантия того, что конкретная информация доступна только тому кругу лиц, для которого она предназначена
- защищенность информации от несанкционированного доступа
- гарантия того, что источником информации является именно то лицо, которое заявлено как ее автор
- гарантия того, что при необходимости можно будет доказать подлинность информации
- гарантия того, что информация представлена в неискаженном виде

2. Что такое целостность информации?

- гарантия того, что информация представлена в неискаженном (исходном) виде
- доступность информации разрешенному кругу лиц
- гарантия того, что представлена не только сама информация, но и её источник, объем, дата последней корректировки
- гарантия того, что информация представляется в полном объеме, а не по частям

3. Что такое аутентичность информации?

- гарантия того, что источником информации является именно то лицо, которое заявлено как ее автор
- гарантия того, что информация сейчас существует в ее исходном виде
- гарантия того, что конкретная информация доступна только тому кругу лиц, для которого она предназначена

Тема 2. Стандарты и спецификации в области информационной безопасности

Лекция 2.1. Требования безопасности к информационным системам (2 часа)

Рассматриваемые вопросы:

Структура и принципы функционирования современных вычислительных систем. Проблемы обеспечения безопасности обработки и хранения информации в вычислительных системах. Базовые этапы построения системы комплексной защиты вычислительных систем. Анализ моделей нарушителя. Угрозы информационно-программному обеспечению вычислительных систем и их классификация. Функции системы защиты по предупреждению угроз и устранению последствий их реализации. Классификация способов и средств комплексной защиты информации. Классификация методов защиты информации с использованием программно-аппаратных средств вычислительной системы.

Лекция 2.2. Стандарты информационной безопасности распределенных систем (2 часа)

Рассматриваемые вопросы:

Сервисы безопасности в вычислительных сетях: аутентификация, аутентификация партнеров по общению, управление доступом, конфиденциальность данных, конфиденциальность трафика, целостность данных, неотказываемость. Механизмы безопасности. Администрирование средств безопасности информационной системы: сервисов безопасности, механизмов безопасности. Обеспечение доступности информации. Защитные меры.

Лекция 2.3. Стандарты информационной безопасности в РФ (2 часа)

Рассматриваемые вопросы:

Стандарты информационной безопасности. Гостехкомиссия и ее роль в обеспечении информационной безопасности в РФ. Документы по оценке защищенности автоматизированных систем в РФ. Показатели защищенности. Классы защищенности.

Стандарты оценки безопасности вычислительных систем. Требования руководящих документов Гостехкомиссии.

Лабораторная работа № 4. Открытые порты и запущенные службы (2 часа)

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 (2 часа)

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

СРС по теме 2. (2 часа)

Подготовка к лекциям.

Изучение дополнительного теоретического материала.

Подготовка теоретического материала и данных для выполнения лабораторных работ.

Подготовка и прохождение тестирования (с использованием программы информационной системы «*КТест»*).

Примеры вопросов теста:

1. Угрозы безопасности распределенным вычислительным системам классифицируются:
   - по цели воздействия
   - по характеру воздействия
   - по условию начала воздействия
   - по расположению субъекта относительно объекта атаки
   - по соответствию уровня модели ISO/OSI операционной системе
   - по уровню эталонной модели ISO/OSI, на котором производится воздействие
   - по условию окончания воздействия
2. По характеру воздействия угрозы распределенным вычислительным системам классифицируются на:
   - Пассивное (прослушивание канала)
   - Активное (производится изменения в системе)
   - Удаленное (используется сеть Интернет)
   - Скрытое (применяются средства криптографии)
   - Безвозмездное (оплата пользователем не требуется)
3. Сколько потенциальных каналов несанкционированного доступа обнаружено в TCP/IP-сети?
   - Около 135
   - 32
   - не больше 50
   - более 500

Дисциплинарный модуль 2

Продолжительность модуля 11 недель.

Тема 3. Вредоносное программное обеспечение

Лекция 3.1. Компьютерные вирусы (2 часа)

Рассматриваемые вопросы:

История появления компьютерных вирусов и факторы, влияющие на их распространение. Понятие компьютерного вируса. Основные этапы жизненного цикла вирусов. Объекты внедрения, режимы функционирования и специальные функции вирусов. Схемы заражения файлов. Схемы заражения загрузчиков. Способы маскировки, используемые вирусами. Классификация компьютерных вирусов.

Лекция 3.2. Программные закладки и троянские кони (2 часа)

Рассматриваемые вопросы:

Программными закладки (троянские кони). Классификация закладок. Резидентные закладки. Воздействие программных закладок на системы: перехват, искажение, сборка мусора. Примеры программных закладок и «троянцев». Клавиатурные шпионы: имитаторы, фильтры и заместители.

Лекция 3.3. Защита, обнаружение и удаление компьютерных вирусов (2 часа)

Рассматриваемые вопросы:

Общая организация защиты от компьютерных вирусов. Транзитный и динамический режимы антивирусной защиты. Поиск вирусов по сигнатурам и обезвреживание обнаруженных вирусов. Углубленный анализ на наличие вирусов путем контроля эталонного состояния компьютерной системы. Защита от деструктивных действий и размножения вирусов. Использование средств аппаратного и программного контроля. Стратегия заблаговременной подготовки к эффективной ликвидации последствий вирусной эпидемии. Технология гарантированного восстановление вычислительной системы после заражения компьютерными вирусами.

Лабораторная работа № 6. Вирусы и антивирусные системы (2 часа)

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 (2 часа)

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.

СРС по теме 3. (7 часов)

Подготовка к лекциям.

Изучение дополнительного теоретического материала.

Подготовка теоретического материала и данных для выполнения лабораторных работ.

Подготовка и прохождение тестирования (с использованием программы информационной системы «*КТест*»).

Примеры вопросов теста:

1. Компьютерный вирус – это…

• программа, которая может «заражать» другие программы, модифицируя их так, чтобы включать в них свою, возможно, измененную копию

• код, обладающий способностью к распространению (возможно, с изменениями) путём внедрения в другие программы

• следствие ошибки в операционной системе компьютера

• безвредный код, внедряющийся в другие программы

• программа, которая может «заражать» другие программы, полностью изменяя их код

2. Создание компьютерных вирусов является…

• преступлением

• последствием сбоев операционной системы

• необходимым компонентом подготовки программистов

• побочным эффектом при разработке программного обеспечения

3. К антивирусным программам НЕ относятся:

• интерпретаторы

• фаги

• мониторы

• ревизоры

• фильтры

4. По среде обитания вирусы делятся на…

- файловые, загрузочные, макровирусы, сетевые
- резидентные и нерезидентные
- безвредные, неопасные, опасные, очень опасные
- «спутники», «черви», невидимки, полиморфные, резидентные
- командные, загружаемые, выполняемые

Тема 4. Криптография, шифрование и защита данных

Лекция 4.1. Введение и основные понятия криптографии (2 часа)

Рассматриваемые вопросы:

Введение в криптографию. Представление защищаемой информации. Угрозы безопасности информации. Ценность информации. Основные термины и понятия криптографии. Открытые сообщения и их характеристики. Модели открытых сообщений; исторический очерк развития криптографии. Общая организация криптографической защиты информации. Использование общесистемных и специализированных программных средств для шифрования файлов, и работы с секретными внешними носителями информации.

Лекция 4.2. Методы криптографического шифрования (2 часа)

Рассматриваемые вопросы:

Типы криптографических систем. Простые методы шифрования: шифры подстановки и перестановки. Подстановки с переменным коэффициентом сдвига. Многослойные шифры. Скоростные и недетерминированные программные шифры. Основы скоростного шифрования. Внесение неопределенностей в процесс криптографических преобразований. Стандарты шифрования.

Лекция 4.3. Электронная цифровая подпись (2 часа)

Рассматриваемые вопросы:

Ассиметричное шифрование. Использование псевдослучайных чисел для генерации ключей. Выбор порождающего числа и максимизация длины последовательности чисел ключа. Режимы шифрования. Особенности шифрования данных в режиме реального времени. Шифрование ключа при необходимости его хранения с зашифрованными данными. Протоколы распределения ключей. Протоколы установления подлинности.

Лабораторная работа № 9. Применение методов гаммирования файлов (2 часа)

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 (4 часа)

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 шифрования и дешифрования открытого текста.

Лабораторная работа № 11. Разработка алгоритма определения частоты букв и его применение для дешифровки текста, зашифрованного методом подстановки (2 часа)

Задание: На основе учебного материала по криптоаналитическим методам дешифровки защищенных данных изучить метод подстановки и реализовать его, разработав алгоритм.

СРС по теме 4 (10 часов)

Подготовка к лекциям.

Изучение дополнительного теоретического материала.

Подготовка теоретического материала и данных для выполнения лабораторных работ.

Подготовка и прохождение тестирования (с использованием программы информационной системы «*КТест*»).

Примеры вопросов теста:

1. Криптографический алгоритм - это...

- формула, используемая для шифрования и расшифровки сообщений
- формула, используемая для шифрования сообщения
- формула, используемая для расшифровки сообщения
- программа для передачи зашифрованного сообщения
- последовательность использования ключей для дешифровки

2. Криптосистема - это…

- совокупность алгоритма расшифровки и шифрования, открытых текстов, способов, методов шифровки.
- совокупность ключей для шифровки и дешифровки
- совокупность открытых текстов и шифртекстов
- механизм распознавания открытого текста

3. Шифрование - это...

- преобразование информации в целях сокрытия от неавторизованных лиц с предоставлением авторизованным пользователям доступа
- преобразование информации в целях ограниченного использования в госструктурах
- преобразование информации в целях сокрытия от окружающих людей
- преобразование информации в целях конфиденциальности на предприятии

Тема 5. Методы и средства обеспечения информационной безопасности

Лекция 5.1. Системы идентификации и аутентификации пользователей (2 часа)

Рассматриваемые вопросы:

Идентификация пользователей и установление их подлинности при доступе к компьютерным ресурсам. Основные этапы допуска к ресурсам вычислительной системы. Использование простого пароля. Использование динамически изменяющегося пароля. Взаимная проверка подлинности и другие случаи опознания. Парольное разграничение доступа и комбинированные методы. Защита программных средств от несанкционированного копирования, исследования и модификации. Привязка программ к среде функционирования. Защита программ от несанкционированного запуска.

Лекция 5.2. Методы разграничения доступа (2 часа)

Рассматриваемые вопросы:

Способы разграничения доступа к компьютерным ресурсам. Разграничение доступа по спискам. Использование матрицы установления полномочий. Произвольное и принудительное управление доступом. Разграничение доступа по уровням секретности и категориям. Особенности программной реализации контроля установленных полномочий.

Лекция 5.3. Регистрация и аудит (2 часа)

Рассматриваемые вопросы:

Определение и содержание регистрации и аудита информационных систем. Фиксация событий безопасности. Аудит и эффективность системы безопасности. Реализация механизмов регистрации и аудита. Задачи аудита. Практические средства регистрации и аудита. Регистрационный журнал. Подозрительная активность. Этапы регистрации и методы аудита событий информационной системы. Статистические и эвристические методы анализа информации с целью выявления несанкционированных действий.

Лекция 5.4. Оценка затрат на информационную безопасность (2 часа)

Рассматриваемые вопросы:

Методики оценки затрат: прикладного информационного анализа (Applied Information Economics), потребительского индекса (Customer Index, CI), добавленной экономической стоимости (Economic Value Added), исходной экономической стоимости (Economic Value Sourced), управления портфелем активов (Portfolio Management), оценки возможностей (Real Option Valuation), жизненного цикла ИС (System Life Cycle Analysis), системы сбалансированных показателей (Balanced Scorecard(BSC)), TCO (Total Cost of Ownership), функционально-стоимостного анализа (Activity Based Costing)

Лабораторная работа № 13. Восстановление паролей к документам MS Office (2 часа)

Задание: На основе учебного материала по криптографическим методам шифрования документов подготовить файлы в формате MS Word, MS Excel, MS Access, защитить их, подобранным для этой операции, паролем и проверить на чтение, редактирование. Затем воспользоваться программой Accent OFFICE Recovery и восстановить пароли к документам MS Office.

Лабораторная работа № 14. Вскрытие паролей файловых архивов (2 часа)

Задание: На основе учебного материала по криптографическим методам шифрования документов подготовить файл и провести архивацию его разными форматами. Затем воспользоваться программой Visual Zip Password Recovery Processor (VZPRP) и восстановить пароли к архивам. Проверить возможность прочтения архивированных файлов.

Лабораторная работа № 15. Экономический расчет коэффициентов эффективности информационной безопасности предприятия (2 часа)

Задание: Изучить теоретические аспекты экономического расчета коэффициентов эффективности информационной безопасности предприятия. Рассчитать показатель эффективности инвестиций на информационную безопасность предприятия (метод ROI для оценки возврата инвестиций). Оформить расчеты в виде отчета эффективности информационной безопасности предприятия.

СРС по теме 5 (8 часов)

Подготовка к лекциям.

Изучение дополнительного теоретического материала.

Повторение пройденного материала всех разделов.

Подготовка к контрольному тестированию (с использованием программы информационной системы «*КТест*»).

Подготовка к экзамену.

2.3. 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.

3. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине «Защита информации» 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.

4. РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА

4.1. Основная литература

1. Мельников В.П. Информационная безопасность и защита информации: учеб. посо бие / 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.

4.2. 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. Защита интеллектуальной собственности, 2018 г. – коллекция "Экономика и менеджмент – Издательство Дашков и К" ЭБС ЛАНЬ
3. Куприянов А.И. Основы защиты информации: учеб. пособие / А.И. Куприянов, 2008г. 3

4.3. Методические указания

1. Проценко И.Г. Защита информации. Конспект лекций. / И.Г. Проценко – Петропавловск-Камчатский: КамчатГТУ, 2019. – 66 с.
2. Проценко И.Г. Защита информации. Лабораторный практикум. / И.Г. Проценко – Петропавловск-Камчатский: КамчатГТУ, 2019. – 50 с.

4.4. Перечень ресурсов *информационно-телекоммуникационной сети «Интернет»*

1. 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/
2. 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/
3. 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

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

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

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

Лекции посвящаются рассмотрению наиболее важных концептуальных вопросов: основным понятиям; теоретическим основам информационной безопасности, 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. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации или на практическом занятии.

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 экзамену. 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 защиты данных и обеспечения информационной безопасности 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.

6. КУРСОВОЙ ПРОЕКТ (РАБОТА)

В соответствии с учебным планом курсовое проектирование по дисциплине «Защита информации» не предусмотрено.

7. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

7.1. Перечень *информационных технологий, используемых при осуществлении образовательного процесса*

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.

7.2. Перечень программного обеспечения, используемого при осуществлении образовательного процесса

При освоении дисциплины используется лицензионное программное обеспечение: пакет Microsoft Office;

Кроме этого используется программное обеспечение информационной системы «КТест» и программные средства, необходимые для выполнения лабораторных работ, указанных в аннотации к работам (см. *Проценко И.Г.* Защита информации: лабораторный практикум. – Петропавловск-Камчатский: КамчатГТУ, 2019. – 50 с.)

7.3. Перечень информационно-справочных систем

При освоении дисциплины используются следующие информационно-справочные системы:

– 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

8. 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 «Защита информации».

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 № 7-520 с комплектом учебной мебели на 25 посадочных мест;

– для лабораторных работ - лабораторная аудитория № 7-401, 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 «Защита информации»;
– информационная система «*КТест*», установленная на всех рабочих станциях.