МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Магнитогорский государственный технический университет»
(ФГБОУ ВО «МГТУ им. Г.И. Носова»)

УТВЕРЖДАЮ:
Директор института гуманитарного образования
_____ О.В. Гневэк
«__» _____ 2016 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Обработки и защита документированной информации (Б1.В.ОД.13)

НАИМЕНОВАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Направление подготовки (специальность)
46.03.02 Документоведение и архивоведение
шифр наименование направления подготовки

Документоведение и документационное обеспечение управления
наименование направленности (профиля) подготовки

Уровень высшего образования – бакалавриат

Программа подготовки – академический бакалавриат

Форма обучения
Заочная

Институт *Гуманитарного образования*

Кафедра *Социологии, документоведения и архивоведения*
Курс 5

Магнитогорск
2016 г.

Рабочая программа составлена на основе ФГОС ВО по направлению подготовки 46.03.02 Документоведение и архивоведение, утвержденного приказом МОиН РФ от «6» марта 2015 № 176.

Рабочая программа рассмотрена и одобрена на заседании кафедры социологии, документоведения и архивоведения «05» сентября 2016 г., протокол № 1.

Зав. кафедрой _____ / С.С. Великанова /
(подпись) (И.О. Фамилия)

Рабочая программа одобрена методической комиссией института гуманитарного образования «05» сентября 2016 г., протокол № 1.

Председатель _____ / О.В. Гневэк /
(подпись) (И.О. Фамилия)

Рабочая программа составлена: доцент каф. СДиА, к.п.н., доцент
(должность, ученая степень, ученое звание)

_____ / Е.П. Романов /
(подпись) (И.О. Фамилия)

Рецензент: Ст. архивист архива ОАО «ММК»
(должность, ученая степень, ученое звание)

_____ / С.А. Белобородова /
(подпись) (И.О. Фамилия)

Лист регистрации изменений и дополнений

№ п/п	Раздел программы	Краткое содержание изменения/дополнения	Дата. № протокола заседания кафедры	Подпись зав. кафедрой
1	п.8, п.9.	актуализация учебно-методического и информационного обеспечения дисциплины; актуализация материально-технического обеспечения дисциплины	23.10.2017, № 2	
2	п.8, п.9.	актуализация учебно-методического и информационного обеспечения дисциплины; актуализация материально-технического обеспечения дисциплины	01.10.2018, №2	
3	п.8, п.9.	актуализация учебно-методического и информационного обеспечения дисциплины; актуализация материально - технического обеспечения дисциплины	07.10.2019, №2	
4	п.8. п.9.	актуализация учебно-методического и информационного обеспечения дисциплины; актуализация материально-технического обеспечения дисциплины	03.09.2020, № 1	

1. Цели освоения дисциплины (модуля)

Цель курса: сформировать у студентов теоретические знания по основам защиты информации при обращении с компьютерной техникой и программным обеспечением и, в особенности, в области применения различных сетевых технологий, а также практических навыков обеспечения защиты информации в системах обработки информации.

2. Место дисциплины (модуля) в структуре образовательной программы подготовки бакалавра (магистра, специалиста)

Дисциплина «Обработка и защита документированной информации» входит в базовую часть образовательной программы по направлению 46.03.02 Документоведение и архивоведение (профиль «Документоведение и документационное обеспечение управления»).

Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин: Введение в профессию, Государственные, муниципальные и ведомственные архивы, Делопроизводство коммерческих предприятий, Делопроизводство муниципальных учреждений, Документационное обеспечение административных отношений в РФ, Документационное обеспечение архивного дела и информационной сферы в РФ, Документационное обеспечение государственного устройства в РФ, Документационное обеспечение гражданских отношений в РФ, Документационное обеспечение трудовых отношений в РФ, Индексация и кодификация информации в профессиональной деятельности, Информатика, Кадровое делопроизводство и архивы документов по личному составу, Моделирование систем документации организации, Организация и технология документационного обеспечения управления, Основы архивоведения, Основы секретарского обслуживания, Продвижение научной продукции, Проектная деятельность.

Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин: Документирование деятельности негосударственных организаций, Документационное обеспечение управления на предприятиях различных организационно-правовых форм, Документы и документооборот в бухгалтерском учете, Международные стандарты управления документами, Методы рационализации ДОУ, Обработки и защита документированной информации, Организация и технология документационного обеспечения управления, Персональные данные и их документирование, Управление информационными ресурсами в России и за рубежом, Современные проблемы документоведения и архивоведения, Производственная - практика по получению профессиональных умений и опыта профессиональной деятельности, Производственная – преддипломная практика, Государственная итоговая аттестация.

При освоении данной дисциплины необходимы знания, умения и навыки в оформлении и составлении документов; знание законодательных и нормативно-методических документов в сфере информации и документирования; знание правовых норм, предусматривающих ответственность за определенный вид деяний.

3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения

В результате освоения дисциплины (модуля) «Деловая переписка» обучающийся должен обладать следующими компетенциями:

ОК-10 способностью к использованию основных методов, способов и средств получения, хранения, переработки информации

ОПК-2 владением базовыми знаниями в области информационных технологий

ОПК-4 владением навыками использования компьютерной техники и информа-

ционных технологий в поиске источников и литературы, использовании правовых баз данных, составлении библиографических и архивных обзоров

ОПК-6 способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

ПК-6 способностью анализировать ситуацию на рынке информационных продуктов и услуг, давать экспертную оценку современным системам электронного документооборота и ведения электронного архива

ПК-14 владением навыками использования компьютерной техники и информационных технологий в документационном обеспечении управления и архивном деле

ПК-15 способностью совершенствовать технологии документационного обеспечения управления и архивного дела на базе использования средств автоматизации

ПК-17 владением методами защиты информации

Структурный элемент компетенции	Планируемые результаты обучения
ОК-10 способностью к использованию основных методов, способов и средств получения, хранения, переработки информации	
Знать	Принципы организации и функционирования компьютерных систем. Основные программные средства для работы с документированной информацией. Принципы и технические средства хранения, обработки и передачи информации в ПК и компьютерных сетях в аспекте обеспечения информационной безопасности и защиты информации.
Уметь:	Работать с операционной системой и программными средствами общего назначения. Настраивать операционную систему и программные средства общего назначения с позиции требований информационной безопасности и защиты информации Анализировать явные и скрытые угрозы защищаемой информации.
Владеть:	Основными методами, способами и средствами получения, хранения, переработки информации. Навыками обеспечения защиты информации штатными средствами операционной системы. Навыками получения, хранения и уничтожения информации с учетом требований информационной безопасности.
ОПК-2 владением базовыми знаниями в области информационных технологий	
Знать	Базовые понятия в области ИТ. Сущность и общую характеристику информационных процессов информационного общества в аспекте информационной безопасности. Современное состояние уровня и направлений развития программных средств в области обеспечения информационной безопасности и защиты информации.

Структурный элемент компетенции	Планируемые результаты обучения
Уметь	Самостоятельно ориентироваться в современных информационных технологиях профессиональной области. Применять с профессиональной деятельности современные средства ИКТ. Обеспечивать защиту информации во время работы с современными средствами ИКТ.
Владеть	Навыками использования современных ИКТ. Принципами работы служб Интернет для сбора профессиональной информации. Базовыми приемами размещения информации в открытом доступе с помощью современных ИКТ.
ОПК-4 владением навыками использования компьютерной техники и информационных технологий в поиске источников и литературы, использовании правовых баз данных, составлении библиографических и архивных обзоров	
Знать	Основные понятия и определения в области обеспечения информационной безопасности и защиты информации. Классификации вредоносных программ Способы защиты информации в автоматизированных системах обработки данных, глобальных и локальных сетях, защиты от вредоносных программ
Уметь	Сохранять информацию от несанкционированного доступа. Настраивать и использовать специализированное антивирусное ПО. Использовать методы и средства защиты информации.
Владеть	Профессиональным языком предметной области знания. Навыками защиты и борьбы с вредоносными программами. Навыками применения программных средств защиты информации в компьютерных сетях.
ОПК-6 способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	
Знать	Основные положения государственной политики обеспечения информационной безопасности и защиты информации. Нормы информационной этики и права. Принципы работы с информацией на различных ресурсах, с учетом требований информационной безопасности.
Уметь	Применять на практике соответствующие требования и нормы обеспечения информационной безопасности и защиты информации. Соблюдать права интеллектуальной собственности на информацию. Оформлять результаты исследований и вести текущую работу с учетом требований и норм обеспечения информационной безопасности и защиты информации.
Владеть	Основными методами исследования в области информационной безопасности и практическими умениями и навыками их использования.

Структурный элемент компетенции	Планируемые результаты обучения
	Общими принципами соблюдения требований информационной этики и права. Способами совершенствования профессиональных знаний и умений путем использования возможностей информационной среды, с учетом требований государственных нормативных актов и информационной этики и права
ПК-6 способностью анализировать ситуацию на рынке информационных продуктов и услуг, давать экспертную оценку современным системам электронного документооборота и ведения электронного архива	
Знать	Основные понятия офисных информационных технологий. Особенности обеспечения защиты информации в офисных ИТ. Сферы применения методов обеспечения защиты информации в офисных ИТ.
Уметь	Демонстрировать навыки работы в офисных ИТ. Характеризовать основные способы защиты информации в офисных ИТ. Применять навыки настройки основных аспектов обеспечения защиты информации штатными средствами офисных ИТ.
Владеть	Навыком объяснения необходимости настройки офисных ИТ с позиции обеспечения информационной безопасности Навыком выделения основных способов защиты информации в офисных ИТ. Навыком настройки защиты информации в офисных ИТ.
ПК-14 владением навыками использования компьютерной техники и информационных технологий в документационном обеспечении управления и архивном деле	
Знать	Принципы использования компьютерной техники в документационном обеспечении управления и архивном деле. Принципы использования ИТ в документационном обеспечении управления и архивном деле. Принципы обеспечения информационной безопасности и защиты информации в процессе.
Уметь:	Работать с информацией в локальных сетях. Работать с информацией в глобальных сетях. Обеспечивать информационную безопасности и защиту информации в процессе работы.
Владеть:	Базовыми приемами работы с профессиональной информацией. Способами обеспечения защиты информации в процессе работы с профессиональной информацией. Нормативно-правовой информацией в области обеспечения защиты профессиональной информации.
ПК-15 способностью совершенствовать технологии документационного обеспечения управления и архивного дела на базе использования средств автоматизации	
Знать	Технологии документационного обеспечения управления и архивного дела на базе использования средств автоматизации. Способы обеспечения защиты информации с помощью средств автоматизации. Сферы применения способов обеспечения информационной

Структурный элемент компетенции	Планируемые результаты обучения
	безопасности на уровне технологий документационного обеспечения управления и архивного дела на базе использования средств автоматизации.
Уметь	Применять в стандартных рабочих ситуациях способы обеспечения информационной безопасности в средствах автоматизации. Характеризовать способы обеспечения информационной безопасности в технологиях документационного обеспечения управления и архивного дела на базе использования средств автоматизации. Корректно использовать средства защиты информации в средствах автоматизации технологий документационного обеспечения управления и архивного дела
Владеть	Навыком формулирования основных требований информационной безопасности к средствам автоматизации технологии документационного обеспечения управления и архивного дела. Навыком объяснения основных средств и методов обеспечения информационной безопасности в процессе работы с технологиями. Навыком применения средств и методов обеспечения информационной безопасности в процессе работы с технологиями.
ПК-17 владением методами защиты информации	
Знать	Нормативно-терминологическая база в области защиты информационной безопасности. Критерии отнесения информации к защищаемой. Методы и средства защиты информации.
Уметь:	Ориентироваться в программном обеспечении, необходимом для обеспечения защиты информации. Определять вид конфиденциальной информации. Применять на практике основные способы защиты информации на различных носителях.
Владеть:	Нормативно-терминологической базой в области защиты информации. Основными методами защиты информации на различных носителях. Основными методами построения системы защиты документированной информации в профессиональной области.

4. Структура и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет 3 зачетные единицы 108 акад. часа, в том числе:

- контактная работа – 11,3 акад. часов:
  - аудиторная – 8 акад. часа;
  - внеаудиторная – 3,2 акад. часа;
- самостоятельная работа – 88,1 акад. часов;
- подготовка к экзамену – 8,7 акад. часа.

Раздел/ тема дисциплины	Курс	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа (в акад. часах)	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код и структурный элемент компетенции
		лекции	лаборат. занятия	практич. занятия				
1. Информационная безопасность		2/2и			38,1	Самостоятельное изучение учебной и научной литературы Выполнение практических и теоретических заданий	контрольный тест	ОК-9 – зув, ОК-10 – зув, ОПК-2 – зув, ОПК-4 – зув, ПК-16 – зув
Итого по разделу (зимняя сессия)		4/4и			38,1			
2. Защита информации				2/2и	50	Самостоятельное изучение учебной и научной литературы Выполнение практических и теоретических заданий	контрольный тест	ОК-9 – зув, ОК-10 – зув, ОПК-2 – зув, ОПК-4 – зув, ПК-16 – зув
Итого по разделу (летняя сессия)		4/4и		2/2и	50		Контрольная работа	

Раздел/ тема дисциплины	Курс	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа (в акад. часах)	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код и структурный элемент компетенции
		лекции	лаборат. занятия	практич. занятия				
Итого по курсу		6/6и		2/2и			**Промежуточная аттестация – экзамен**	
Итого по дисциплине	5	6/6и		2/2и	**88,1**		**8,7**	

5. Образовательные и информационные технологии

Для реализации предусмотренных видов учебной работы используются интерактивные технологии – организация образовательного процесса, которая предполагает активное и нелинейное взаимодействие всех участников, достижение на этой основе личностно значимого для них образовательного результата. Наряду со специализированными технологиями такого рода принцип интерактивности прослеживается в большинстве современных образовательных технологий. Интерактивность подразумевает субъект-субъектные отношения в ходе образовательного процесса и, как следствие, формирование саморазвивающейся информационно-ресурсной среды.

В ходе проведения занятий предусматривается использование средств вычислительной техники при выполнении заданий.

6. Учебно-методическое обеспечение самостоятельной работы студентов

Аудиторная самостоятельная работа студентов на данном курсе не предусмотрена.

Внеаудиторная самостоятельная работа студентов осуществляется в виде изучения лекционного курса и литературы по соответствующему разделу с проработкой материала (выполнение тестов и практических заданий).

Пример практических заданий по курсу:

1. Информационная безопасность

Лабораторная работа «Работа с браузером»

Ответить на следующие вопросы. Ответы продемонстрировать преподавателю в виде скриншотов или развернутого текстового описания:

1. Как установить страницу, с которой будет происходить начальная загрузка?
2. Как заблокировать рекламу, отображаемую во всплывающих окнах?
3. Как позволить отдельным ресурсам использование всплывающих окон?
4. Как составить список сайтов, доступ к которым заблокирован?
5. Как очистить кэш браузера? Для чего это нужно делать?
6. Что такое файлы «cookie», для чего они нужны, в чем их опасность?
7. Что такое «режим инкогнито» («приватный режим»)? Для чего он нужен? Как его включить?
8. Что такое «плагин»? Для чего он нужен? Как установить и удалить плагин?
9. Где хранятся пароли в вашем любимом браузере? Как получить к ним доступ?
10. Настройте синхронизацию для вашего браузера. Что это такое? Для чего необходимо использовать синхронизацию?
11. Настройте приоритетные поисковые системы в браузере.
12. Поменяйте оформление браузера по вашему вкусу.

Лабораторная работа «Настройка прав доступа

в операционной системе Windows»

Ответы продемонстрировать преподавателю в виде скриншотов или развернутого текстового описания.

Задание 1 «Создание учетной записи пользователя»

1. Создайте учетную запись для своего пользователя.
2. Тип учетной записи – с ограниченными возможностями.
3. Выберите изображение для своей учетной записи.
4. Установите пароль.
5. Установите параметр «Требовать нажатие клавиш Ctrl+Alt+Delete» («Классическое окно ввода»).
6. Отключите учетную запись «Гость» (если она есть).

Задание 2 «Установление пароля для экранной заставки»

Рабочий стол (правая кнопка мыши) ® Свойства ® Заставка

1. Выберите заставку из предложенных.
2. При необходимости настройте параметры по вашему вкусу.
3. Установите флажок «Защита паролем».
4. Проверьте. Если пароль на заставку не работает, подумайте, почему это может быть (подсказка – учетная запись пользователя).

Задание 3 «Личные папки пользователя»

Войдите в систему под своей учетной записью. Выберите папку, доступ к которой вы хотите ограничить. Щелкните на ней правой кнопкой мыши, в меню выберите Свойства ® Вкладка Доступ. Установите флажок «Отменить общий доступ к этой папке».

Лабораторная работа «Защита информации в текстовом редакторе»

Задание 1

Самостоятельно ознакомиться с возможностями настройки защиты информации в текстовом редакторе.

Задание 2

Настроить следующие способы защиты документа:

1. Документ Фамилия_Doc1 при открытии требует пароль на доступ к файлу, модификация файла запрещена (изменение текста невозможно).
2. Документ Фамилия_Doc2 открывается только для чтения.
3. Документ Фамилия_Doc3 при открытии требует пароль на доступ к файлу и редактирование (2 разных пароля).

Лабораторная работа «Защита данных с помощью архивирования»

- Создайте на рабочем диске папку «Фамилия». Скопируйте в нее файлы следующего типа *.doc, *.xls, *.jpg.

- Заархивируйте папку с паролем с помощью любой программы-архиватора. Имя архива должно быть вида «Фамилия».
- Продемонстрируйте результаты преподавателю.

2. Защита информации

Лабораторная работа «Защита личной информации при пользовании сервисами Google»

Ответы продемонстрировать преподавателю в виде скриншотов или развернутого текстового описания:

1. Просмотрите историю поисковых запросов. Отключите сохранение истории.
2. Просмотрите историю загруженных игр.
3. Просмотрите историю местоположений. Подумайте, каким образом можно отменять сохранение истории, не используя ее отключение. Попробуйте проделать эти действия. Проверьте результат в течение нескольких дней.
4. Очистите данные в настройках рекламы. Отключите сервис Google Analytics.
5. Просмотрите данные о контактах – все ли контакты вам необходимы? Настройте сведения о контактах.
6. Привяжите свой аккаунт к номеру телефона, активизируйте передачу информации о подозрительных действиях. Для чего это нужно?
7. Проверьте список устройств, с которых происходило подключение к аккаунту. Для чего это нужно? Что можно сделать с незнакомым устройством?
8. Проверьте настройки доступа к аккаунту. Просмотрите список приложений, сайтов и устройств, связанных с вашим аккаунтом Google. Убедитесь, что все они надежны, и удалите ненужные. Не забывайте очищать данный список после удаления игр и приложений. Для чего необходимо это делать?
9. Запретите непроверенным приложениям доступ к аккаунту.
10. Проверьте резервный адрес электронной почты. Для чего он необходим?
11. Что такое «двухэтапная авторизация и для чего она необходима»?
12. Настройте сохранение данных аккаунта.

Лабораторная работа «Антивирусная программа»

Задание 1

Самостоятельно познакомиться с возможностями антивирусной программы, установленной на компьютере. Изучить следующие пункты:

1. Запуск программы.
2. Основное окно программы.
3. Окно помощи.

Задание 2

Изучить особенности:

1. Проверка компьютера (полностью).

2. Запуск проверки подключаемого носителя.

- по требованию пользователя;

- автоматический запуск при подключении.

3. Контроль за контентом:

- шпионские программы;

- «заражённые» сайты;

- фишинг-атаки и пр.

Лабораторная работа «Защита информации в социальных сетях»

Рассмотрите особенности защиты информации в наиболее распространенных социальных сетях (В контакте, Одноклассники, Мой мир, Фейсбук и др.)

Ответить на следующие вопросы, доказать ответ скриншотами:

1. Доступность создания «фейковых» анкет (Ненастоящие имя, фамилия, либо использование данных известных людей)

2. Доступность закрытия информации при регистрации (дата рождения, образовательные заведения и пр.)

3. Вы обнаружили в социальной сети ваш «клон». Ваши действия? (описать со ссылками и скриншотами)

4. Вы обнаружили, что некий человек пишет вам негативные и агрессивные сообщения. Ваши действия? (показать скриншоты)

5. Имеете ли вы возможность создания определенных списков друзей, с различными уровнями допуска к вашей информации?

6. Вы разместили в своем аккаунте информацию конфиденциального характера. Каким образом вы можете ограничить доступ остальных к этой информации? (показать скриншоты)
Ответить на вопрос для:

- Фотографии;
- Фотоальбома;
- Видеозаписи;
- Текстовой записи.

7. Какие действия и тексты в приложении должны заставить вас насторожиться? Что может, а чего не может просить от вас приложение?

8. Какие действия вы должны предпринять, получив подобное сообщение?

Я вообще-то с просьбой к тебе) Как-то даже неудобно спрашивать, если честно) У тебя есть рублей пятьсот мне на модем закинуть надо?) А то закончились на нем деньги. А я отдам чуть позже!)

9. Каким образом вы можете восстановить утраченный пароль?

10. Охарактеризуйте в целом возможности защиты личной информации в выбранной вами социальной сети.

7. Оценочные средства для проведения промежуточной аттестации

а) Планируемые результаты обучения и оценочные средства для проведения промежуточной аттестации:

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
ОК-10 способностью к использованию основных методов, способов и средств получения, хранения, переработки информации		
Знать	Принципы организации и функционирования компьютерных систем. Основные программные средства для работы с документированной информацией. Принципы и технические средства хранения, обработки и передачи информации в ПК и компьютерных сетях в аспекте обеспечения информационной безопасности и защиты информации.	1. Какие новые возможности и новые проблемы влечет за собой стремительное развитие информационной среды обитания? 2. Какие новые возможности для человека возникают в информационном обществе? 3. Основные направления развития информационных технологий. 4. Основные информационные проблемы обеспечения национальной безопасности. 5. Каковы основные цели и объекты информационной безопасности страны. 6. Основные цели и методы информационной войны. 7. Информационное оружие 8. Опыты ведения информационных войн. 9. Сценарии будущих информационных войн.
Уметь:	Работать с операционной системой и программными средствами общего назначения. Настраивать операционную систему и программные средства об-	1 Программная система защиты информации отвечает за: а) Сохранность всей введённой в информационную систему информации. **б) Реализацию заданной политики безопасности.** в) Корректное поведение пользователей. 2 Аутентификация это:

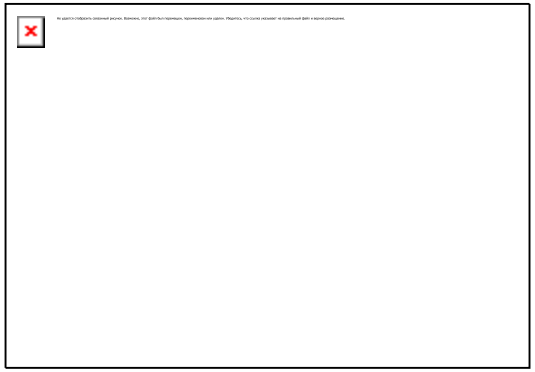
Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
	щего назначения с позиции требований информационной безопасности и защиты информации Анализировать явные и скрытые угрозы защищаемой информации.	**а) Подтверждение заявленного идентификатора.** б) Процесс ввода текста без отображения на экране. в) Ввод сведений личного характера. 3 Политика безопасности это: **а) Правила определения разрешённых и запрещённых операций в** информационной системе. б) Правила поведения пользователей. в) Инструкция действий администратора по обеспечению информационной безопасности. 4 Монитор безопасности это: а) Личный терминал системного администратора. **б) Совокупность резидентных программ, реализующих политику** безопасности. в) Программа контроля данных аудита. 5 Дискреционная политика доступа: **а) Определяет права доступа идентифицированных субъектов к объектам на основе заданных внешних правил (матрицы доступа).** б) Определяет права доступа субъектов к объектам или разрешает информационные потоки между объектами на основе изменяемых меток прав доступа или конфиденциальности. в) Является алгоритмом формирования матрицы доступа. г) Содержит инструкцию для системного администратора по предоставлению прав доступа различным пользователям.
Владеть:	Основными методами, способами и средствами получения, хранения, переработки информа-	***Контрольная работа*** **Защита информации с помощью криптографии**

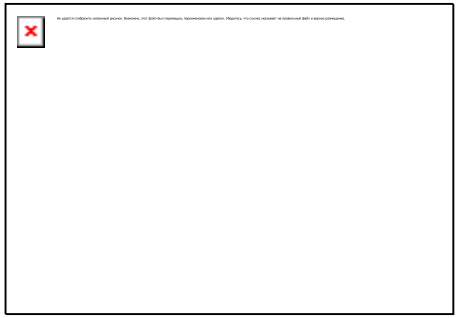
Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
	ции. Навыками обеспечения защиты информации штатными средствами операционной системы. Навыками получения, хранения и уничтожения информации с учетом требований информационной безопасности.	**1. Цель работы** Целью работы является исследование защиты информации с применением простейших принципов криптографии. **2. Теоретическая часть** **2.1 Шифры замены** Сущность шифрования методом замены заключается в следующем [2]. Пусть шифруются сообщения на русском языке и замене подлежит каждая буква этих сообщений. Тогда, букве **А** исходного алфавита сопоставляется некоторое множество символов (шифрозамен) $\mathbf{M_А}$**, Б –** $\mathbf{M_Б}$**, …, Я –** $\mathbf{M_Я}$. Шифрозамены выбираются таким образом, чтобы любые два множества ($\mathbf{M_i}$ и $\mathbf{M_j}$, $\mathbf{i \neq j}$) не содержали одинаковых элементов ($\mathbf{M_i \cap M_j = \varnothing}$). Таблица, приведенная на рис.1, является ключом шифра замены. Зная ее, можно осуществить как шифрование, так и расшифрование.  Рис.1. Таблица шифрозамен При шифровании каждая буква **А** открытого сообщения заменяется любым символом из множества $\mathbf{M_А}$. Если в сообщении содержится несколько букв **А**, то каждая из них заменяется на любой символ из $\mathbf{M_А}$. За счет этого с помощью одного ключа можно получить различные варианты шифрограммы для одного и того же открытого сообщения. Так как множества $\mathbf{M_А, M_Б, ..., M_Я}$ попарно не пересекаются, то по каждому символу шифрограммы

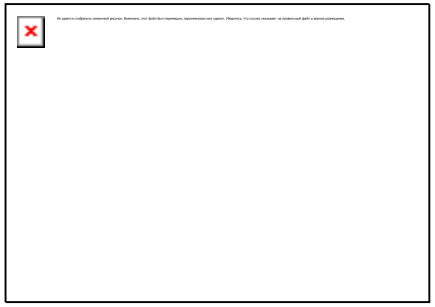
Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		можно однозначно определить, какому множеству он принадлежит, и, следовательно, какую букву открытого сообщения он заменяет. Поэтому расшифрование возможно и открытое сообщение определяется единственным образом. Метод замены часто реализуется многими пользователями при работе на компьютере. Если по забывчивости не переключить на клавиатуре набор символов с латиницы на кириллицу, то вместо букв русского алфавита при вводе текста будут печататься буквы латинского алфавита («шифрозамены»). Шифры замены можно разделить на следующие **подклассы**: - **шифры однозначной замены** (моноалфавитные, простые подстановочные). Количество шифрозамен для каждого символа исходного алфавита равно 1 (| $\mathbf{M}_i$ | = 1 для одного символа); - **полиграммные шифры**. Аналогичен предыдущему за исключением того, что шифрозамене соответствует сразу блок символов исходного сообщения (| $\mathbf{M}_i$ | = 1 для блока символов); - **омофонические шифры** (однозвучные, многозначной замены). Количество шифрозамен для отдельных символов исходного алфавита больше 1 (| $\mathbf{M}_i$ | ≥ 1 для одного символа); - **полиалфавитные шифры** (многоалфавитные). Состоит из нескольких шифров однозначной замены. Выбор варианта алфавита для зашифрования одного символа зависит от особенностей метода шифрования (| $\mathbf{M}_i$ | > 1 для одного символа). Для записи исходных и зашифрованных сообщений используются строго определенные алфавиты. Под **алфавитом** в данном случае понимается набор символов, служащий для записи сообщений. Алфавиты для записи исходных и зашифрованных сообщений могут отличаться. Символы обоих алфавитов могут быть представлены буквами, их сочетаниями, числами, рисунками и т.п. В качестве

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		примера можно привести пляшущих человечков из рассказа А. Конан Дойла () и рукопись рунического письма () из романа Ж. Верна «Путешествие к центру Земли». **2.2. Шифры однозначной замены.** Максимальное количество ключей для любого шифра этого вида не превышает **n!**, где **n** – количество символов в алфавите. С увеличением числа **n** значение **n!** растет очень быстро (1! = 1, 5! = 120, 10! = 3628800, 15! = 1307674368000). При больших **n** для приближенного вычисления **n!** можно воспользоваться формулой Стирлинга  (1) **Шифр Цезаря.** Данный шифр был придуман Гаем Юлием Цезарем и использовался им в своей переписке (1 век до н.э.). Применительно к русскому языку суть его состоит в следующем. Выписывается исходный алфавит (**А, Б, ..., Я**), затем под ним выписывается тот же алфавит, но с циклическим сдвигом на 3 буквы влево.  Рис.2. Таблица шифрозамен для шифра Цезаря При зашифровке буква **А** заменяется буквой **Г**, **Б** - на **Д** и т. д. Так, например, исходное сообщение «АБРАМОВ» после шифрования будет выглядеть «ГДУГПСЕ». Получатель сообщения «ГДУГПСЕ» ищет эти буквы в нижней строке и по буквам над ними восстанавливает исходное сообщение «АБРАМОВ».

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		Ключом в шифре Цезаря является величина сдвига нижней строки алфавита. Количество ключей для всех модификаций данного шифра применительно к алфавиту русского языка равно 33. Возможны различные модификации шифра Цезаря, в частности лозунговый шифр. **Лозунговый шифр.** Для данного шифра построение таблицы шифрозамен основано на лозунге (ключе) – легко запоминаемом слове. Вторая строка таблицы шифрозамен заполняется сначала словом-лозунгом (причем повторяющиеся буквы отбрасываются), а затем остальными буквами, не вошедшие в слово-лозунг, в алфавитном порядке. Например, если выбрано слово-лозунг «ДЯДИНА», то таблица имеет следующий вид.  Рис.3. Таблица шифрозамен для лозунгового шифра При шифровании исходного сообщения «АБРАМОВ» по приведенному выше ключу шифрограмма будет выглядеть «ДЯПДКМИ». В качестве лозунга рекомендуется выбирать фразу, в которой содержаться конечные буквы алфавита. В общем случае, количество вариантов нижней строки (применительно к русскому языку) составляет 33! ($\geq 10^{35}$). **Полибианский квадрат.** Шифр изобретен греческим государственным деятелем, полководцем и историком Полибием (III век до н.э.). Применительно к русскому алфавиту суть шифрования заключалась в следующем. В квадрат 6x6 выписываются буквы.

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		 Рис.4. Таблица шифрозамен для полибианского квадрата Шифруемая буква заменяется на координаты квадрата (строка-столбец), в котором она записана. Например, если исходное сообщение «АБРАМОВ», то шифрограмма – «11 12 36 11 32 34 13». В Древней Греции сообщения передавались с помощью оптического телеграфа (с помощью факелов). Для каждой буквы сообщения в начале поднималось количество факелов, соответствующее номеру строки буквы, а затем номеру столбца. **Шифрующая система Трисемуса (Тритемия).** В 1508 г. аббат из Германии Иоганн Трисемус написал печатную работу по криптологии под названием «Полиграфия». В этой книге он впервые систематически описал применение шифрующих таблиц, заполненных алфавитом в случайном порядке. Для получения такого шифра замены обычно использовались таблица для записи букв алфавита и ключевое слово (или фраза). В таблицу сначала вписывалось по строкам ключевое слово, причем повторяющиеся буквы отбрасывались. Затем эта таблица дополнялась не вошедшими в нее буквами алфавита по порядку. На рис.6 изображена таблица с ключевым словом «ДЯДИНА».

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		 Рис.5. Таблица шифрозамен для шифра Трисемуса Каждая буква открытого сообщения заменяется буквой, расположенной под ней в том же столбце. Если буква находится в последней строке таблицы, то для ее шифрования берут самую верхнюю букву столбца. Например, исходное сообщение «АБРАМОВ», зашифрованное – «ИЙЪИХШК». **2.3. Полиграммные шифры.** **Полиграммные шифры замены** - шифры, которые шифруют сразу группы (блоки) символов. **Шифр Playfair (англ. «Честная игра»).** Был изобретен в 1854 г. Чарльзом Уитстоном, но назван именем лорда Лайона Плейфера, который внедрил данный шифр в государственные службы Великобритании. Он использовался англичанами в Первой мировой войне. Шифр предусматривает шифрование пар символов (биграмм). Таким образом, этот шифр более устойчив к взлому по сравнению с шифром простой замены, так как затрудняется частотный анализ. Он может быть проведен, но не для 26 возможных символов (латинский алфавит), а для 26 x 26 = 676 возможных биграмм. Анализ частоты биграмм возможен, но является значительно более трудным и требует намного большего объема зашифрованного текста. Для шифрования сообщения необходимо разбить его на биграммы (группы из двух символов), при

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		этом, если в биграмме встретятся два одинаковых символа, то между ними добавляется заранее оговоренный вспомогательный символ (в оригинале – **X**, для русского алфавита - **Я**). Например, «зашифрованное сообщение» становится «за ши фр ов ан но ес о**Я** об ще ни е**Я**». Для формирования ключевой таблицы выбирается лозунг и далее она заполняется по правилам шифрующей системы Трисемуса. Например, лозунг «ДЯДИНА»  Рис.6. Ключевая таблица для шифра Playfair Затем, руководствуясь следующими правилами, выполняется зашифровывание пар символов исходного текста: 1. Если символы биграммы исходного текста встречаются в одной строке, то эти символы замещаются на символы, расположенные в ближайших столбцах справа от соответствующих символов. Если символ является последним в строке, то он заменяется на первый символ этой же строки. 2. Если символы биграммы исходного текста встречаются в одном столбце, то они преобразуются в символы того же столбца, находящимися непосредственно под ними. Если символ является нижним в столбце, то он заменяется на первый символ этого же столбца. 3. Если символы биграммы исходного текста находятся в разных столбцах и разных строках, то они

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		заменяются на символы, находящиеся в тех же строках, но соответствующие другим углам прямоугольника. Пример шифрования. - биграмма «за» формирует прямоугольник – заменяется на «жб»; - биграмма «ши» находятся в одном столбце – заменяется на «юе»; - биграмма «фр» находятся в одной строке – заменяется на «хс»; - биграмма «ов» формирует прямоугольник – заменяется на «йж»; - биграмма «ан» находятся в одной строке – заменяется на «ба»; - биграмма «но» формирует прямоугольник – заменяется на «ам»; - биграмма «ес» формирует прямоугольник – заменяется на «гт»; - биграмма «оя» формирует прямоугольник – заменяется на «ка»; - биграмма «об» формирует прямоугольник – заменяется на «па»; - биграмма «ще» формирует прямоугольник – заменяется на «шё»; - биграмма «ни» формирует прямоугольник – заменяется на «ан»; - биграмма «ея» формирует прямоугольник – заменяется на «ги». Шифрограмма – «жб юе хс йж ба ам гт ка па шё ан ги». Для расшифровки необходимо использовать инверсию этих правил, откидывая символы **Я** (или **Х**),

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		если они не несут смысла в исходном сообщении. **3. Практическая часть** Зашифруйте свою фамилию с помощью следующих шифров: - шифра Цезаря; - лозунгового шифра; - полибианского квадрата; - шифрующей системы Трисемуса; - шифра Playfair; При оформлении отчета необходимо привести исходное сообщение (фамилию), таблицу шифрозамен, ключ (если таблица шифрозамен не является ключом) и зашифрованное сообщение.
ОПК-2 владением базовыми знаниями в области информационных технологий		
Знать	Базовые понятия в области ИТ. Сущность и общую характеристику информационных процессов информационного общества в аспекте информационной безопасности. Современное состояние уровня и направлений	1. Наиболее характерные будущие черты информационного образа жизни. 2. Сущность проблемы информационного неравенства. 3. Информационная свобода личности и средства массовой информации. 4. Информационная свобода в информационном обществе. 5. Основные предпосылки для информационных преступлений. 6. Основные виды преступлений в интеллектуальной сфере. 7. Основные виды компьютерных преступлений. 8. Как определены понятия банковская, коммерческая и служебная тайна в Гражданском кодексе Российской Федерации. 9. Как отражены вопросы правового режима информации с ограниченным доступом в зако-

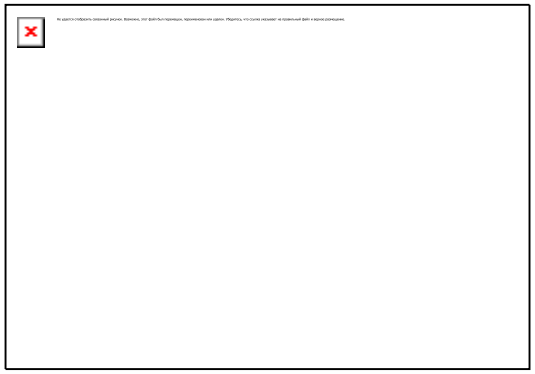
Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
	развития программных средств в области обеспечения информационной безопасности и защиты информации.	нах о государственной и коммерческой тайнах, в гражданском кодексе РФ в статье 139 «Служебная и коммерческая тайна». 10. Какие сведения **не** относятся к коммерческой тайне? 11. Как определяется понятие и содержание конфиденциальной информации в Указе Президента РФ «Об утверждении перечня сведений конфиденциального характера». 12. Структура и содержание документа «Политика информационной безопасности организации».
Уметь:	Самостоятельно ориентироваться в современных информационных технологиях профессиональной области. Применять с профессиональной деятельности современные средства ИКТ. Обеспечивать защиту информации во время работы с современными средствами ИКТ.	1 Мандатная политика доступа: а) Определяет права доступа идентифицированных субъектов к объектам на основе заданных внешних правил (матрицы доступа). **б) Определяет права доступа субъектов к объектам или разрешает информационные потоки между объектами на основе изменяемых меток прав доступа субъектов и меток конфиденциальности объектов.** в) Является алгоритмом формирования матрицы доступа. г) Содержит инструкцию для системного администратора по предоставлению прав доступа различным пользователям. 2 Компьютерным вирусом называется: **а) Программа, способная внедряться в другие программы, с возможностью самовоспроизводства.** б) Вид бактерий, разрушающий микросхемы. в) Процесс разрушения информации на неисправном жёстком диске. 3 Что здесь не относится к антивирусным программам: а) Dr. Web б) AVP **в) Norton DiskDoktor**

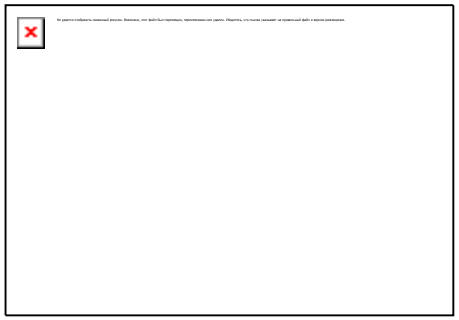
Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		4 В системе стандартов «Общие критерии» требования не объединяются в: а) Классы б) Семейства **в) Группы** 5 В документах Гостехкомиссии под показателями защищённости понимается: а) Экспертная оценка системы защиты информации по пятибалльной шкале. **б) Перечень группы требований, необходимых для выполнения в информационных системах заданного класса защищённости.** в) Временные характеристики реакции системы безопасности на обнаружение несанкционированного доступа.
Владеть:	Навыками использования современных ИКТ. Принципами работы служб Интернет для сбора профессиональной информации. Базовыми приемами размещения информации в открытом доступе с помощью современных ИКТ.	***Контрольная работа*** **Защита информации с помощью криптографии** **1. Цель работы** Целью работы является исследование защиты информации с применением простейших принципов криптографии. **2. Теоретическая часть** **2.1 Шифры замены** Сущность шифрования методом замены заключается в следующем [2]. Пусть шифруются сообщения

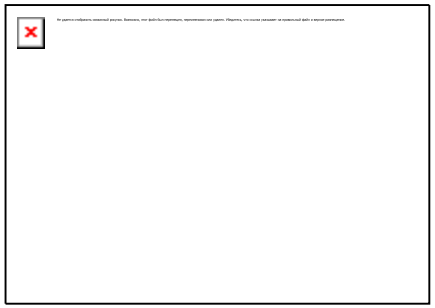
Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		на русском языке и замене подлежит каждая буква этих сообщений. Тогда, букве **А** исходного алфавита сопоставляется некоторое множество символов (шифрозамен) $\mathbf{M_А}$, **Б –** $\mathbf{M_Б}$, **…, Я –** $\mathbf{M_Я}$. Шифрозамены выбираются таким образом, чтобы любые два множества ($\mathbf{M_i}$ и $\mathbf{M_J}$, $\mathbf{i \neq j}$) не содержали одинаковых элементов ($\mathbf{M_i \cap M_J = \varnothing}$). Таблица, приведенная на рис.1, является ключом шифра замены. Зная ее, можно осуществить как шифрование, так и расшифрование.  Рис.1. Таблица шифрозамен При шифровании каждая буква **А** открытого сообщения заменяется любым символом из множества $\mathbf{M_А}$. Если в сообщении содержится несколько букв **А**, то каждая из них заменяется на любой символ из $\mathbf{M_А}$. За счет этого с помощью одного ключа можно получить различные варианты шифрограммы для одного и того же открытого сообщения. Так как множества $\mathbf{M_А}$, $\mathbf{M_Б}$, **...,** $\mathbf{M_Я}$ попарно не пересекаются, то по каждому символу шифрограммы можно однозначно определить, какому множеству он принадлежит, и, следовательно, какую букву открытого сообщения он заменяет. Поэтому расшифрование возможно и открытое сообщение определяется единственным образом. Метод замены часто реализуется многими пользователями при работе на компьютере. Если по забывчивости не переключить на клавиатуре набор символов с латиницы на кириллицу, то вместо букв русского алфавита при вводе текста будут печататься буквы латинского алфавита («шифрозамены»).

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		Шифры замены можно разделить на следующие **подклассы**: - **шифры однозначной замены** (моноалфавитные, простые подстановочные). Количество шифрозамен для каждого символа исходного алфавита равно 1 (| $\mathbf{M}_i$ | = 1 для одного символа); - **полиграммные шифры**. Аналогичен предыдущему за исключением того, что шифрозамене соответствует сразу блок символов исходного сообщения (| $\mathbf{M}_i$ | = 1 для блока символов); - **омофонические шифры** (однозвучные, многозначной замены). Количество шифрозамен для отдельных символов исходного алфавита больше 1 (| $\mathbf{M}_i$ | ≥ 1 для одного символа); - **полиалфавитные шифры** (многоалфавитные). Состоит из нескольких шифров однозначной замены. Выбор варианта алфавита для зашифрования одного символа зависит от особенностей метода шифрования (| $\mathbf{M}_i$ | > 1 для одного символа). Для записи исходных и зашифрованных сообщений используются строго определенные алфавиты. Под **алфавитом** в данном случае понимается набор символов, служащий для записи сообщений. Алфавиты для записи исходных и зашифрованных сообщений могут отличаться. Символы обоих алфавитов могут быть представлены буквами, их сочетаниями, числами, рисунками и т.п. В качестве примера можно привести пляшущих человечков из рассказа А. Конан Дойла () и рукопись рунического письма () из романа Ж. Верна «Путешествие к центру Земли». **2.2. Шифры однозначной замены.** Максимальное количество ключей для любого шифра этого вида не превышает **n!**, где **n** – количество символов в алфавите. С увеличением числа **n** значение **n!** растет очень быстро (1! = 1, 5! = 120, 10! = 3628800, 15! = 1307674368000). При больших **n** для приближенного вычисления **n!** можно вос-

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		пользоваться формулой Стирлинга  (1) **Шифр Цезаря.** Данный шифр был придуман Гаем Юлием Цезарем и использовался им в своей переписке (1 век до н.э.). Применительно к русскому языку суть его состоит в следующем. Выписывается исходный алфавит (**А, Б, ..., Я**), затем под ним выписывается тот же алфавит, но с циклическим сдвигом на 3 буквы влево.  Рис.2. Таблица шифрозамен для шифра Цезаря При зашифровке буква **А** заменяется буквой **Г**, **Б** - на **Д** и т. д. Так, например, исходное сообщение «АБРАМОВ» после шифрования будет выглядеть «ГДУГПСЕ». Получатель сообщения «ГДУГПСЕ» ищет эти буквы в нижней строке и по буквам над ними восстанавливает исходное сообщение «АБРАМОВ». Ключом в шифре Цезаря является величина сдвига нижней строки алфавита. Количество ключей для всех модификаций данного шифра применительно к алфавиту русского языка равно 33. Возможны различные модификации шифра Цезаря, в частности лозунговый шифр. **Лозунговый шифр.** Для данного шифра построение таблицы шифрозамен основано на лозунге (ключе) – легко запоминаемом слове. Вторая строка таблицы шифрозамен заполняется сначала словом-лозунгом (причем повторяющиеся буквы отбрасываются), а затем остальными буквами, не вошедшие в слово-лозунг, в алфавитном порядке. Например, если выбрано слово-лозунг «ДЯДИ-

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		НА», то таблица имеет следующий вид.  Рис.3. Таблица шифрозамен для лозунгового шифра При шифровании исходного сообщения «АБРАМОВ» по приведенному выше ключу шифрограмма будет выглядеть «ДЯПДКМИ». В качестве лозунга рекомендуется выбирать фразу, в которой содержаться конечные буквы алфавита. В общем случае, количество вариантов нижней строки (применительно к русскому языку) составляет 33! ($\geq 10^{35}$). **Полибианский квадрат.** Шифр изобретен греческим государственным деятелем, полководцем и историком Полибием (III век до н.э.). Применительно к русскому алфавиту суть шифрования заключалась в следующем. В квадрат 6x6 выписываются буквы.  Рис.4. Таблица шифрозамен для полибианского квадрата

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		Шифруемая буква заменяется на координаты квадрата (строка-столбец), в котором она записана. Например, если исходное сообщение «АБРАМОВ», то шифрограмма – «11 12 36 11 32 34 13». В Древней Греции сообщения передавались с помощью оптического телеграфа (с помощью факелов). Для каждой буквы сообщения в начале поднималось количество факелов, соответствующее номеру строки буквы, а затем номеру столбца. **Шифрующая система Трисемуса (Тритемия).** В 1508 г. аббат из Германии Иоганн Трисемус написал печатную работу по криптологии под названием «Полиграфия». В этой книге он впервые систематически описал применение шифрующих таблиц, заполненных алфавитом в случайном порядке. Для получения такого шифра замены обычно использовались таблица для записи букв алфавита и ключевое слово (или фраза). В таблицу сначала вписывалось по строкам ключевое слово, причем повторяющиеся буквы отбрасывались. Затем эта таблица дополнялась не вошедшими в нее буквами алфавита по порядку. На рис.6 изображена таблица с ключевым словом «ДЯДИНА».  Рис.5. Таблица шифрозамен для шифра Трисемуса Каждая буква открытого сообщения заменяется буквой, расположенной под ней в том же столбце. Если буква находится в последней строке таблицы, то для ее шифрования берут самую верхнюю букву столбца. Например, исходное сообщение «АБРАМОВ», зашифрованное – «ИЙЪИХШК».

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		2.3. Полиграммные шифры. **Полиграммные шифры замены** - шифры, которые шифруют сразу группы (блоки) символов. **Шифр Playfair (англ. «Честная игра»).** Был изобретен в 1854 г. Чарльзом Уитстоном, но назван именем лорда Лайона Плейфера, который внедрил данный шифр в государственные службы Великобритании. Он использовался англичанами в Первой мировой войне. Шифр предусматривает шифрование пар символов (биграмм). Таким образом, этот шифр более устойчив к взлому по сравнению с шифром простой замены, так как затрудняется частотный анализ. Он может быть проведен, но не для 26 возможных символов (латинский алфавит), а для 26 x 26 = 676 возможных биграмм. Анализ частоты биграмм возможен, но является значительно более трудным и требует намного большего объема зашифрованного текста. Для шифрования сообщения необходимо разбить его на биграммы (группы из двух символов), при этом, если в биграмме встретятся два одинаковых символа, то между ними добавляется заранее оговоренный вспомогательный символ (в оригинале – **X**, для русского алфавита - **Я**). Например, «зашифрованное сообщение» становится «за ши фр ов ан но ес о**Я** об ще ни е**Я**». Для формирования ключевой таблицы выбирается лозунг и далее она заполняется по правилам шифрующей системы Трисемуса. Например, лозунг «ДЯДИНА» 

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		Рис.6. Ключевая таблица для шифра Playfair Затем, руководствуясь следующими правилами, выполняется зашифровывание пар символов исходного текста: 1. Если символы биграммы исходного текста встречаются в одной строке, то эти символы замещаются на символы, расположенные в ближайших столбцах справа от соответствующих символов. Если символ является последним в строке, то он заменяется на первый символ этой же строки. 2. Если символы биграммы исходного текста встречаются в одном столбце, то они преобразуются в символы того же столбца, находящимися непосредственно под ними. Если символ является нижним в столбце, то он заменяется на первый символ этого же столбца. 3. Если символы биграммы исходного текста находятся в разных столбцах и разных строках, то они заменяются на символы, находящиеся в тех же строках, но соответствующие другим углам прямоугольника. Пример шифрования. - биграмма «за» формирует прямоугольник – заменяется на «жб»; - биграмма «ши» находятся в одном столбце – заменяется на «юе»; - биграмма «фр» находятся в одной строке – заменяется на «хс»; - биграмма «ов» формирует прямоугольник – заменяется на «йж»; - биграмма «ан» находятся в одной строке – заменяется на «ба»; - биграмма «но» формирует прямоугольник – заменяется на «ам»;

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		- биграмма «ес» формирует прямоугольник – заменяется на «гт»; - биграмма «оя» формирует прямоугольник – заменяется на «ка»; - биграмма «об» формирует прямоугольник – заменяется на «па»; - биграмма «ще» формирует прямоугольник – заменяется на «шё»; - биграмма «ни» формирует прямоугольник – заменяется на «ан»; - биграмма «ея» формирует прямоугольник – заменяется на «ги». Шифрограмма – «жб юе хс йж ба ам гт ка па шё ан ги». Для расшифровки необходимо использовать инверсию этих правил, откидывая символы **Я** (или **Х**), если они не несут смысла в исходном сообщении. **3. Практическая часть** Зашифруйте свою фамилию с помощью следующих шифров: - шифра Цезаря; - лозунгового шифра; - полибианского квадрата; - шифрующей системы Трисемуса; - шифра Playfair;

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		При оформлении отчета необходимо привести исходное сообщение (фамилию), таблицу шифрозамен, ключ (если таблица шифрозамен не является ключом) и зашифрованное сообщение.
ОПК-4 владением навыками использования компьютерной техники и информационных технологий в поиске источников и литературы, использовании правовых баз данных, составлении библиографических и архивных обзоров		
Знать	Основные понятия и определения в области обеспечения информационной безопасности и защиты информации. Классификации вредоносных программ Способы защиты информации в автоматизированных системах обработки данных, глобальных и локальных сетях, защиты от вредоносных программ	1. Служба информационной безопасности организации. Состав, цели и задачи службы информационной безопасности организации. 2. Роль стандартов и требований по информационной безопасности предприятия в формировании «Политики информационной безопасности организации». 3. Принципы распределения полномочий. 4. Процедуры и методы информационной безопасности организации как составляющие «Политики информационной безопасности организации». 5. Профили защиты. 6. Обязанности сотрудников по обеспечению информационной безопасности. 7. Порядок установления режима конфиденциальности информации. Перечень сведений, относимых к конфиденциальной информации и не подлежащих засекречиванию. 8. Требования, предъявляемые к претендентам на работу с конфиденциальной информацией и к претендентам на должность службу информационной безопасности. 9. Порядок обеспечения сохранности конфиденциальной информации при постоянном или временном прекращении пользователем доступа к конфиденциальному информационному ресурсу. 10. Организационные меры по обеспечению и поддержанию информационной безопасности в период чрезвычайных ситуаций. 11. Виды информации организации, подлежащие защите. 12. Регламентация действий всех категорий сотрудников, допущенных к работе с информационными системами. 13. Система организационно-распорядительных документов учреждения по вопросам обеспечения информационной безопасности.

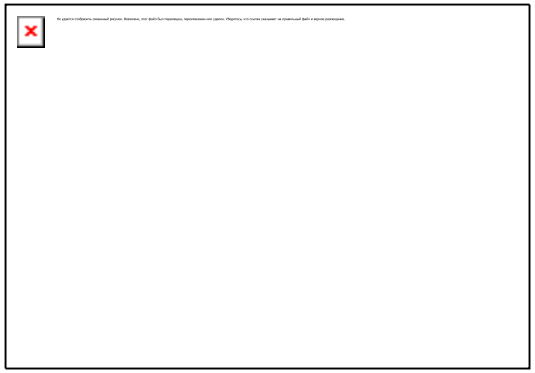
Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
Уметь:	Сохранять информацию от несанкционированного доступа. Настраивать и использовать специализированное антивирусное ПО. Использовать методы и средства защиты информации.	1 Качество системы информационной безопасности может быть оценено: а) Запуском специальной тестовой программы. **б) На основе экспертного анализа различных показателей эффективности.** в) Количеством реализованных защитных функций, декларированных в документации. 2 Какое утверждение верно: а) Последние версии антивирусных программ и регулярное обновление ОС гарантируют защиту от вирусов. **б) ОС с грамотно реализованной системой защиты от несанкционированного доступа лучше защищена от вирусных атак.** в) Защиту от вирусов гарантирует использование только лицензионного программного обеспечения. 3 Брандмауэр это: а) Источник бесперебойного питания. **б) Межсетевой фильтр.** в) Программа просмотра Web-страниц. 4 Цифровая подпись это: а) Ключевое слово или набор цифр в конце электронного документа, известное только отправителю и получателю. б) Цифровое представление графического изображения персональной подписи человека. **в) Результат применения специальной функции к содержимому документа с ключом, известным только отправителю, и который можно проверить с помощью ключа, известного всем получателям.** 5 Виртуальный защищённый канал строится: **а) Путём шифрации информации, проходящей через открытые**

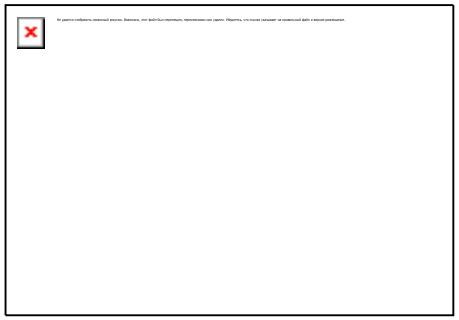
Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		глобальные сети. б) Для передачи видео и аудио информации в привилегированном, защищённом от задержек и прерываний режиме. в) Для имитации использования системы защиты информации с целью ввести в заблуждение возможного злоумышленника.
Владеть:	Профессиональным языком предметной области знания. Навыками защиты и борьбы с вредоносными программами. Навыками применения программных средств защиты информации в компьютерных сетях.	***Контрольная работа*** **Защита информации с помощью криптографии** **1. Цель работы** Целью работы является исследование защиты информации с применением простейших принципов криптографии. **2. Теоретическая часть** **2.1 Шифры замены** Сущность шифрования методом замены заключается в следующем [2]. Пусть шифруются сообщения на русском языке и замене подлежит каждая буква этих сообщений. Тогда, букве **А** исходного алфавита сопоставляется некоторое множество символов (шифрозамен) $\mathbf{M_А}$**, Б –** $\mathbf{M_Б}$**, …, Я –** $\mathbf{M_Я}$. Шифрозамены выбираются таким образом, чтобы любые два множества ($\mathbf{M_i}$ и $\mathbf{M_J}$, $\mathbf{i \neq j}$) не содержали одинаковых элементов ($\mathbf{M_i \cap M_J = \varnothing}$). Таблица, приведенная на рис.1, является ключом шифра замены. Зная ее, можно осуществить как шифрование, так и расшифрование.

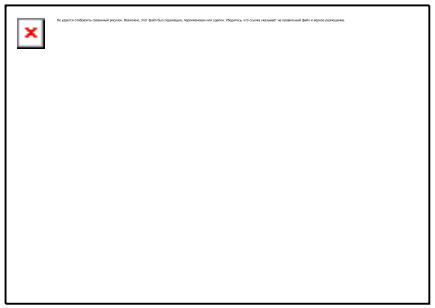
Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		 Рис.1. Таблица шифрозамен При шифровании каждая буква **А** открытого сообщения заменяется любым символом из множества $\mathbf{М_А}$. Если в сообщении содержится несколько букв **А**, то каждая из них заменяется на любой символ из $\mathbf{М_А}$. За счет этого с помощью одного ключа можно получить различные варианты шифрограммы для одного и того же открытого сообщения. Так как множества $\mathbf{М_А, М_Б, ..., М_Я}$ попарно не пересекаются, то по каждому символу шифрограммы можно однозначно определить, какому множеству он принадлежит, и, следовательно, какую букву открытого сообщения он заменяет. Поэтому расшифрование возможно и открытое сообщение определяется единственным образом. Метод замены часто реализуется многими пользователями при работе на компьютере. Если по забывчивости не переключить на клавиатуре набор символов с латиницы на кириллицу, то вместо букв русского алфавита при вводе текста будут печататься буквы латинского алфавита («шифрозамены»). Шифры замены можно разделить на следующие **подклассы**: - **шифры однозначной замены** (моноалфавитные, простые подстановочные). Количество шифрозамен для каждого символа исходного алфавита равно 1 ($\mid \mathbf{М_i} \mid = 1$ для одного символа); - **полиграммные шифры**. Аналогичен предыдущему за исключением того, что шифрозамене соответствует сразу блок символов исходного сообщения ($\mid \mathbf{М_i} \mid = 1$ для блока символов);

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		- **омофонические шифры** (однозвучные, многозначной замены). Количество шифрозамен для отдельных символов исходного алфавита больше 1 ($\| \mathbf{M}_i \| \geq 1$ для одного символа); - **полиалфавитные шифры** (многоалфавитные). Состоит из нескольких шифров однозначной замены. Выбор варианта алфавита для зашифрования одного символа зависит от особенностей метода шифрования ($\| \mathbf{M}_i \| > 1$ для одного символа). Для записи исходных и зашифрованных сообщений используются строго определенные алфавиты. Под **алфавитом** в данном случае понимается набор символов, служащий для записи сообщений. Алфавиты для записи исходных и зашифрованных сообщений могут отличаться. Символы обоих алфавитов могут быть представлены буквами, их сочетаниями, числами, рисунками и т.п. В качестве примера можно привести пляшущих человечков из рассказа А. Конан Дойла () и рукопись рунического письма () из романа Ж. Верна «Путешествие к центру Земли». **2.2. Шифры однозначной замены.** Максимальное количество ключей для любого шифра этого вида не превышает **n!**, где **n** – количество символов в алфавите. С увеличением числа **n** значение **n!** растет очень быстро (1! = 1, 5! = 120, 10! = 3628800, 15! = 1307674368000). При больших **n** для приближенного вычисления **n!** можно воспользоваться формулой Стирлинга  (1) **Шифр Цезаря.** Данный шифр был придуман Гаем Юлием Цезарем и использовался им в своей переписке (1 век до н.э.). Применительно к русскому языку суть его состоит в следующем. Выписывает-

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		ся исходный алфавит (**А, Б, ..., Я**), затем под ним выписывается тот же алфавит, но с циклическим сдвигом на 3 буквы влево.  Рис.2. Таблица шифрозамен для шифра Цезаря При зашифровке буква **А** заменяется буквой **Г**, **Б** - на **Д** и т. д. Так, например, исходное сообщение «АБРАМОВ» после шифрования будет выглядеть «ГДУГПСЕ». Получатель сообщения «ГДУГПСЕ» ищет эти буквы в нижней строке и по буквам над ними восстанавливает исходное сообщение «АБРАМОВ». Ключом в шифре Цезаря является величина сдвига нижней строки алфавита. Количество ключей для всех модификаций данного шифра применительно к алфавиту русского языка равно 33. Возможны различные модификации шифра Цезаря, в частности лозунговый шифр. **Лозунговый шифр.** Для данного шифра построение таблицы шифрозамен основано на лозунге (ключе) – легко запоминаемом слове. Вторая строка таблицы шифрозамен заполняется сначала словом-лозунгом (причем повторяющиеся буквы отбрасываются), а затем остальными буквами, не вошедшие в слово-лозунг, в алфавитном порядке. Например, если выбрано слово-лозунг «ДЯДИНА», то таблица имеет следующий вид.  Рис.3. Таблица шифрозамен для лозунгового шифра При шифровании исходного сообщения «АБРАМОВ» по приведенному выше ключу шифрограмма

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		будет выглядеть «ДЯПДКМИ». В качестве лозунга рекомендуется выбирать фразу, в которой содержаться конечные буквы алфавита. В общем случае, количество вариантов нижней строки (применительно к русскому языку) составляет 33! ($\geq 10^{35}$). **Полибианский квадрат.** Шифр изобретен греческим государственным деятелем, полководцем и историком Полибием (III век до н.э.). Применительно к русскому алфавиту суть шифрования заключалась в следующем. В квадрат 6х6 выписываются буквы.  Рис.4. Таблица шифрозамен для полибианского квадрата Шифруемая буква заменяется на координаты квадрата (строка-столбец), в котором она записана. Например, если исходное сообщение «АБРАМОВ», то шифрограмма – «11 12 36 11 32 34 13». В Древней Греции сообщения передавались с помощью оптического телеграфа (с помощью факелов). Для каждой буквы сообщения в начале поднималось количество факелов, соответствующее номеру строки буквы, а затем номеру столбца. **Шифрующая система Трисемуса (Тритемия).** В 1508 г. аббат из Германии Иоганн Трисемус напи-

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		сал печатную работу по криптологии под названием «Полиграфия». В этой книге он впервые систематически описал применение шифрующих таблиц, заполненных алфавитом в случайном порядке. Для получения такого шифра замены обычно использовались таблица для записи букв алфавита и ключевое слово (или фраза). В таблицу сначала вписывалось по строкам ключевое слово, причем повторяющиеся буквы отбрасывались. Затем эта таблица дополнялась не вошедшими в нее буквами алфавита по порядку. На рис.6 изображена таблица с ключевым словом «ДЯДИНА».  Рис.5. Таблица шифрозамен для шифра Трисемуса Каждая буква открытого сообщения заменяется буквой, расположенной под ней в том же столбце. Если буква находится в последней строке таблицы, то для ее шифрования берут самую верхнюю букву столбца. Например, исходное сообщение «АБРАМОВ», зашифрованное – «ИЙЪИХШК». **2.3. Полиграммные шифры.** **Полиграммные шифры замены** - шифры, которые шифруют сразу группы (блоки) символов. **Шифр Playfair (англ. «Честная игра»).** Был изобретен в 1854 г. Чарльзом Уитстоном, но назван именем лорда Лайона Плейфера, который внедрил данный шифр в государственные службы Великобритании. Он использовался англичанами в Первой мировой войне. Шифр предусматривает шиф-

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		рование пар символов (биграмм). Таким образом, этот шифр более устойчив к взлому по сравнению с шифром простой замены, так как затрудняется частотный анализ. Он может быть проведен, но не для 26 возможных символов (латинский алфавит), а для 26 x 26 = 676 возможных биграмм. Анализ частоты биграмм возможен, но является значительно более трудным и требует намного большего объема зашифрованного текста. Для шифрования сообщения необходимо разбить его на биграммы (группы из двух символов), при этом, если в биграмме встретятся два одинаковых символа, то между ними добавляется заранее оговоренный вспомогательный символ (в оригинале – **X**, для русского алфавита - **Я**). Например, «зашифрованное сообщение» становится «за ши фр ов ан но ес о**Я** об ще ни е**Я**». Для формирования ключевой таблицы выбирается лозунг и далее она заполняется по правилам шифрующей системы Трисемуса. Например, лозунг «ДЯДИНА»  Рис.6. Ключевая таблица для шифра Playfair Затем, руководствуясь следующими правилами, выполняется зашифровывание пар символов исходного текста: 1. Если символы биграммы исходного текста встречаются в одной строке, то эти символы замещаются на символы, расположенные в ближайших столбцах справа от соответствующих символов. Ес-

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		ли символ является последним в строке, то он заменяется на первый символ этой же строки. 2. Если символы биграммы исходного текста встречаются в одном столбце, то они преобразуются в символы того же столбца, находящимися непосредственно под ними. Если символ является нижним в столбце, то он заменяется на первый символ этого же столбца. 3. Если символы биграммы исходного текста находятся в разных столбцах и разных строках, то они заменяются на символы, находящиеся в тех же строках, но соответствующие другим углам прямоугольника. Пример шифрования. - биграмма «за» формирует прямоугольник – заменяется на «жб»; - биграмма «ши» находятся в одном столбце – заменяется на «юе»; - биграмма «фр» находятся в одной строке – заменяется на «хс»; - биграмма «ов» формирует прямоугольник – заменяется на «йж»; - биграмма «ан» находятся в одной строке – заменяется на «ба»; - биграмма «но» формирует прямоугольник – заменяется на «ам»; - биграмма «ес» формирует прямоугольник – заменяется на «гт»; - биграмма «оя» формирует прямоугольник – заменяется на «ка»; - биграмма «об» формирует прямоугольник – заменяется на «па»; - биграмма «ще» формирует прямоугольник – заменяется на «шё»;

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		- биграмма «ни» формирует прямоугольник – заменяется на «ан»; - биграмма «ея» формирует прямоугольник – заменяется на «ги». Шифрограмма – «жб юе хс йж ба ам гт ка па шё ан ги». Для расшифровки необходимо использовать инверсию этих правил, откидывая символы **Я** (или **Х**), если они не несут смысла в исходном сообщении. **3. Практическая часть** Зашифруйте свою фамилию с помощью следующих шифров: - шифра Цезаря; - лозунгового шифра; - полибианского квадрата; - шифрующей системы Трисемуса; - шифра Playfair; При оформлении отчета необходимо привести исходное сообщение (фамилию), таблицу шифрозамен, ключ (если таблица шифрозамен не является ключом) и зашифрованное сообщение.
ОПК-6 способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности		
Знать	Основные положения государственной поли-	1. Политика безопасности учреждения. 2. Программа безопасности учреждения.

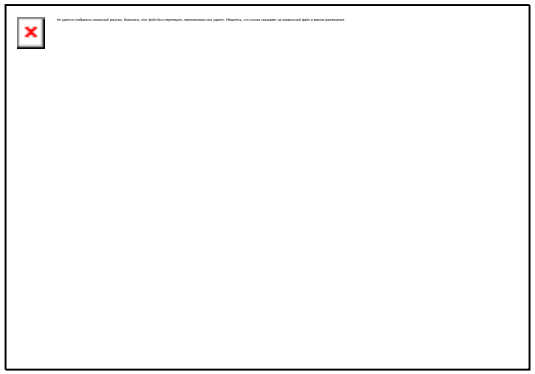
Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
	тики обеспечения информационной безопасности и защиты информации. Нормы информационной этики и права. Принципы работы с информацией на различных ресурсах, с учетом требований информационной безопасности.	3. Способы распространения программного обеспечения. 4. Базовые методы нейтрализации систем защиты от несанкционированного копирования. 5. Техническая защита от несанкционированного копирования. 6. Требования пожарной безопасности к объектам информатизации. 7. Способы обеспечения безопасной работы в Интернет. 8. Администраторы штатных и дополнительных средств защиты. 9. Обнаружение сетевой атаки. 10. Принципы функционирования брандмауэров. 11. Способы защиты файлов от постороннего доступа.
Уметь:	Применять на практике соответствующие требования и нормы обеспечения информационной безопасности и защиты информации. Соблюдать права интеллектуальной собственности на информацию. Оформлять результаты исследований и вести текущую работу с учетом требований и норм обеспечения информационной безопасности и защиты информации.	1 Программная система защиты информации отвечает за: *а) Сохранность всей введённой в информационную систему информации.* **б) Реализацию заданной политики безопасности.** в) Корректное поведение пользователей. 2 Аутентификация это: **а) Подтверждение заявленного идентификатора.** б) Процесс ввода текста без отображения на экране. в) Ввод сведений личного характера. 3 Политика безопасности это: **а) Правила определения разрешённых и запрещённых операций в** информационной системе. б) Правила поведения пользователей. в) Инструкция действий администратора по обеспечению информационной безопасности. 4 Монитор безопасности это:

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		а) Личный терминал системного администратора. **б) Совокупность резидентных программ, реализующих политику** безопасности. в) Программа контроля данных аудита. 5 Дискреционная политика доступа: **а) Определяет права доступа идентифицированных субъектов к объектам на основе заданных внешних правил (матрицы доступа).** б) Определяет права доступа субъектов к объектам или разрешает информационные потоки между объектами на основе изменяемых меток прав доступа или конфиденциальности. в) Является алгоритмом формирования матрицы доступа. г) Содержит инструкцию для системного администратора по предоставлению прав доступа различным пользователям.
Владеть:	Основными методами исследования в области информационной безопасности и практическими умениями и навыками их использования. Общими принципами соблюдения требований информационной этики и права. Способами совершенствования профессиональных знаний и умений путем использова-	***Контрольная работа*** **Защита информации с помощью криптографии** **1. Цель работы** Целью работы является исследование защиты информации с применением простейших принципов криптографии. **2. Теоретическая часть** **2.1 Шифры замены** Сущность шифрования методом замены заключается в следующем [2]. Пусть шифруются сообщения на русском языке и замене подлежит каждая буква этих сообщений. Тогда, букве **А** исходного алфавита сопоставляется некоторое множество символов (шифрозамен) **$М_А$, Б – $М_Б$, …, Я – $М_Я$**. Шифроза-

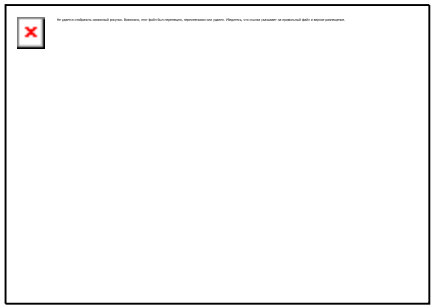
Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
	ния возможностей информационной среды, с учетом требований государственных нормативных актов и информационной этики и права	мены выбираются таким образом, чтобы любые два множества ($\mathbf{M}_i$ и $\mathbf{M}_j$, $\mathbf{i \neq j}$) не содержали одинаковых элементов ($\mathbf{M}_i \cap \mathbf{M}_j = \mathbf{\varnothing}$). Таблица, приведенная на рис.1, является ключом шифра замены. Зная ее, можно осуществить как шифрование, так и расшифрование.  Рис.1. Таблица шифрозамен При шифровании каждая буква **А** открытого сообщения заменяется любым символом из множества $\mathbf{M}_А$. Если в сообщении содержится несколько букв **А**, то каждая из них заменяется на любой символ из $\mathbf{M}_А$. За счет этого с помощью одного ключа можно получить различные варианты шифрограммы для одного и того же открытого сообщения. Так как множества $\mathbf{M}_А$, $\mathbf{M}_Б$, ..., $\mathbf{M}_Я$ попарно не пересекаются, то по каждому символу шифрограммы можно однозначно определить, какому множеству он принадлежит, и, следовательно, какую букву открытого сообщения он заменяет. Поэтому расшифрование возможно и открытое сообщение определяется единственным образом. Метод замены часто реализуется многими пользователями при работе на компьютере. Если по забывчивости не переключить на клавиатуре набор символов с латиницы на кириллицу, то вместо букв русского алфавита при вводе текста будут печататься буквы латинского алфавита («шифрозамены»). Шифры замены можно разделить на следующие **подклассы**: - **шифры однозначной замены** (моноалфавитные, простые подстановочные). Количество шифро-

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		замен для каждого символа исходного алфавита равно 1 (| $\mathbf{M}_i$ | = 1 для одного символа); - **полиграммные шифры**. Аналогичен предыдущему за исключением того, что шифрозамене соответствует сразу блок символов исходного сообщения (| $\mathbf{M}_i$ | = 1 для блока символов); - **омофонические шифры** (однозвучные, многозначной замены). Количество шифрозамен для отдельных символов исходного алфавита больше 1 (| $\mathbf{M}_i$ | ≥ 1 для одного символа); - **полиалфавитные шифры** (многоалфавитные). Состоит из нескольких шифров однозначной замены. Выбор варианта алфавита для зашифрования одного символа зависит от особенностей метода шифрования (| $\mathbf{M}_i$ | > 1 для одного символа). Для записи исходных и зашифрованных сообщений используются строго определенные алфавиты. Под **алфавитом** в данном случае понимается набор символов, служащий для записи сообщений. Алфавиты для записи исходных и зашифрованных сообщений могут отличаться. Символы обоих алфавитов могут быть представлены буквами, их сочетаниями, числами, рисунками и т.п. В качестве примера можно привести пляшущих человечков из рассказа А. Конан Дойла () и рукопись рунического письма () из романа Ж. Верна «Путешествие к центру Земли». **2.2. Шифры однозначной замены.** Максимальное количество ключей для любого шифра этого вида не превышает **n!**, где **n** – количество символов в алфавите. С увеличением числа **n** значение **n!** растет очень быстро (1! = 1, 5! = 120, 10! = 3628800, 15! = 1307674368000). При больших **n** для приближенного вычисления **n!** можно воспользоваться формулой Стирлинга

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		 (1) **Шифр Цезаря.** Данный шифр был придуман Гаем Юлием Цезарем и использовался им в своей переписке (1 век до н.э.). Применительно к русскому языку суть его состоит в следующем. Выписывается исходный алфавит (**А, Б, ..., Я**), затем под ним выписывается тот же алфавит, но с циклическим сдвигом на 3 буквы влево.  Рис.2. Таблица шифрозамен для шифра Цезаря При зашифровке буква **А** заменяется буквой **Г**, **Б** - на **Д** и т. д. Так, например, исходное сообщение «АБРАМОВ» после шифрования будет выглядеть «ГДУГПСЕ». Получатель сообщения «ГДУГПСЕ» ищет эти буквы в нижней строке и по буквам над ними восстанавливает исходное сообщение «АБРАМОВ». Ключом в шифре Цезаря является величина сдвига нижней строки алфавита. Количество ключей для всех модификаций данного шифра применительно к алфавиту русского языка равно 33. Возможны различные модификации шифра Цезаря, в частности лозунговый шифр. **Лозунговый шифр.** Для данного шифра построение таблицы шифрозамен основано на лозунге (ключе) – легко запоминаемом слове. Вторая строка таблицы шифрозамен заполняется сначала словом-лозунгом (причем повторяющиеся буквы отбрасываются), а затем остальными буквами, не вошедшие в слово-лозунг, в алфавитном порядке. Например, если выбрано слово-лозунг «ДЯДИНА», то таблица имеет следующий вид.

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		 Рис.3. Таблица шифрозамен для лозунгового шифра При шифровании исходного сообщения «АБРАМОВ» по приведенному выше ключу шифрограмма будет выглядеть «ДЯПДКМИ». В качестве лозунга рекомендуется выбирать фразу, в которой содержаться конечные буквы алфавита. В общем случае, количество вариантов нижней строки (применительно к русскому языку) составляет 33! ($\geq 10^{35}$). **Полибианский квадрат.** Шифр изобретен греческим государственным деятелем, полководцем и историком Полибием (III век до н.э.). Применительно к русскому алфавиту суть шифрования заключалась в следующем. В квадрат 6х6 выписываются буквы.  Рис.4. Таблица шифрозамен для полибианского квадрата Шифруемая буква заменяется на координаты квадрата (строка-столбец), в котором она записана.

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		Например, если исходное сообщение «АБРАМОВ», то шифрограмма – «11 12 36 11 32 34 13». В Древней Греции сообщения передавались с помощью оптического телеграфа (с помощью факелов). Для каждой буквы сообщения в начале поднималось количество факелов, соответствующее номеру строки буквы, а затем номеру столбца. **Шифрующая система Трисемуса (Тритемия).** В 1508 г. аббат из Германии Иоганн Трисемус написал печатную работу по криптологии под названием «Полиграфия». В этой книге он впервые систематически описал применение шифрующих таблиц, заполненных алфавитом в случайном порядке. Для получения такого шифра замены обычно использовались таблица для записи букв алфавита и ключевое слово (или фраза). В таблицу сначала вписывалось по строкам ключевое слово, причем повторяющиеся буквы отбрасывались. Затем эта таблица дополнялась не вошедшими в нее буквами алфавита по порядку. На рис.6 изображена таблица с ключевым словом «ДЯДИНА».  Рис.5. Таблица шифрозамен для шифра Трисемуса Каждая буква открытого сообщения заменяется буквой, расположенной под ней в том же столбце. Если буква находится в последней строке таблицы, то для ее шифрования берут самую верхнюю букву столбца. Например, исходное сообщение «АБРАМОВ», зашифрованное – «ИЙЪИХШК».

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		2.3. Полиграммные шифры. **Полиграммные шифры замены** - шифры, которые шифруют сразу группы (блоки) символов. **Шифр Playfair (англ. «Честная игра»).** Был изобретен в 1854 г. Чарльзом Уитстоном, но назван именем лорда Лайона Плейфера, который внедрил данный шифр в государственные службы Великобритании. Он использовался англичанами в Первой мировой войне. Шифр предусматривает шифрование пар символов (биграмм). Таким образом, этот шифр более устойчив к взлому по сравнению с шифром простой замены, так как затрудняется частотный анализ. Он может быть проведен, но не для 26 возможных символов (латинский алфавит), а для 26 x 26 = 676 возможных биграмм. Анализ частоты биграмм возможен, но является значительно более трудным и требует намного большего объема зашифрованного текста. Для шифрования сообщения необходимо разбить его на биграммы (группы из двух символов), при этом, если в биграмме встретятся два одинаковых символа, то между ними добавляется заранее оговоренный вспомогательный символ (в оригинале – **X**, для русского алфавита - **Я**). Например, «зашифрованное сообщение» становится «за ши фр ов ан но ес о**Я** об ще ни е**Я**». Для формирования ключевой таблицы выбирается лозунг и далее она заполняется по правилам шифрующей системы Трисемуса. Например, лозунг «ДЯДИНА» 

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		Рис.6. Ключевая таблица для шифра Playfair Затем, руководствуясь следующими правилами, выполняется зашифровывание пар символов исходного текста: 1. Если символы биграммы исходного текста встречаются в одной строке, то эти символы замещаются на символы, расположенные в ближайших столбцах справа от соответствующих символов. Если символ является последним в строке, то он заменяется на первый символ этой же строки. 2. Если символы биграммы исходного текста встречаются в одном столбце, то они преобразуются в символы того же столбца, находящимися непосредственно под ними. Если символ является нижним в столбце, то он заменяется на первый символ этого же столбца. 3. Если символы биграммы исходного текста находятся в разных столбцах и разных строках, то они заменяются на символы, находящиеся в тех же строках, но соответствующие другим углам прямоугольника. Пример шифрования. - биграмма «за» формирует прямоугольник – заменяется на «жб»; - биграмма «ши» находятся в одном столбце – заменяется на «юе»; - биграмма «фр» находятся в одной строке – заменяется на «хс»; - биграмма «ов» формирует прямоугольник – заменяется на «йж»; - биграмма «ан» находятся в одной строке – заменяется на «ба»; - биграмма «но» формирует прямоугольник – заменяется на «ам»;

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		- биграмма «ес» формирует прямоугольник – заменяется на «гт»; - биграмма «оя» формирует прямоугольник – заменяется на «ка»; - биграмма «об» формирует прямоугольник – заменяется на «па»; - биграмма «ще» формирует прямоугольник – заменяется на «шё»; - биграмма «ни» формирует прямоугольник – заменяется на «ан»; - биграмма «ея» формирует прямоугольник – заменяется на «ги». Шифрограмма – «жб юе хс йж ба ам гт ка па шё ан ги». Для расшифровки необходимо использовать инверсию этих правил, откидывая символы **Я** (или **Х**), если они не несут смысла в исходном сообщении. **3. Практическая часть** Зашифруйте свою фамилию с помощью следующих шифров: - шифра Цезаря; - лозунгового шифра; - полибианского квадрата; - шифрующей системы Трисемуса; - шифра Playfair;

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		При оформлении отчета необходимо привести исходное сообщение (фамилию), таблицу шифрозамен, ключ (если таблица шифрозамен не является ключом) и зашифрованное сообщение.
ПК-6 способностью анализировать ситуацию на рынке информационных продуктов и услуг, давать экспертную оценку современным системам электронного документооборота и ведения электронного архива		
Знать	Основные понятия офисных информационных технологий. Особенности обеспечения защиты информации в офисных ИТ. Сферы применения методов обеспечения защиты информации в офисных ИТ.	1. Выбор паролей. Хранение паролей. Передача пароля по сети. 2. Системы отражения атак. 3. Регламентация процесса авторизации 4. Защита от сетевых атак и шпионажа. 5. Способы обеспечения безопасной работы в Интернет. 6. Авторское право 7. Лицензирование и патентование 8. Право распоряжения, право владения, право пользования. 9. Нормативно-правовая основа мер по защите авторских прав 10. Этические нормы при работе с информацией 11. Нетикет 12. Закон «Об информации, информационных технологиях и о защите информации» 13. Закон «О средствах массовой информации» 14. Закон «О рекламе» 15. Закон «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» 16. Закон «Об обеспечении доступа к информации о деятельности судов в российской федерации» 17. Закон «О защите детей от информации, причиняющей вред их здоровью и развитию»
Уметь:	Демонстрировать навыки работы в офисных ИТ.	1 Мандатная политика доступа: а) Определяет права доступа идентифицированных субъектов к объектам на основе заданных внешних правил (матрицы доступа).

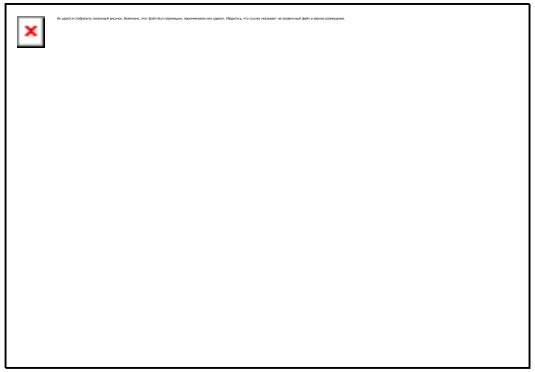
Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
	Характеризовать основные способы защиты информации в офисных ИТ. Применять навыки настройки основных аспектов обеспечения защиты информации штатными средствами офисных ИТ.	**б) Определяет права доступа субъектов к объектам или разрешает информационные потоки между объектами на основе изменяемых меток прав доступа субъектов и меток конфиденциальности объектов.** в) Является алгоритмом формирования матрицы доступа. г) Содержит инструкцию для системного администратора по предоставлению прав доступа различным пользователям. 2 Компьютерным вирусом называется: **а) Программа, способная внедряться в другие программы, с возможностью самовоспроизводства.** б) Вид бактерий, разрушающий микросхемы. в) Процесс разрушения информации на неисправном жёстком диске. 3 В документах Гостехкомиссии под показателями защищённости понимается: а) Экспертная оценка системы защиты информации по пятибалльной шкале. **б) Перечень группы требований, необходимых для выполнения в информационных системах заданного класса защищённости.** в) Временные характеристики реакции системы безопасности на обнаружение несанкционированного доступа. 4 Качество системы информационной безопасности может быть оценено: а) Запуском специальной тестовой программы. **б) На основе экспертного анализа различных показателей эффективности.** в) Количеством реализованных защитных функций, декларированных в документации. 5 Какое утверждение верно: а) Последние версии антивирусных программ и регулярное обновление ОС гарантируют защиту от вирусов.

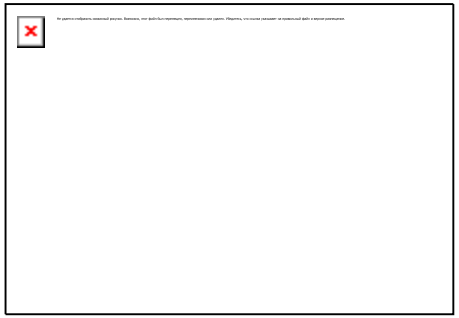
Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		б) ОС с грамотно реализованной системой защиты от несанкционированного доступа лучше защищена от вирусных атак. в) Защиту от вирусов гарантирует использование только лицензионного программного обеспечения.
Владеть:	Навыком объяснения необходимости настройки офисных ИТ с позиции обеспечения информационной безопасности Навыком выделения основных способов защиты информации в офисных ИТ. Навыком настройки защиты информации в офисных ИТ.	***Контрольная работа*** **Защита информации с помощью криптографии** **1. Цель работы** Целью работы является исследование защиты информации с применением простейших принципов криптографии. **2. Теоретическая часть** **2.1 Шифры замены** Сущность шифрования методом замены заключается в следующем [2]. Пусть шифруются сообщения на русском языке и замене подлежит каждая буква этих сообщений. Тогда, букве **А** исходного алфавита сопоставляется некоторое множество символов (шифрозамен) $\mathbf{М_А}$, **Б –** $\mathbf{М_Б}$, **…, Я –** $\mathbf{М_Я}$. Шифрозамены выбираются таким образом, чтобы любые два множества ($\mathbf{М_i}$ и $\mathbf{М_J}$, $\mathbf{i \neq j}$) не содержали одинаковых элементов ($\mathbf{М_i \cap М_J = Ø}$). Таблица, приведенная на рис.1, является ключом шифра замены. Зная ее, можно осуществить как шифрование, так и расшифрование. 

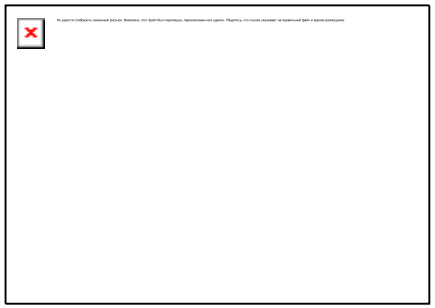
Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		Рис.1. Таблица шифрозамен При шифровании каждая буква **А** открытого сообщения заменяется любым символом из множества $\mathbf{M_А}$. Если в сообщении содержится несколько букв **А**, то каждая из них заменяется на любой символ из $\mathbf{M_А}$. За счет этого с помощью одного ключа можно получить различные варианты шифрограммы для одного и того же открытого сообщения. Так как множества $\mathbf{M_А}$, $\mathbf{M_Б}$, ..., $\mathbf{M_Я}$ попарно не пересекаются, то по каждому символу шифрограммы можно однозначно определить, какому множеству он принадлежит, и, следовательно, какую букву открытого сообщения он заменяет. Поэтому расшифрование возможно и открытое сообщение определяется единственным образом. Метод замены часто реализуется многими пользователями при работе на компьютере. Если по забывчивости не переключить на клавиатуре набор символов с латиницы на кириллицу, то вместо букв русского алфавита при вводе текста будут печататься буквы латинского алфавита («шифрозамены»). Шифры замены можно разделить на следующие **подклассы**: - **шифры однозначной замены** (моноалфавитные, простые подстановочные). Количество шифрозамен для каждого символа исходного алфавита равно 1 ($|\mathbf{M_i}| = 1$ для одного символа); - **полиграммные шифры**. Аналогичен предыдущему за исключением того, что шифрозамене соответствует сразу блок символов исходного сообщения ($|\mathbf{M_i}| = 1$ для блока символов); - **омофонические шифры** (однозвучные, многозначной замены). Количество шифрозамен для отдельных символов исходного алфавита больше 1 ($|\mathbf{M_i}| \geq 1$ для одного символа); - **полиалфавитные шифры** (многоалфавитные). Состоит из нескольких шифров однозначной заме-

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		ны. Выбор варианта алфавита для зашифрования одного символа зависит от особенностей метода шифрования (| $\mathbf{M}_i$ | > 1 для одного символа). Для записи исходных и зашифрованных сообщений используются строго определенные алфавиты. Под **алфавитом** в данном случае понимается набор символов, служащий для записи сообщений. Алфавиты для записи исходных и зашифрованных сообщений могут отличаться. Символы обоих алфавитов могут быть представлены буквами, их сочетаниями, числами, рисунками и т.п. В качестве примера можно привести пляшущих человечков из рассказа А. Конан Дойла () и рукопись рунического письма () из романа Ж. Верна «Путешествие к центру Земли». **2.2. Шифры однозначной замены.** Максимальное количество ключей для любого шифра этого вида не превышает **n!**, где **n** – количество символов в алфавите. С увеличением числа **n** значение **n!** растет очень быстро (1! = 1, 5! = 120, 10! = 3628800, 15! = 1307674368000). При больших **n** для приближенного вычисления **n!** можно воспользоваться формулой Стирлинга  (1) **Шифр Цезаря.** Данный шифр был придуман Гаем Юлием Цезарем и использовался им в своей переписке (1 век до н.э.). Применительно к русскому языку суть его состоит в следующем. Выписывается исходный алфавит (**А, Б, ..., Я**), затем под ним выписывается тот же алфавит, но с циклическим сдвигом на 3 буквы влево.

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		 Рис.2. Таблица шифрозамен для шифра Цезаря При зашифровке буква **А** заменяется буквой **Г**, **Б** - на **Д** и т. д. Так, например, исходное сообщение «АБРАМОВ» после шифрования будет выглядеть «ГДУГПСЕ». Получатель сообщения «ГДУГПСЕ» ищет эти буквы в нижней строке и по буквам над ними восстанавливает исходное сообщение «АБРАМОВ». Ключом в шифре Цезаря является величина сдвига нижней строки алфавита. Количество ключей для всех модификаций данного шифра применительно к алфавиту русского языка равно 33. Возможны различные модификации шифра Цезаря, в частности лозунговый шифр. **Лозунговый шифр.** Для данного шифра построение таблицы шифрозамен основано на лозунге (ключе) – легко запоминаемом слове. Вторая строка таблицы шифрозамен заполняется сначала словом-лозунгом (причем повторяющиеся буквы отбрасываются), а затем остальными буквами, не вошедшие в слово-лозунг, в алфавитном порядке. Например, если выбрано слово-лозунг «ДЯДИНА», то таблица имеет следующий вид.  Рис.3. Таблица шифрозамен для лозунгового шифра При шифровании исходного сообщения «АБРАМОВ» по приведенному выше ключу шифрограмма будет выглядеть «ДЯПДКМИ». В качестве лозунга рекомендуется выбирать фразу, в которой содержаться конечные буквы алфави-

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		та. В общем случае, количество вариантов нижней строки (применительно к русскому языку) составляет 33! (≥ 10^{35}). **Полибианский квадрат.** Шифр изобретен греческим государственным деятелем, полководцем и историком Полибием (III век до н.э.). Применительно к русскому алфавиту суть шифрования заключалась в следующем. В квадрат 6х6 выписываются буквы.  Рис.4. Таблица шифрозамен для полибианского квадрата Шифруемая буква заменяется на координаты квадрата (строка-столбец), в котором она записана. Например, если исходное сообщение «АБРАМОВ», то шифрограмма – «11 12 36 11 32 34 13». В Древней Греции сообщения передавались с помощью оптического телеграфа (с помощью факелов). Для каждой буквы сообщения в начале поднималось количество факелов, соответствующее номеру строки буквы, а затем номеру столбца. **Шифрующая система Трисемуса (Тритемия).** В 1508 г. аббат из Германии Иоганн Трисемус написал печатную работу по криптологии под названием «Полиграфия». В этой книге он впервые систематически описал применение шифрующих таблиц, заполненных алфавитом в случайном порядке.

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		Для получения такого шифра замены обычно использовались таблица для записи букв алфавита и ключевое слово (или фраза). В таблицу сначала вписывалось по строкам ключевое слово, причем повторяющиеся буквы отбрасывались. Затем эта таблица дополнялась не вошедшими в нее буквами алфавита по порядку. На рис.6 изображена таблица с ключевым словом «ДЯДИНА».  Рис.5. Таблица шифрозамен для шифра Трисемуса Каждая буква открытого сообщения заменяется буквой, расположенной под ней в том же столбце. Если буква находится в последней строке таблицы, то для ее шифрования берут самую верхнюю букву столбца. Например, исходное сообщение «АБРАМОВ», зашифрованное – «ИЙЪИХШК». **2.3. Полиграммные шифры.** **Полиграммные шифры замены** - шифры, которые шифруют сразу группы (блоки) символов. **Шифр Playfair (англ. «Честная игра»).** Был изобретен в 1854 г. Чарльзом Уитстоном, но назван именем лорда Лайона Плейфера, который внедрил данный шифр в государственные службы Великобритании. Он использовался англичанами в Первой мировой войне. Шифр предусматривает шифрование пар символов (биграмм). Таким образом, этот шифр более устойчив к взлому по сравнению с шифром простой замены, так как затрудняется частотный анализ. Он может быть проведен, но не

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		для 26 возможных символов (латинский алфавит), а для 26 x 26 = 676 возможных биграмм. Анализ частоты биграмм возможен, но является значительно более трудным и требует намного большего объема зашифрованного текста. Для шифрования сообщения необходимо разбить его на биграммы (группы из двух символов), при этом, если в биграмме встретятся два одинаковых символа, то между ними добавляется заранее оговоренный вспомогательный символ (в оригинале – **X**, для русского алфавита - **Я**). Например, «зашифрованное сообщение» становится «за ши фр ов ан но ес о**Я** об ще ни е**Я**». Для формирования ключевой таблицы выбирается лозунг и далее она заполняется по правилам шифрующей системы Трисемуса. Например, лозунг «ДЯДИНА»  Рис.6. Ключевая таблица для шифра Playfair Затем, руководствуясь следующими правилами, выполняется зашифровывание пар символов исходного текста: 1. Если символы биграммы исходного текста встречаются в одной строке, то эти символы замещаются на символы, расположенные в ближайших столбцах справа от соответствующих символов. Если символ является последним в строке, то он заменяется на первый символ этой же строки.

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		2. Если символы биграммы исходного текста встречаются в одном столбце, то они преобразуются в символы того же столбца, находящимися непосредственно под ними. Если символ является нижним в столбце, то он заменяется на первый символ этого же столбца. 3. Если символы биграммы исходного текста находятся в разных столбцах и разных строках, то они заменяются на символы, находящиеся в тех же строках, но соответствующие другим углам прямоугольника. Пример шифрования. - биграмма «за» формирует прямоугольник – заменяется на «жб»; - биграмма «ши» находятся в одном столбце – заменяется на «юе»; - биграмма «фр» находятся в одной строке – заменяется на «хс»; - биграмма «ов» формирует прямоугольник – заменяется на «йж»; - биграмма «ан» находятся в одной строке – заменяется на «ба»; - биграмма «но» формирует прямоугольник – заменяется на «ам»; - биграмма «ес» формирует прямоугольник – заменяется на «гт»; - биграмма «оя» формирует прямоугольник – заменяется на «ка»; - биграмма «об» формирует прямоугольник – заменяется на «па»; - биграмма «ще» формирует прямоугольник – заменяется на «шё»;

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		- биграмма «ни» формирует прямоугольник – заменяется на «ан»; - биграмма «ея» формирует прямоугольник – заменяется на «ги». Шифрограмма – «жб юе хс йж ба ам гт ка па шё ан ги». Для расшифровки необходимо использовать инверсию этих правил, откидывая символы **Я** (или **Х**), если они не несут смысла в исходном сообщении. **3. Практическая часть** Зашифруйте свою фамилию с помощью следующих шифров: - шифра Цезаря; - лозунгового шифра; - полибианского квадрата; - шифрующей системы Трисемуса; - шифра Playfair; При оформлении отчета необходимо привести исходное сообщение (фамилию), таблицу шифрозамен, ключ (если таблица шифрозамен не является ключом) и зашифрованное сообщение.
ПК-14 владением навыками использования компьютерной техники и информационных технологий в документационном обеспечении управления и архивном деле		
Знать	Принципы использования компьютерной тех-	1. Рассмотрите вопросы лицензирования в области защиты информации в законе «О лицензировании отдельных видов деятельности» от 8 августа 2001 года номер 128-ФЗ (Принят

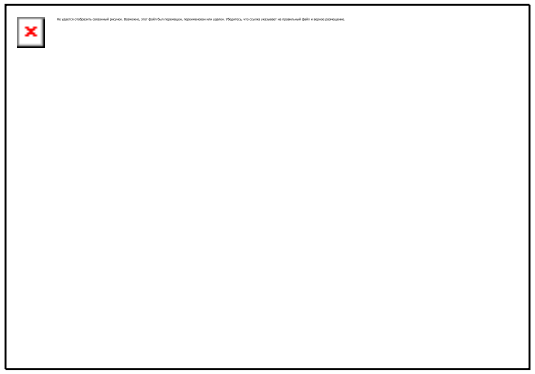
Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
	ники в документационном обеспечении управления и архивном деле. Принципы использования ИТ в документационном обеспечении управления и архивном деле. Принципы обеспечения информационной безопасности и защиты информации в процессе.	Государственной Думой 13 июля 2001 года). 2. Законодательные принципы кадровой защиты информационной безопасности. 3. Организация конфиденциального делопроизводства. 4. Возможные причины утечки информации при нарушении персоналом правил работы с конфиденциальной информацией. 5. Требования, предъявляемые к претендентам на работу с конфиденциальной информацией и к претендентам на должность в службу информационной безопасности. 6. Кадровая политика предприятия. Возможные источники пополнения предприятия кадрами для работы с конфиденциальной информацией. 7. Порядок организации и проведения конкурсов на замещения вакантных должностей, связанных с безопасностью информации. 8. Методы проверки кандидатов на работу. Отражение вопросов информационной безопасности в трудовых и коллективных договорах.
Уметь:	Работать с информацией в локальных сетях. Работать с информацией в глобальных сетях. Обеспечивать информационную безопасности и защиту информации в процессе работы.	1 Программная система защиты информации отвечает за: а) Сохранность всей введённой в информационную систему информации. **б) Реализацию заданной политики безопасности.** в) Корректное поведение пользователей. 2 Аутентификация это: **а) Подтверждение заявленного идентификатора.** б) Процесс ввода текста без отображения на экране. в) Ввод сведений личного характера. 3 Политика безопасности это: **а) Правила определения разрешённых и запрещённых операций в** информационной системе. б) Правила поведения пользователей.

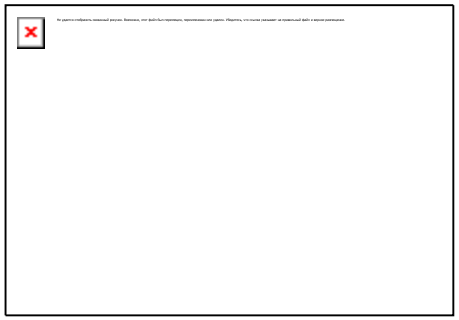
Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		в) Инструкция действий администратора по обеспечению информационной безопасности. 4 Монитор безопасности это: а) Личный терминал системного администратора. **б) Совокупность резидентных программ, реализующих политику** безопасности. в) Программа контроля данных аудита. 5 Дискреционная политика доступа: **а) Определяет права доступа идентифицированных субъектов к объектам на основе заданных внешних правил (матрицы доступа).** б) Определяет права доступа субъектов к объектам или разрешает информационные потоки между объектами на основе изменяемых меток прав доступа или конфиденциальности. в) Является алгоритмом формирования матрицы доступа. г) Содержит инструкцию для системного администратора по предоставлению прав доступа различным пользователям.
Владеть:	Базовыми приемами работы с профессиональной информацией. Способами обеспечения защиты информации в процессе работы с профессиональной информацией. Нормативно-правовой информацией в области обеспечения защиты профессиональной ин-	***Контрольная работа*** **Защита информации с помощью криптографии** **1. Цель работы** Целью работы является исследование защиты информации с применением простейших принципов криптографии. **2. Теоретическая часть** **2.1 Шифры замены** Сущность шифрования методом замены заключается в следующем [2]. Пусть шифруются сообщения

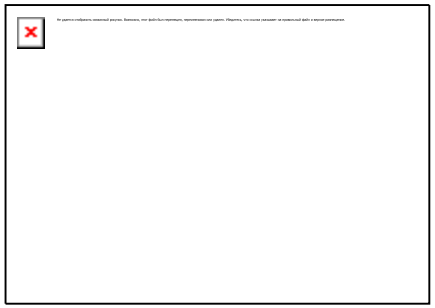
Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
	формации.	на русском языке и замене подлежит каждая буква этих сообщений. Тогда, букве **А** исходного алфавита сопоставляется некоторое множество символов (шифрозамен) $\mathbf{M_А}$, **Б –** $\mathbf{M_Б}$, **…, Я –** $\mathbf{M_Я}$. Шифрозамены выбираются таким образом, чтобы любые два множества ($\mathbf{M_i}$ и $\mathbf{M_J}$, $\mathbf{i \neq j}$) не содержали одинаковых элементов ($\mathbf{M_i \cap M_J = \varnothing}$). Таблица, приведенная на рис.1, является ключом шифра замены. Зная ее, можно осуществить как шифрование, так и расшифрование.  Рис.1. Таблица шифрозамен При шифровании каждая буква **А** открытого сообщения заменяется любым символом из множества $\mathbf{M_А}$. Если в сообщении содержится несколько букв **А**, то каждая из них заменяется на любой символ из $\mathbf{M_А}$. За счет этого с помощью одного ключа можно получить различные варианты шифрограммы для одного и того же открытого сообщения. Так как множества $\mathbf{M_А}$, $\mathbf{M_Б}$, **...,** $\mathbf{M_Я}$ попарно не пересекаются, то по каждому символу шифрограммы можно однозначно определить, какому множеству он принадлежит, и, следовательно, какую букву открытого сообщения он заменяет. Поэтому расшифрование возможно и открытое сообщение определяется единственным образом. Метод замены часто реализуется многими пользователями при работе на компьютере. Если по забывчивости не переключить на клавиатуре набор символов с латиницы на кириллицу, то вместо букв русского алфавита при вводе текста будут печататься буквы латинского алфавита («шифрозамены»).

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		Шифры замены можно разделить на следующие **подклассы**: - **шифры однозначной замены** (моноалфавитные, простые подстановочные). Количество шифрозамен для каждого символа исходного алфавита равно 1 (| $\mathbf{M}_i$ | = 1 для одного символа); - **полиграммные шифры**. Аналогичен предыдущему за исключением того, что шифрозамене соответствует сразу блок символов исходного сообщения (| $\mathbf{M}_i$ | = 1 для блока символов); - **омофонические шифры** (однозвучные, многозначной замены). Количество шифрозамен для отдельных символов исходного алфавита больше 1 (| $\mathbf{M}_i$ | ≥ 1 для одного символа); - **полиалфавитные шифры** (многоалфавитные). Состоит из нескольких шифров однозначной замены. Выбор варианта алфавита для зашифрования одного символа зависит от особенностей метода шифрования (| $\mathbf{M}_i$ | > 1 для одного символа). Для записи исходных и зашифрованных сообщений используются строго определенные алфавиты. Под **алфавитом** в данном случае понимается набор символов, служащий для записи сообщений. Алфавиты для записи исходных и зашифрованных сообщений могут отличаться. Символы обоих алфавитов могут быть представлены буквами, их сочетаниями, числами, рисунками и т.п. В качестве примера можно привести пляшущих человечков из рассказа А. Конан Дойла () и рукопись рунического письма () из романа Ж. Верна «Путешествие к центру Земли». **2.2. Шифры однозначной замены.** Максимальное количество ключей для любого шифра этого вида не превышает **n!**, где **n** – количество символов в алфавите. С увеличением числа **n** значение **n!** растет очень быстро (1! = 1, 5! = 120, 10! = 3628800, 15! = 1307674368000). При больших **n** для приближенного вычисления **n!** можно вос-

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		пользоваться формулой Стирлинга  (1) **Шифр Цезаря.** Данный шифр был придуман Гаем Юлием Цезарем и использовался им в своей переписке (1 век до н.э.). Применительно к русскому языку суть его состоит в следующем. Выписывается исходный алфавит (**А, Б, ..., Я**), затем под ним выписывается тот же алфавит, но с циклическим сдвигом на 3 буквы влево.  Рис.2. Таблица шифрозамен для шифра Цезаря При зашифровке буква **А** заменяется буквой **Г**, **Б** - на **Д** и т. д. Так, например, исходное сообщение «АБРАМОВ» после шифрования будет выглядеть «ГДУГПСЕ». Получатель сообщения «ГДУГПСЕ» ищет эти буквы в нижней строке и по буквам над ними восстанавливает исходное сообщение «АБРАМОВ». Ключом в шифре Цезаря является величина сдвига нижней строки алфавита. Количество ключей для всех модификаций данного шифра применительно к алфавиту русского языка равно 33. Возможны различные модификации шифра Цезаря, в частности лозунговый шифр. **Лозунговый шифр.** Для данного шифра построение таблицы шифрозамен основано на лозунге (ключе) – легко запоминаемом слове. Вторая строка таблицы шифрозамен заполняется сначала словом-лозунгом (причем повторяющиеся буквы отбрасываются), а затем остальными буквами, не вошедшие в слово-лозунг, в алфавитном порядке. Например, если выбрано слово-лозунг «ДЯДИ-

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		НА», то таблица имеет следующий вид.  Рис.3. Таблица шифрозамен для лозунгового шифра При шифровании исходного сообщения «АБРАМОВ» по приведенному выше ключу шифрограмма будет выглядеть «ДЯПДКМИ». В качестве лозунга рекомендуется выбирать фразу, в которой содержаться конечные буквы алфавита. В общем случае, количество вариантов нижней строки (применительно к русскому языку) составляет 33! ($\geq 10^{35}$). **Полибианский квадрат.** Шифр изобретен греческим государственным деятелем, полководцем и историком Полибием (III век до н.э.). Применительно к русскому алфавиту суть шифрования заключалась в следующем. В квадрат 6x6 выписываются буквы.  Рис.4. Таблица шифрозамен для полибианского квадрата

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		Шифруемая буква заменяется на координаты квадрата (строка-столбец), в котором она записана. Например, если исходное сообщение «АБРАМОВ», то шифрограмма – «11 12 36 11 32 34 13». В Древней Греции сообщения передавались с помощью оптического телеграфа (с помощью факелов). Для каждой буквы сообщения в начале поднималось количество факелов, соответствующее номеру строки буквы, а затем номеру столбца. **Шифрующая система Трисемуса (Тритемия).** В 1508 г. аббат из Германии Иоганн Трисемус написал печатную работу по криптологии под названием «Полиграфия». В этой книге он впервые систематически описал применение шифрующих таблиц, заполненных алфавитом в случайном порядке. Для получения такого шифра замены обычно использовались таблица для записи букв алфавита и ключевое слово (или фраза). В таблицу сначала вписывалось по строкам ключевое слово, причем повторяющиеся буквы отбрасывались. Затем эта таблица дополнялась не вошедшими в нее буквами алфавита по порядку. На рис.6 изображена таблица с ключевым словом «ДЯДИНА».  Рис.5. Таблица шифрозамен для шифра Трисемуса Каждая буква открытого сообщения заменяется буквой, расположенной под ней в том же столбце. Если буква находится в последней строке таблицы, то для ее шифрования берут самую верхнюю букву столбца. Например, исходное сообщение «АБРАМОВ», зашифрованное – «ИЙЪИХШК».

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		2.3. Полиграммные шифры. **Полиграммные шифры замены** - шифры, которые шифруют сразу группы (блоки) символов. **Шифр Playfair (англ. «Честная игра»).** Был изобретен в 1854 г. Чарльзом Уитстоном, но назван именем лорда Лайона Плейфера, который внедрил данный шифр в государственные службы Великобритании. Он использовался англичанами в Первой мировой войне. Шифр предусматривает шифрование пар символов (биграмм). Таким образом, этот шифр более устойчив к взлому по сравнению с шифром простой замены, так как затрудняется частотный анализ. Он может быть проведен, но не для 26 возможных символов (латинский алфавит), а для 26 x 26 = 676 возможных биграмм. Анализ частоты биграмм возможен, но является значительно более трудным и требует намного большего объема зашифрованного текста. Для шифрования сообщения необходимо разбить его на биграммы (группы из двух символов), при этом, если в биграмме встретятся два одинаковых символа, то между ними добавляется заранее оговоренный вспомогательный символ (в оригинале – **X**, для русского алфавита - **Я**). Например, «зашифрованное сообщение» становится «за ши фр ов ан но ес о**Я** об ще ни е**Я**». Для формирования ключевой таблицы выбирается лозунг и далее она заполняется по правилам шифрующей системы Трисемуса. Например, лозунг «ДЯДИНА» 

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		Рис.6. Ключевая таблица для шифра Playfair Затем, руководствуясь следующими правилами, выполняется зашифровывание пар символов исходного текста: 1. Если символы биграммы исходного текста встречаются в одной строке, то эти символы замещаются на символы, расположенные в ближайших столбцах справа от соответствующих символов. Если символ является последним в строке, то он заменяется на первый символ этой же строки. 2. Если символы биграммы исходного текста встречаются в одном столбце, то они преобразуются в символы того же столбца, находящимися непосредственно под ними. Если символ является нижним в столбце, то он заменяется на первый символ этого же столбца. 3. Если символы биграммы исходного текста находятся в разных столбцах и разных строках, то они заменяются на символы, находящиеся в тех же строках, но соответствующие другим углам прямоугольника. Пример шифрования. - биграмма «за» формирует прямоугольник – заменяется на «жб»; - биграмма «ши» находятся в одном столбце – заменяется на «юе»; - биграмма «фр» находятся в одной строке – заменяется на «хс»; - биграмма «ов» формирует прямоугольник – заменяется на «йж»; - биграмма «ан» находятся в одной строке – заменяется на «ба»; - биграмма «но» формирует прямоугольник – заменяется на «ам»;

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		- биграмма «ес» формирует прямоугольник – заменяется на «гт»; - биграмма «оя» формирует прямоугольник – заменяется на «ка»; - биграмма «об» формирует прямоугольник – заменяется на «па»; - биграмма «ще» формирует прямоугольник – заменяется на «шё»; - биграмма «ни» формирует прямоугольник – заменяется на «ан»; - биграмма «ея» формирует прямоугольник – заменяется на «ги». Шифрограмма – «жб юе хс йж ба ам гт ка па шё ан ги». Для расшифровки необходимо использовать инверсию этих правил, откидывая символы **Я** (или **Х**), если они не несут смысла в исходном сообщении. **3. Практическая часть** Зашифруйте свою фамилию с помощью следующих шифров: - шифра Цезаря; - лозунгового шифра; - полибианского квадрата; - шифрующей системы Трисемуса; - шифра Playfair;

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		При оформлении отчета необходимо привести исходное сообщение (фамилию), таблицу шифрозамен, ключ (если таблица шифрозамен не является ключом) и зашифрованное сообщение.
ПК-15 способностью совершенствовать технологии документационного обеспечения управления и архивного дела на базе использования средств автоматизации		
Знать	Технологии документационного обеспечения управления и архивного дела на базе использования средств автоматизации. Способы обеспечения защиты информации с помощью средств автоматизации. Сферы применения способов обеспечения информационной безопасности на уровне технологий документационного обеспечения управления и архивного дела на базе использования средств автоматизации.	1. Эргономические и нормативные требования к организации рабочего места пользователя. 2. Организация антивирусной защиты. 3. Организация парольной защиты. 4. Инструкция по организации парольной защиты. 5. Общие подходы к построению парольных систем. 6. Защита от плагиата. 7. Дайте характеристику следующих форм защиты информации: патентование, авторское право, товарные знаки («Патентный закон РФ», «О товарных знаках, знаках обслуживания и наименовании мест происхождения товаров»).
Уметь:	Применять в стандартных рабочих ситуациях способы обеспечения	1 Программная система защиты информации отвечает за: *а) Сохранность всей введённой в информационную систему информации.*

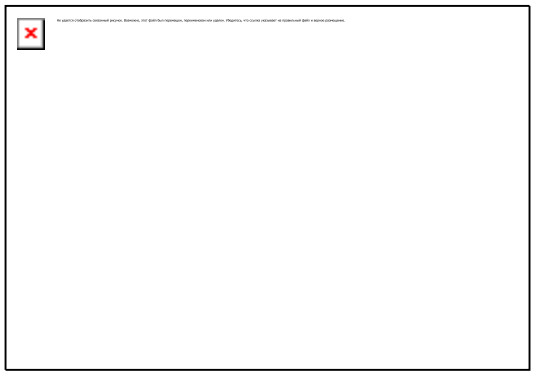
Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
	информационной безопасности в средствах автоматизации. Характеризовать способы обеспечения информационной безопасности в технологиях документационного обеспечения управления и архивного дела на базе использования средств автоматизации. Корректно использовать средства защиты информации в средствах автоматизации технологий документационного обеспечения управления и архивного дела	**б) Реализацию заданной политики безопасности.** в) Корректное поведение пользователей. 2 Аутентификация это: **а) Подтверждение заявленного идентификатора.** б) Процесс ввода текста без отображения на экране. в) Ввод сведений личного характера. 3 Политика безопасности это: **а) Правила определения разрешённых и запрещённых операций в** информационной системе. б) Правила поведения пользователей. в) Инструкция действий администратора по обеспечению информационной безопасности. 4 Монитор безопасности это: а) Личный терминал системного администратора. **б) Совокупность резидентных программ, реализующих политику** безопасности. в) Программа контроля данных аудита. 5 Дискреционная политика доступа: **а) Определяет права доступа идентифицированных субъектов к объектам на основе заданных внешних правил (матрицы доступа).** б) Определяет права доступа субъектов к объектам или разрешает информационные потоки между объектами на основе изменяемых меток прав доступа или конфиденциальности. в) Является алгоритмом формирования матрицы доступа. г) Содержит инструкцию для системного администратора по предоставлению прав доступа различным пользователям.

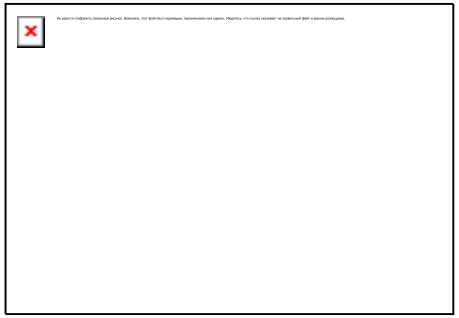
Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
Владеть:		***Контрольная работа*** **Защита информации с помощью криптографии** **1. Цель работы** Целью работы является исследование защиты информации с применением простейших принципов криптографии. **2. Теоретическая часть** **2.1 Шифры замены** Сущность шифрования методом замены заключается в следующем [2]. Пусть шифруются сообщения на русском языке и замене подлежит каждая буква этих сообщений. Тогда, букве **А** исходного алфавита сопоставляется некоторое множество символов (шифрозамен) $\mathbf{M_А}$**, Б –** $\mathbf{M_Б}$**, …, Я –** $\mathbf{M_Я}$. Шифрозамены выбираются таким образом, чтобы любые два множества ($\mathbf{M_i}$ и $\mathbf{M_J}$, $\mathbf{i \neq j}$) не содержали одинаковых элементов ($\mathbf{M_i \cap M_J = \varnothing}$). Таблица, приведенная на рис.1, является ключом шифра замены. Зная ее, можно осуществить как шифрование, так и расшифрование.  Рис.1. Таблица шифрозамен При шифровании каждая буква **А** открытого сообщения заменяется любым символом из множества $\mathbf{M_А}$. Если в сообщении содержится несколько букв **А**, то каждая из них заменяется на любой символ из $\mathbf{M_А}$. За счет этого с помощью одного ключа можно получить различные варианты шифро-

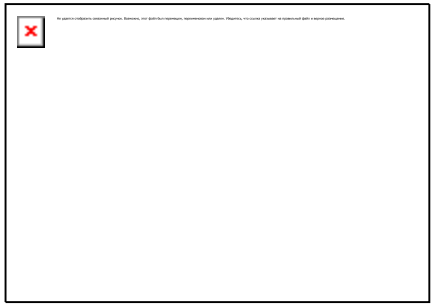
Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		граммы для одного и того же открытого сообщения. Так как множества $\mathbf{M_А, M_Б, ..., M_Я}$ попарно не пересекаются, то по каждому символу шифрограммы можно однозначно определить, какому множеству он принадлежит, и, следовательно, какую букву открытого сообщения он заменяет. Поэтому расшифрование возможно и открытое сообщение определяется единственным образом. Метод замены часто реализуется многими пользователями при работе на компьютере. Если по забывчивости не переключить на клавиатуре набор символов с латиницы на кириллицу, то вместо букв русского алфавита при вводе текста будут печататься буквы латинского алфавита («шифрозамены»). Шифры замены можно разделить на следующие **подклассы**: - **шифры однозначной замены** (моноалфавитные, простые подстановочные). Количество шифрозамен для каждого символа исходного алфавита равно 1 ($\mid \mathbf{M}_i \mid = 1$ для одного символа); - **полиграммные шифры**. Аналогичен предыдущему за исключением того, что шифрозамене соответствует сразу блок символов исходного сообщения ($\mid \mathbf{M}_i \mid = 1$ для блока символов); - **омофонические шифры** (однозвучные, многозначной замены). Количество шифрозамен для отдельных символов исходного алфавита больше 1 ($\mid \mathbf{M}_i \mid \geq 1$ для одного символа); - **полиалфавитные шифры** (многоалфавитные). Состоит из нескольких шифров однозначной замены. Выбор варианта алфавита для зашифрования одного символа зависит от особенностей метода шифрования ($\mid \mathbf{M}_i \mid > 1$ для одного символа). Для записи исходных и зашифрованных сообщений используются строго определенные алфавиты. Под **алфавитом** в данном случае понимается набор символов, служащий для записи сообщений.

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		Алфавиты для записи исходных и зашифрованных сообщений могут отличаться. Символы обоих алфавитов могут быть представлены буквами, их сочетаниями, числами, рисунками и т.п. В качестве примера можно привести пляшущих человечков из рассказа А. Конан Дойла () и рукопись рунического письма () из романа Ж. Верна «Путешествие к центру Земли». **2.2. Шифры однозначной замены.** Максимальное количество ключей для любого шифра этого вида не превышает **n!**, где **n** – количество символов в алфавите. С увеличением числа **n** значение **n!** растет очень быстро (1! = 1, 5! = 120, 10! = 3628800, 15! = 1307674368000). При больших **n** для приближенного вычисления **n!** можно воспользоваться формулой Стирлинга  (1) **Шифр Цезаря.** Данный шифр был придуман Гаем Юлием Цезарем и использовался им в своей переписке (1 век до н.э.). Применительно к русскому языку суть его состоит в следующем. Выписывается исходный алфавит (**А, Б, ..., Я**), затем под ним выписывается тот же алфавит, но с циклическим сдвигом на 3 буквы влево.  Рис.2. Таблица шифрозамен для шифра Цезаря При зашифровке буква **А** заменяется буквой **Г**, **Б** - на **Д** и т. д. Так, например, исходное сообщение «АБРАМОВ» после шифрования будет выглядеть «ГДУГПСЕ». Получатель сообщения «ГДУГПСЕ»

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		ищет эти буквы в нижней строке и по буквам над ними восстанавливает исходное сообщение «АБРАМОВ». Ключом в шифре Цезаря является величина сдвига нижней строки алфавита. Количество ключей для всех модификаций данного шифра применительно к алфавиту русского языка равно 33. Возможны различные модификации шифра Цезаря, в частности лозунговый шифр. **Лозунговый шифр.** Для данного шифра построение таблицы шифрозамен основано на лозунге (ключе) – легко запоминаемом слове. Вторая строка таблицы шифрозамен заполняется сначала словом-лозунгом (причем повторяющиеся буквы отбрасываются), а затем остальными буквами, не вошедшие в слово-лозунг, в алфавитном порядке. Например, если выбрано слово-лозунг «ДЯДИНА», то таблица имеет следующий вид.  Рис.3. Таблица шифрозамен для лозунгового шифра При шифровании исходного сообщения «АБРАМОВ» по приведенному выше ключу шифрограмма будет выглядеть «ДЯПДКМИ». В качестве лозунга рекомендуется выбирать фразу, в которой содержаться конечные буквы алфавита. В общем случае, количество вариантов нижней строки (применительно к русскому языку) составляет 33! ($\geq 10^{35}$). **Полибианский квадрат.** Шифр изобретен греческим государственным деятелем, полководцем и историком Полибием (III век до н.э.). Применительно к русскому алфавиту суть шифрования заключалась в следующем. В квадрат 6х6 выписываются буквы.

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		 Рис.4. Таблица шифрозамен для полибианского квадрата Шифруемая буква заменяется на координаты квадрата (строка-столбец), в котором она записана. Например, если исходное сообщение «АБРАМОВ», то шифрограмма – «11 12 36 11 32 34 13». В Древней Греции сообщения передавались с помощью оптического телеграфа (с помощью факелов). Для каждой буквы сообщения в начале поднималось количество факелов, соответствующее номеру строки буквы, а затем номеру столбца. **Шифрующая система Трисемуса (Тритемия).** В 1508 г. аббат из Германии Иоганн Трисемус написал печатную работу по криптологии под названием «Полиграфия». В этой книге он впервые систематически описал применение шифрующих таблиц, заполненных алфавитом в случайном порядке. Для получения такого шифра замены обычно использовались таблица для записи букв алфавита и ключевое слово (или фраза). В таблицу сначала вписывалось по строкам ключевое слово, причем повторяющиеся буквы отбрасывались. Затем эта таблица дополнялась не вошедшими в нее буквами алфавита по порядку. На рис.6 изображена таблица с ключевым словом «ДЯДИНА».

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		 Рис.5. Таблица шифрозамен для шифра Трисемуса Каждая буква открытого сообщения заменяется буквой, расположенной под ней в том же столбце. Если буква находится в последней строке таблицы, то для ее шифрования берут самую верхнюю букву столбца. Например, исходное сообщение «АБРАМОВ», зашифрованное – «ИЙЪИХШК». **2.3. Полиграммные шифры.** **Полиграммные шифры замены** - шифры, которые шифруют сразу группы (блоки) символов. **Шифр Playfair (англ. «Честная игра»).** Был изобретен в 1854 г. Чарльзом Уитстоном, но назван именем лорда Лайона Плейфера, который внедрил данный шифр в государственные службы Великобритании. Он использовался англичанами в Первой мировой войне. Шифр предусматривает шифрование пар символов (биграмм). Таким образом, этот шифр более устойчив к взлому по сравнению с шифром простой замены, так как затрудняется частотный анализ. Он может быть проведен, но не для 26 возможных символов (латинский алфавит), а для 26 x 26 = 676 возможных биграмм. Анализ частоты биграмм возможен, но является значительно более трудным и требует намного большего объема зашифрованного текста. Для шифрования сообщения необходимо разбить его на биграммы (группы из двух символов), при

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		этом, если в биграмме встретятся два одинаковых символа, то между ними добавляется заранее оговоренный вспомогательный символ (в оригинале – **X**, для русского алфавита - **Я**). Например, «зашифрованное сообщение» становится «за ши фр ов ан но ес о**Я** об ще ни е**Я**». Для формирования ключевой таблицы выбирается лозунг и далее она заполняется по правилам шифрующей системы Трисемуса. Например, лозунг «ДЯДИНА»  Рис.6. Ключевая таблица для шифра Playfair Затем, руководствуясь следующими правилами, выполняется зашифровывание пар символов исходного текста: 1. Если символы биграммы исходного текста встречаются в одной строке, то эти символы замещаются на символы, расположенные в ближайших столбцах справа от соответствующих символов. Если символ является последним в строке, то он заменяется на первый символ этой же строки. 2. Если символы биграммы исходного текста встречаются в одном столбце, то они преобразуются в символы того же столбца, находящимися непосредственно под ними. Если символ является нижним в столбце, то он заменяется на первый символ этого же столбца. 3. Если символы биграммы исходного текста находятся в разных столбцах и разных строках, то они

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		заменяются на символы, находящиеся в тех же строках, но соответствующие другим углам прямоугольника. Пример шифрования. - биграмма «за» формирует прямоугольник – заменяется на «жб»; - биграмма «ши» находятся в одном столбце – заменяется на «юе»; - биграмма «фр» находятся в одной строке – заменяется на «хс»; - биграмма «ов» формирует прямоугольник – заменяется на «йж»; - биграмма «ан» находятся в одной строке – заменяется на «ба»; - биграмма «но» формирует прямоугольник – заменяется на «ам»; - биграмма «ес» формирует прямоугольник – заменяется на «гт»; - биграмма «оя» формирует прямоугольник – заменяется на «ка»; - биграмма «об» формирует прямоугольник – заменяется на «па»; - биграмма «ще» формирует прямоугольник – заменяется на «шё»; - биграмма «ни» формирует прямоугольник – заменяется на «ан»; - биграмма «ея» формирует прямоугольник – заменяется на «ги». Шифрограмма – «жб юе хс йж ба ам гт ка па шё ан ги». Для расшифровки необходимо использовать инверсию этих правил, откидывая символы **Я** (или **Х**),

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		если они не несут смысла в исходном сообщении. **3. Практическая часть** Зашифруйте свою фамилию с помощью следующих шифров: - шифра Цезаря; - лозунгового шифра; - полибианского квадрата; - шифрующей системы Трисемуса; - шифра Playfair; При оформлении отчета необходимо привести исходное сообщение (фамилию), таблицу шифрозамен, ключ (если таблица шифрозамен не является ключом) и зашифрованное сообщение.
ПК-17 владением методами защиты информации		
Знать	Нормативно-терминологическая база в области защиты информационной безопасности. Критерии отнесения информации к защищаемой. Методы и средства за-	1. Текущая работа с персоналом, допущенным к конфиденциальной информации. Дисциплинарная ответственность. Меры поощрения и наказания. 2. Порядок завершения текущей работы с сотрудниками, владеющими конфиденциальной информацией при их увольнении. 3. Обязанности сотрудников по обеспечению информационной безопасности. 4. Защита от инсайдера. 5. Общие сведения о компьютерных вирусах. Определение компьютерных вирусов. Классификация компьютерных вирусов по среде обитания, поражаемой операционной системе, особенностям алгоритма работы, деструктивным возможностям.

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
	щиты информации.	6. Источники распространения, группы риска. Последствия действий вирусов, примеры (со ссылками на источники информации). Использования компьютерных вирусов для организации каналов утечки и несанкционированного доступа к информации. 7. Принципы функционирования компьютерных вирусов. Нерезидентные файловые вирусы. Принципы заражения пакетных файлов. Формат и принципы заражения COM-программ. Формат и принципы заражения EXE-программ. 8. Резидентные компьютерные вирусы. Структура файлового резидентного вируса. Структуры загрузочного дискеты и MBR жесткого диска. Загрузочные вирусы. Жизненный цикл и среда обитания компьютерных вирусов. Симптомы заражения и вызываемые вирусами эффекты. Повторное заражение. Примеры. 9. Полиморфные и стелс-вирусы. Сетевые вирусы. Криптовирусы. Примеры. 10. Вирусы-макросы для Microsoft Word и Microsoft Excel. Примеры. 11. Вирусы-черви. Признаки заражения. Профилактика заражения. Примеры. 12. Программные антивирусные средства. Определения и общие принципы функционирования фагов, детекторов, ревизоров, вакцин, сторожей. Структура антивирусной программы. Принципы выбора сигнатуры компьютерного вируса. 13. Обзор отечественных и зарубежных антивирусных продуктов (eTrust Antivirus и др.). Действия при обнаружении и способы устранения вирусов 14. Законодательные принципы организационной защиты информационной безопасности. 15. Порядок установления режима конфиденциальности информации. Перечень сведений, относимых к конфиденциальной информации и не подлежащих засекречиванию. 16. Регламентация действий всех категорий сотрудников, допущенных к работе с информационными системами. 17. Организация конфиденциального делопроизводства. 18. Порядок обеспечения сохранности конфиденциальной информации при постоянном или временном прекращении пользователем доступа к конфиденциальному информационному ресурсу. 19. Возможные причины утечки информации при нарушении персоналом правил работы с конфиденциальной информацией.

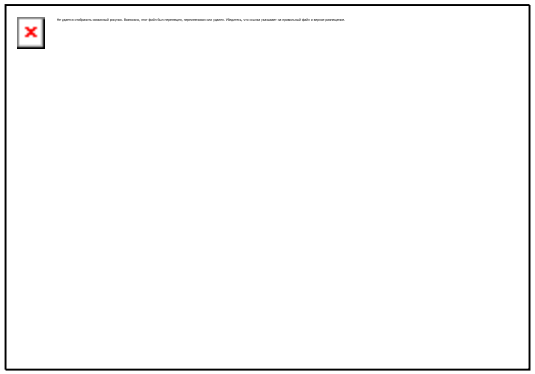
Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		20. Организационные меры по обеспечению и поддержанию информационной безопасности в период чрезвычайных ситуаций. 21. Мероприятия по защите от несанкционированного доступа. Какие методы позволяют с наибольшей точностью определить состояние информационной безопасности учреждения?
Уметь:	Ориентироваться в программном обеспечении, необходимом для обеспечения защиты информации. Определять вид конфиденциальной информации. Применять на практике основные способы защиты информации на различных носителях.	1 Мандатная политика доступа: а) Определяет права доступа идентифицированных субъектов к объектам на основе заданных внешних правил (матрицы доступа). **б) Определяет права доступа субъектов к объектам или разрешает информационные потоки между объектами на основе изменяемых меток прав доступа субъектов и меток конфиденциальности объектов.** в) Является алгоритмом формирования матрицы доступа. г) Содержит инструкцию для системного администратора по предоставлению прав доступа различным пользователям. 2 Компьютерным вирусом называется: **а) Программа, способная внедряться в другие программы, с возможностью самовоспроизводства.** б) Вид бактерий, разрушающий микросхемы. в) Процесс разрушения информации на неисправном жёстком диске. 3 Что здесь не относится к антивирусным программам: а) Dr. Web б) AVP **в) Norton DiskDoktor** 4 В системе стандартов «Общие критерии» требования не объединяются в: а) Классы

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		б) Семейства **в) Группы** 5 В документах Гостехкомиссии под показателями защищённости понимается: а) Экспертная оценка системы защиты информации по пятибалльной шкале. **б) Перечень группы требований, необходимых для выполнения в информационных системах заданного класса защищённости.** в) Временные характеристики реакции системы безопасности на обнаружение несанкционированного доступа.
Владеть:	Нормативно-терминологической базой в области защиты информации. Основными методами защиты информации на различных носителях. Основными методами построения системы защиты документированной информации в профессиональной области.	***Контрольная работа*** **Защита информации с помощью криптографии** **1. Цель работы** Целью работы является исследование защиты информации с применением простейших принципов криптографии. **2. Теоретическая часть** **2.1 Шифры замены** Сущность шифрования методом замены заключается в следующем [2]. Пусть шифруются сообщения на русском языке и замене подлежит каждая буква этих сообщений. Тогда, букве **А** исходного алфавита сопоставляется некоторое множество символов (шифрозамен) $\mathbf{M_А}$, **Б –** $\mathbf{M_Б}$, **…, Я –** $\mathbf{M_Я}$. Шифрозамены выбираются таким образом, чтобы любые два множества ($\mathbf{M_i}$ и $\mathbf{M_J}$, $\mathbf{i \neq j}$) не содержали одинако-

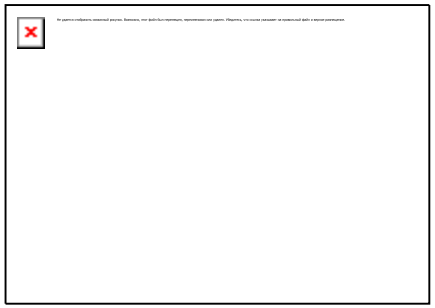
Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		вых элементов ($\mathbf{M_I} \cap \mathbf{M_J} = \mathbf{\varnothing}$). Таблица, приведенная на рис.1, является ключом шифра замены. Зная ее, можно осуществить как шифрование, так и расшифрование.  Рис.1. Таблица шифрозамен При шифровании каждая буква **А** открытого сообщения заменяется любым символом из множества $\mathbf{M_А}$. Если в сообщении содержится несколько букв **А**, то каждая из них заменяется на любой символ из $\mathbf{M_А}$. За счет этого с помощью одного ключа можно получить различные варианты шифрограммы для одного и того же открытого сообщения. Так как множества $\mathbf{M_А}$, $\mathbf{M_Б}$, ..., $\mathbf{M_Я}$ попарно не пересекаются, то по каждому символу шифрограммы можно однозначно определить, какому множеству он принадлежит, и, следовательно, какую букву открытого сообщения он заменяет. Поэтому расшифрование возможно и открытое сообщение определяется единственным образом. Метод замены часто реализуется многими пользователями при работе на компьютере. Если по забывчивости не переключить на клавиатуре набор символов с латиницы на кириллицу, то вместо букв русского алфавита при вводе текста будут печататься буквы латинского алфавита («шифрозамены»). Шифры замены можно разделить на следующие **подклассы**: - **шифры однозначной замены** (моноалфавитные, простые подстановочные). Количество шифро-

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		замен для каждого символа исходного алфавита равно 1 (| $\mathbf{M}_i$ | = 1 для одного символа); - **полиграммные шифры**. Аналогичен предыдущему за исключением того, что шифрозамене соответствует сразу блок символов исходного сообщения (| $\mathbf{M}_i$ | = 1 для блока символов); - **омофонические шифры** (однозвучные, многозначной замены). Количество шифрозамен для отдельных символов исходного алфавита больше 1 (| $\mathbf{M}_i$ | ≥ 1 для одного символа); - **полиалфавитные шифры** (многоалфавитные). Состоит из нескольких шифров однозначной замены. Выбор варианта алфавита для зашифрования одного символа зависит от особенностей метода шифрования (| $\mathbf{M}_i$ | > 1 для одного символа). Для записи исходных и зашифрованных сообщений используются строго определенные алфавиты. Под **алфавитом** в данном случае понимается набор символов, служащий для записи сообщений. Алфавиты для записи исходных и зашифрованных сообщений могут отличаться. Символы обоих алфавитов могут быть представлены буквами, их сочетаниями, числами, рисунками и т.п. В качестве примера можно привести пляшущих человечков из рассказа А. Конан Дойла () и рукопись рунического письма () из романа Ж. Верна «Путешествие к центру Земли». **2.2. Шифры однозначной замены.** Максимальное количество ключей для любого шифра этого вида не превышает **n!**, где **n** – количество символов в алфавите. С увеличением числа **n** значение **n!** растет очень быстро (1! = 1, 5! = 120, 10! = 3628800, 15! = 1307674368000). При больших **n** для приближенного вычисления **n!** можно воспользоваться формулой Стирлинга

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		 (1) **Шифр Цезаря.** Данный шифр был придуман Гаем Юлием Цезарем и использовался им в своей переписке (1 век до н.э.). Применительно к русскому языку суть его состоит в следующем. Выписывается исходный алфавит (**А, Б, ..., Я**), затем под ним выписывается тот же алфавит, но с циклическим сдвигом на 3 буквы влево.  Рис.2. Таблица шифрозамен для шифра Цезаря При зашифровке буква **А** заменяется буквой **Г**, **Б** - на **Д** и т. д. Так, например, исходное сообщение «АБРАМОВ» после шифрования будет выглядеть «ГДУГПСЕ». Получатель сообщения «ГДУГПСЕ» ищет эти буквы в нижней строке и по буквам над ними восстанавливает исходное сообщение «АБРАМОВ». Ключом в шифре Цезаря является величина сдвига нижней строки алфавита. Количество ключей для всех модификаций данного шифра применительно к алфавиту русского языка равно 33. Возможны различные модификации шифра Цезаря, в частности лозунговый шифр. **Лозунговый шифр.** Для данного шифра построение таблицы шифрозамен основано на лозунге (ключе) – легко запоминаемом слове. Вторая строка таблицы шифрозамен заполняется сначала словом-лозунгом (причем повторяющиеся буквы отбрасываются), а затем остальными буквами, не вошедшие в слово-лозунг, в алфавитном порядке. Например, если выбрано слово-лозунг «ДЯДИНА», то таблица имеет следующий вид.

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		 Рис.3. Таблица шифрозамен для лозунгового шифра При шифровании исходного сообщения «АБРАМОВ» по приведенному выше ключу шифрограмма будет выглядеть «ДЯПДКМИ». В качестве лозунга рекомендуется выбирать фразу, в которой содержаться конечные буквы алфавита. В общем случае, количество вариантов нижней строки (применительно к русскому языку) составляет 33! ($\geq 10^{35}$). **Полибианский квадрат.** Шифр изобретен греческим государственным деятелем, полководцем и историком Полибием (III век до н.э.). Применительно к русскому алфавиту суть шифрования заключалась в следующем. В квадрат 6х6 выписываются буквы.  Рис.4. Таблица шифрозамен для полибианского квадрата Шифруемая буква заменяется на координаты квадрата (строка-столбец), в котором она записана.

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		Например, если исходное сообщение «АБРАМОВ», то шифрограмма – «11 12 36 11 32 34 13». В Древней Греции сообщения передавались с помощью оптического телеграфа (с помощью факелов). Для каждой буквы сообщения в начале поднималось количество факелов, соответствующее номеру строки буквы, а затем номеру столбца. **Шифрующая система Трисемуса (Тритемия).** В 1508 г. аббат из Германии Иоганн Трисемус написал печатную работу по криптологии под названием «Полиграфия». В этой книге он впервые систематически описал применение шифрующих таблиц, заполненных алфавитом в случайном порядке. Для получения такого шифра замены обычно использовались таблица для записи букв алфавита и ключевое слово (или фраза). В таблицу сначала вписывалось по строкам ключевое слово, причем повторяющиеся буквы отбрасывались. Затем эта таблица дополнялась не вошедшими в нее буквами алфавита по порядку. На рис.6 изображена таблица с ключевым словом «ДЯДИНА».  Рис.5. Таблица шифрозамен для шифра Трисемуса Каждая буква открытого сообщения заменяется буквой, расположенной под ней в том же столбце. Если буква находится в последней строке таблицы, то для ее шифрования берут самую верхнюю букву столбца. Например, исходное сообщение «АБРАМОВ», зашифрованное – «ИЙЪИХШК».

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		2.3. Полиграммные шифры. **Полиграммные шифры замены** - шифры, которые шифруют сразу группы (блоки) символов. **Шифр Playfair (англ. «Честная игра»).** Был изобретен в 1854 г. Чарльзом Уитстоном, но назван именем лорда Лайона Плейфера, который внедрил данный шифр в государственные службы Великобритании. Он использовался англичанами в Первой мировой войне. Шифр предусматривает шифрование пар символов (биграмм). Таким образом, этот шифр более устойчив к взлому по сравнению с шифром простой замены, так как затрудняется частотный анализ. Он может быть проведен, но не для 26 возможных символов (латинский алфавит), а для 26 x 26 = 676 возможных биграмм. Анализ частоты биграмм возможен, но является значительно более трудным и требует намного большего объема зашифрованного текста. Для шифрования сообщения необходимо разбить его на биграммы (группы из двух символов), при этом, если в биграмме встретятся два одинаковых символа, то между ними добавляется заранее оговоренный вспомогательный символ (в оригинале – **X**, для русского алфавита - **Я**). Например, «зашифрованное сообщение» становится «за ши фр ов ан но ес о**Я** об ще ни е**Я**». Для формирования ключевой таблицы выбирается лозунг и далее она заполняется по правилам шифрующей системы Трисемуса. Например, лозунг «ДЯДИНА» 

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		Рис.6. Ключевая таблица для шифра Playfair Затем, руководствуясь следующими правилами, выполняется зашифровывание пар символов исходного текста: 1. Если символы биграммы исходного текста встречаются в одной строке, то эти символы замещаются на символы, расположенные в ближайших столбцах справа от соответствующих символов. Если символ является последним в строке, то он заменяется на первый символ этой же строки. 2. Если символы биграммы исходного текста встречаются в одном столбце, то они преобразуются в символы того же столбца, находящимися непосредственно под ними. Если символ является нижним в столбце, то он заменяется на первый символ этого же столбца. 3. Если символы биграммы исходного текста находятся в разных столбцах и разных строках, то они заменяются на символы, находящиеся в тех же строках, но соответствующие другим углам прямоугольника. Пример шифрования. - биграмма «за» формирует прямоугольник – заменяется на «жб»; - биграмма «ши» находятся в одном столбце – заменяется на «юе»; - биграмма «фр» находятся в одной строке – заменяется на «хс»; - биграмма «ов» формирует прямоугольник – заменяется на «йж»; - биграмма «ан» находятся в одной строке – заменяется на «ба»; - биграмма «но» формирует прямоугольник – заменяется на «ам»;

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		- биграмма «ес» формирует прямоугольник – заменяется на «гт»; - биграмма «оя» формирует прямоугольник – заменяется на «ка»; - биграмма «об» формирует прямоугольник – заменяется на «па»; - биграмма «ще» формирует прямоугольник – заменяется на «шё»; - биграмма «ни» формирует прямоугольник – заменяется на «ан»; - биграмма «ея» формирует прямоугольник – заменяется на «ги». Шифрограмма – «жб юе хс йж ба ам гт ка па шё ан ги». Для расшифровки необходимо использовать инверсию этих правил, откидывая символы **Я** (или **Х**), если они не несут смысла в исходном сообщении. **3. Практическая часть** Зашифруйте свою фамилию с помощью следующих шифров: - шифра Цезаря; - лозунгового шифра; - полибианского квадрата; - шифрующей системы Трисемуса; - шифра Playfair;

Структурный элемент компетенции	Планируемые результаты обучения	Оценочные средства
		При оформлении отчета необходимо привести исходное сообщение (фамилию), таблицу шифрозамен, ключ (если таблица шифрозамен не является ключом) и зашифрованное сообщение.

б) Порядок проведения промежуточной аттестации, показатели и критерии оценивания:

Промежуточная аттестация проводится в форме зачёта.

При подготовке к зачету особое внимание следует обратить на следующие моменты:

1. Регулярное прочтение (не меньше трёх раз) и осмысление теоретического материала;
2. Выполнение практических заданий с опорой на теоретический комментарий и образцы;
3. Постоянную и добросовестную работу на практических занятиях, а также самостоятельную работу.

Критерии оценки (в соответствии с формируемыми компетенциями и планируемыми результатами обучения):

- на оценку **«отлично»** – студент должен показать высокий уровень знаний не только на уровне воспроизведения и объяснения информации, но и интеллектуальные навыки решения проблем и задач, нахождения уникальных ответов к проблемам, оценки и вынесения критических суждений;
- на оценку **«хорошо»** – студент должен показать знания не только на уровне воспроизведения и объяснения информации, но и интеллектуальные навыки решения проблем и задач, нахождения уникальных ответов к проблемам;
- на оценку **«удовлетворительно»** – студент должен показать знания на уровне воспроизведения и объяснения информации, интеллектуальные навыки решения простых задач;
- на оценку **«неудовлетворительно»** – студент не может показать знания на уровне воспроизведения и объяснения информации, не может показать интеллектуальные навыки решения простых задач.

8 Учебно-методическое и информационное обеспечение дисциплины (модуля)

а) Основная литература:

1. Вострецова, Е.В. Основы информационной безопасности : учебное пособие для студентов вузов / Е.В. Вострецова.— Екатеринбург : Изд-во Урал. ун-та, 2019.— 204 с — Режим доступа: http://elar.urfu.ru/bitstream/10995/73899/3/978-5-7996-2677-8_2019.pdf - Заголовок с экрана

2. Нестеров, С. А. Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров. — Москва : Издательство Юрайт, 2019. — 321 с. — Режим доступа: https://biblio-online.ru/viewer/informacionnaya-bezopasnost-434171#page/1 - Заголовок с экрана

3.Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 161 с. — Режим доступа: https://urait.ru/viewer/zaschita-informacii-422772#page/1- Заголовок с экран

б) Дополнительная литература:

1. Лось, А. Б. Криптографические методы защиты информации для изучающих ком-пьютерную безопасность : учебник для академического бакалавриата / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2019. — 473 с. — Режим доступа: https://biblio-online.ru/viewer/kriptograficheskie-metody-zaschity-informacii-dlya-izuchayuschih-kompyuternuyu-bezopasnost-447581#page/1 - Заголовок с экрана

2. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах : учебное пособие / В. Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2020. — 592 с. — Режим доступа:— https://znanium.com/read?id=358722

3. Сетевая защита информации. Лабораторный практикум : учебное пособие [для вузов] / Д. Н. Мазнин [и др.] ; Магнитогорский гос. технический ун-т им. Г. И. Носова. - Магнитогорск : МГТУ им. Г. И. Носова, 2019. - 1 CD-ROM. - Загл. с титул. экрана. - URL: https://magtu.informsystema.ru/uploader/fileUpload?name=3824.pdf&show=dcatalogues/1/1530260/3824.pdf&view=true (дата обращения: 27.08.2020). - Макрообъект. - ISBN 978-5-9967-1605-0. - Текст : электронный. - Сведения доступны также на CD-ROM.

4. Чернова, Е. В. Информационная безопасность : учебное пособие / Е. В. Чернова ; МГТУ. - [2-е изд., подгот. по печ. изд. 2011 г.]. - Магнитогорск : МГТУ, 2015. - 1 электрон. опт. диск (CD-ROM). - Загл. с титул. экрана. - URL: https://magtu.informsystema.ru/uploader/fileUpload?name=1453.pdf&show=dcatalogues/1/1123976/1453.pdf&view=true (дата обращения: 27.08.2020). - Макрообъект. - Текст : электронный. - Сведения доступны также на CD-ROM.

г) Программное обеспечение и Интернет-ресурсы:

Программное обеспечение:

Наименование ПО	№ договора	Срок действия лицензии
MS Windows 7	Д-1227 от 08.10.2018	11.10.2021
MS Office 2007 Professional	№ 135 от 17.09.2007	бессрочно
FAR Manager	свободно распространяемое	бессрочно
7Zip	свободно распространяемое	бессрочно

Базы данных, информационно-справочные системы, сайты:

1. Библиотека ФГБОУ ВПО «МГТУ» [Электронный ресурс]. Режим доступа: http://www.magtu.ru, свободный.
2. Web-сервер властных структур Российской Федерации [Электронный ресурс]. – Режим доступа: www.gov.ru, свободный.
3. Web-сервер Совета безопасности РФ [Электронный ресурс]. – Режим доступа: www.scrf.gov.ru, свободный.
4. Web-сервер Федерального агентства правительственной связи и информации при Президенте Российской Федерации [Электронный ресурс]. – Режим доступа: www.fagci.ru, свободный.
5. Web-сервер Государственной технической комиссии при Президенте Российской Федерации [Электронный ресурс]. – Режим доступа: www.infotecs.ru/gtc, свободный.
6. Сервер Государственной Думы Федерального Собрания РФ [Электронный ресурс]. – Режим доступа: www.duma.gov.ru, свободный.
7. Web-сервер Верховного Суда Российской Федерации [Электронный ресурс]. – Режим доступа: www.supcourt.ru, свободный.
8. Web-сервер подразделения по выявлению и пресечению преступлений, совершаемых с использованием поддельных кредитных карт, и преступлений, совершаемых путем несанкционированного доступа в компьютерные сети и базы данных [Электронный ресурс]. – Режим доступа: www.cyberpolice.ru, свободный.

9. Портал по информационной безопасности [Электронный ресурс]. – Режим доступа: www.infosecurity.report.ru, свободный.

10. Портал по информационной безопасности [Электронный ресурс]. – Режим доступа: www.void.ru, свободный.

11. Центр исследования компьютерной преступности [Электронный ресурс]. – Режим доступа: www.crime-research.ru, свободный.

12. Интернет и Право [Электронный ресурс]. – Режим доступа: www.internet-law.ru, свободный.

9 Материально-техническое обеспечение дисциплины (модуля)

Материально-техническое обеспечение дисциплины включает:

Учебные аудитории для проведения дистанционных занятий лекционного типа	Стол компьютерный, стол письменный, стул офисный, документ-камера Epson, источник бесперебойного питания POWERCOMIMD-1500AP , камера высокого разрешения, компьютер персональный (тип6), проектор ViewSonicPJD7526W, спикерфон настольный Calisto-620 Plantronics, веб-камера LogiteachC920, система акустическая настольная, стереогарнитура (микрофон с шумоподавлением), экраннастенныйDigis Optimal-C MW DSOC-11032*2
Учебные аудитории для проведения практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Стол компьютерный, стол письменный, стул офисный, документ-камера Epson, источник бесперебойного питания POWERCOMIMD-1500AP , камера высокого разрешения, компьютер персональный (тип6), проектор ViewSonicPJD7526W, спикерфон настольный Calisto-620 Plantronics, веб-камера LogiteachC920, система акустическая настольная, стереогарнитура (микрофон с шумоподавлением), экраннастенныйDigis Optimal-C MW DSOC-11032*2
Помещения для самостоятельной работы обучающихся	Персональные компьютеры с пакетом MS Office, выходом в Интернет и с доступом в электронную информационно-образовательную среду университета
Помещение для хранения и профилактического обслуживания учебного оборудования	Стеллажи для хранения учебно-наглядных пособий и учебно-методической документации.