МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

имени академика М.Д. Миллионщикова

«УТВЕРЖДАЮ»

Первый проректор

И.Г Гайрабеков

____

«01» 09 2020г.

РАБОЧАЯ ПРОГРАММА

дисциплины

«Защита информации»

Направление подготовки

09.03.01 «Информатика и вычислительная техника»

Направленность (профиль)

«Информатика и вычислительная техника»

Квалификация выпускника

Бакалавр

Грозный - 2020

1. Цели и задачи дисциплины

Дисциплина «Защита информации» предназначена для изучения принципов информационной безопасности, подходов к анализу его информационной инфраструктуры, принципов организации, проектирования и анализа систем защиты информации, освоения основ их комплексного построения на различных уровнях защиты.

Дисциплина закладывает набор базовых знаний, которые позволят выпускникам адаптироваться в условиях бурного развития информационных технологий. Обучение студентов данному курсу способствует воспитанию у них стремления к постоянному повышению профессиональной компетентности, расширению профессионального кругозора, умения ориентироваться в тенденциях и направлениях развития комплексной защиты информации.

Задачи дисциплины – дать знания:

- основ комплексного обеспечения защиты информации;
- основ организационно-правового обеспечения защиты информации.

2. Место дисциплины в структуре образовательной программы

Учебная дисциплина «Защита информации» относится к базовой части профессионального цикла по направлению подготовки 09.03.01 «Информатика и вычислительная техника».

Для освоения дисциплины «Защита информации» студенту необходимо знание следующих предшествующих дисциплин:

1. Основы алгоритмизации и программирования
2. Информатика
3. Операционные системы

Последующие дисциплины, для которых данная дисциплина является предшествующей:

1. Вычислительные машины, сети и телекоммуникации

2. Управление базами данных

3. Программирование

4. Теория кодирования информации

5. Информационные технологии

3.Требования к результатам освоения дисциплины

Выпускник, освоивший программу бакалавриата, должен обладать следующими компетенциями и индикаторами их достижения:

ОПК-1. Способен применять естественнонаучные и общеинженерные знания, методы математического анализа и моделирования, теоретического и экспериментального исследования в профессиональной деятельности

- **ИД-1 ОПК-1-знать**: основы высшей математики, физики, основы вычислительной техники и программирования
- **ИД-1 ОПК-1-уметь:** решать стандартные профессиональные задачи с применением естественнонаучных и общеинженерных знаний, методов математического анализа и моделирования.
- **ИД-1 ОПК-1-иметь навыки:** теоретического и экспериментального исследования объектов профессиональной деятельности.

ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно - коммуникационных технологий и с учетом основных требований информационной безопасности.

- **ИД-1 ОПК-3-знать**: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
- **ИД-1 ОПК-3-уметь:** решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
- **ИД-1 ОПК-3-иметь навыки:** подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.

4.**Объем дисциплины и виды учебной работы**

Таблица 1

Вид учебной работы	**Всего часов/ зач.ед.**
	ОФО
	3 семестр
Контактная работа (всего)	45/1,25
В том числе:	
Лекции	15/0,4
Лабораторные работы	30/0,8
Самостоятельная работа (всего)	**63/1,8**
В том числе:	
Курсовая работа (проект)	-
Расчетно-графические работы	-
Рефераты	20/0,5
Подготовка презентаций	10/0,3
И (или) другие виды самостоятельной работы:	-
Подготовка к лабораторным работам	13/0,4
Подготовка к практическим занятиям	-
Подготовка к зачету	20/0,6
Вид промежуточной аттестации	тесты
Вид отчетности	**Зачет**

Общая трудоемкость дисциплины	**ВСЕГО в часах**	**108**
	ВСЕГО в зач. ед.	**3**

5. Содержание дисциплины

5.1. Разделы дисциплины и виды занятий

Таблица 2

№ п/п	Наименование раздела дисциплины по семестрам	Лекц. зан. часы	Лаб. зан. часы	Всего часов
		ОФО	**ОФО**	**ОФО**
1.	ОСНОВНЫЕ ПОНЯТИЯ И АНАЛИЗ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	2	4	6
2.	Стандарты и спецификации в области информационной безопасности	2	4	6
3.	Политика безопасности	2	4	6
4.	Принципы криптографической защиты информации	2	4	6
5.	Криптографические алгоритмы	2	4	6
6.	Технологии аутентификации	2	4	6
7.	Обеспечение безопасности операционных систем	3	6	9
	Итого	15	30	45

5.2. Лекционные занятия

Таблица 3

№ п/п	Наименование раздела дисциплины	Содержание раздела
1.	ОСНОВНЫЕ ПОНЯТИЯ И АНАЛИЗ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	Основные понятия защиты информации и информационной безопасности. Понятие идентификации, аутентификации, авторизации. Анализ угроз информационной безопасности. Несанкционированный доступ к компьютерной информации Общие критерии безопасности. Цель и концепции общих критериев

2.	Стандарты и спецификации в области информационной безопасности	Критерии оценки надежных автоматизированных систем. Гармонизированные критерии европейских стран. Руководящие документы по защите информации Гостехкомиссии России. Другие стандарты в области информационной безопасности
3.	Политика безопасности	Основные понятия политики безопасности. Управленческие меры обеспечения информационной безопасности. Структура политики безопасности. Процедуры безопасности
4.	Принципы криптографической защиты информации	Основные понятия криптографической защиты. Симметричные и ассиметричные алгоритмы шифрования. Комбинированные криптосистемы шифрования
5.	Криптографические алгоритмы	Функции хэширования. Процедура формирования и проверки электронно-цифровой подписи. Управление крипто ключами
6.	Технологии аутентификации	Аутентификация и авторизация. Аутентификация на основе паролей. Строгая аутентификация. Биометрическая аутентификация.
7.	Обеспечение безопасности операционных систем	Угрозы безопасности операционных систем. Понятие защищенной ОС. Архитектура подсистемы защиты ОС. Правила разграничения доступа между пользователями

5.3. Лабораторные занятия

Таблица 4

№ п/п	Наименование раздела дисциплины	Наименование лабораторных занятий
1.	ОСНОВНЫЕ ПОНЯТИЯ И АНАЛИЗ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	***Лабораторная работа №1.***Разграничение прав пользователей
		Лабораторная работа №1.Разграничение прав пользователей - продолжение
		Лабораторная работа №1.Разграничение прав пользователей - продолжение
2.	Стандарты и спецификации в области информационной безопасности	***Лабораторная работа №2.***Реализация политики безопасности в защищенных версиях операционной системы Windows
		Лабораторная работа №2.Реализация политики безопасности в защищенных версиях операционной системы Windows - продолжение
		Лабораторная работа №2.Реализация политики безопасности в защищенных версиях операционной системы Windows - продолжение
3.	Политика безопасности	***Лабораторная работа №3.***Разграничение доступа к ресурсам в защищенных версиях операционной системы Windows

		Лабораторная работа №3.Разграничение доступа к ресурсам в защищенных версиях операционной системы Windows - продолжение
		Лабораторная работа №3.Разграничение доступа к ресурсам в защищенных версиях операционной системы Windows - продолжение
4.	Принципы криптографической защиты информации Криптографические алгоритмы	***Лабораторная работа №4.***Использование программной системы PGP для обеспечения конфиденциальности и целостности информационных ресурсов
		Лабораторная работа №4.Использование программной системы PGP для обеспечения конфиденциальности и целостности информационных ресурсов - продолжение
		Лабораторная работа №4.Использование программной системы PGP для обеспечения конфиденциальности и целостности информационных ресурсов - предложение
5.	Технологии аутентификации	***Лабораторная работа №5.***Использование программных средств контроля и анализа выполнения политики безопасности на примере операционной системы Windows XP/7
		Лабораторная работа №5.Использование программных средств контроля и анализа выполнения политики безопасности на примере операционной системы Windows XP/7 - продолжение
		Лабораторная работа №5.Использование программных средств контроля и анализа выполнения политики безопасности на примере операционной системы Windows XP/7 - продолжение
6.	Обеспечение безопасности операционных систем	***Лабораторная работа №6.*** Использование программного продукта Acronis. Восстановление данных.
		Лабораторная работа №6. Использование программного продукта Acronis. Восстановление данных - продолжение
		Лабораторная работа №6. Использование программного продукта Acronis. Создание резервной копии пространства памяти

5.4. Практические занятия (семинары): планом не предусмотрены

6.Самостоятельная работа студентов по дисциплине

Способ организации самостоятельной работы: подготовка презентаций

Тематика докладов для презентаций:

1. Анализ методов повышения надежности хранения информации на жестких магнитных дисках
2. ГОСТ Р ИСО/МЭК 15408 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий» Части 1, 2, 3

3. Анализ средств защиты от спама
4. Анализ методов обеспечения безопасности домашней сети
5. Анализ методов изучения поведения нарушителей безопасности компьютерных систем
6. Анализ методов перехвата паролей пользователей компьютерных систем и методов противодействия им
7. Сравнительный анализ антивирусных пакетов
8. Анализ методов обеспечения безопасности электронного магазина
9. Анализ методов организации антивирусной защиты компьютерных систем
10. Сравнительный анализ систем обнаружения атак
11. Анализ средств безопасности в пакете Microsoft Office
12. ГОСТ Р ИСО/МЭК ТО 15446 «Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности»
13. Сравнительный анализ средств защиты электронной почты
14. ГОСТ Р ИСО/МЭК ТО 19791 «Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем»

Учебно-методическое обеспечение для самостоятельной работы студентов:

1. Алексеев В.А. Методы и средства криптографической защиты информации : методические указания к проведению лабораторных работ по курсу «Методы и средства защиты компьютерной информации» / Алексеев В.А.. — Липецк : Липецкий государственный технический университет, ЭБС АСВ, 2019. — 16 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/17710.htm
2. Джонс К.Д. Инструментальные средства обеспечения безопасности : учебное пособие / Джонс К.Д., Шема М., Джонсон Б.С.. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 913 с. — ISBN 978-5-4497-0871-7. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/102011.html

7. Оценочные средства

Вопросы к рубежной аттестации

Вопросы к 1 –ой рубежной аттестации

1. Основные понятия защиты информации и информационной безопасности
2. Базовые свойства информации применительно к ИБ
3. Идентификация, аутентификация, авторизация
4. Анализ угроз ИБ
5. Признаки классификации угроз
6. НСД к информации. Способы получения НСД
7. Общие критерии безопасности
8. Концепции общих критериев
9. Политика безопасности организации
10. Распределение ролей и обязанностей администраторов и пользователей сети
11. Структура политики безопасности
12. Уровни политики безопасности
13. Процедуры безопасности

Вопросы к 2-ой рубежной аттестации

1. Основные понятия криптографической защиты информации
2. Симметричные криптосистемы шифрования
3. Ассиметричные криптосистемы шифрования
4. Электронная цифровая подпись и функция хэширования

5. Аутентификация, авторизация и администрирование действий пользователей
6. Аутентификация на основе паролей
7. Угрозы безопасности ОС
8. Понятие защищенной ОС
9. Основные функции подсистемы защиты ОС
10. Разграничение доступа к объектам ОС
11. Аудит
12. Технология межсетевых экранов
13. Функции МЭ
14. Дополнительные возможности МЭ
15. Проблемы безопасности МЭ.

Вопросы к зачету

1. Основные понятия защиты информации и информационной безопасности
2. Базовые свойства информации применительно к ИБ
3. Идентификация, аутентификация, авторизация
4. Анализ угроз ИБ
5. Признаки классификации угроз
6. НСД к информации. Способы получения НСД
7. Общие критерии безопасности
8. Концепции общих критериев
9. Политика безопасности организации
10. Распределение ролей и обязанностей администраторов и пользователей сети
11. Структура политики безопасности
12. Уровни политики безопасности
13. Процедуры безопасности
14. Основные понятия криптографической защиты информации
15. Симметричные криптосистемы шифрования
16. Ассиметричные криптосистемы шифрования
17. Электронная цифровая подпись и функция хэширования
18. Аутентификация, авторизация и администрирование действий пользователей
19. Аутентификация на основе многоразовых паролей
20. Аутентификация на основе одноразовых паролей
21. Аутентификация на основе PIN-кода
22. Угрозы безопасности ОС
23. Понятие защищенной ОС
24. Основные функции подсистемы защиты ОС
25. Разграничение доступа к объектам ОС
26. Аудит
27. Технология межсетевых экранов
28. Функции МЭ
29. Дополнительные возможности МЭ

Образец билета рубежной к I рубежной аттестации:

Грозненский Государственный Нефтяной Технический Университет
им. акад. М.Д. Миллионщикова
Кафедра «Информатика и вычислительная техника»
Дисциплина «Защита информации»
1-я рубежная аттестация
Группа: **Семестр:**
Билет № 1

1. Признаки классификации угроз
2. НСД к информации. Способы получения НСД

Преподаватель_____

Образец билета рубежной к II рубежной аттестации:

Грозненский Государственный Нефтяной Технический Университет
им. акад. М.Д. Миллионщикова
Кафедра «Информатика и вычислительная техника»
Дисциплина «Защита информации»
2-я рубежная аттестация
Группа: **Семестр:**
Билет № 2

1. Основные понятия криптографической защиты информации
2. Симметричные криптосистемы шифрования

Преподаватель_____

Образец билета к зачету:

Грозненский Государственный Нефтяной Технический Университет

им. акад. М.Д. Миллионщикова

Кафедра «Информатика и вычислительная техника»
Дисциплина «Защита информации»
Группа: **Семестр:**

Билет № 1

1. Основные понятия криптографической защиты информации
2. Симметричные криптосистемы шифрования
3. Ассиметричные криптосистемы шифрования

Подпись преподавателя_____ **Подпись заведующего кафедрой**_____

Текущий контроль

Образец типового задания для лабораторных занятий

Лабораторная работа № 1 Разграничение прав пользователей.

Цель: освоение основ криптографической защиты информации.

Задачи: ознакомление с методами шифрования, использование методов шифрования, дешифрования, освоение основных понятий.

Шифрова́ние — обратимое преобразование информации в целях сокрытия от неавторизованных лиц, с предоставлением, в это же время, авторизованным пользователям доступа к ней. Главным образом, шифрование служит задачей соблюдения конфиденциальности передаваемой информации. Важной особенностью любого алгоритма шифрования является использование ключа, который утверждает выбор конкретного преобразования из совокупности возможных для данного алгоритма. Пользователи являются авторизованными, если они обладают определённым аутентичным ключом. Вся сложность и, собственно, задача шифрования состоит в том, как именно реализован этот процесс. В целом, шифрование состоит из двух составляющих — зашифровывание и расшифровывание(дешифрование).

кодирование информации — процесс преобразования сигнала из формы, удобной для непосредственного использования информации, в форму, удобную для передачи, хранения или автоматической переработки.

ключ — секретная информация, используемая криптографическим алгоритмом при зашифровании/расшифровании сообщений, постановке и проверке цифровой подписи, вычислении кодов аутентичности (mac).

симметричное шифрование

В симметричных криптосистемах для шифрования и расшифровывания используется один и тот же ключ. Отсюда название — симметричные. Алгоритм и ключ выбирается заранее и известен обеим сторонам. Сохранение ключа в секретности является важной задачей для установления и поддержки защищённого канала связи. В связи с этим, возникает проблема начальной передачи ключа (синхронизации ключей). Кроме того существуют методы криптоатак, позволяющие так или иначе дешифровать информацию не имея ключа или же с помощью его перехвата на этапе согласования. В целом эти моменты являются проблемой криптостойкости конкретного алгоритма шифрования и являются аргументом при выборе конкретного алгоритма.

Асимметричное шифрование

В системах с открытым ключом используются два ключа — открытый и закрытый, связанные определённым математическим образом друг с другом. Открытый ключ передаётся по открытому (то есть незащищённому, доступному для наблюдения) каналу и

используется для шифрования сообщения и для проверки ЭЦП. Для расшифровки сообщения и для генерации ЭЦП используется секретный ключ.

Данная схема решает проблему симметричных схем, связанную с начальной передачей ключа другой стороне. Если в симметричных схемах злоумышленник перехватит ключ, то он сможет как «слушать», так и вносить правки в передаваемую информацию. В асимметричных системах другой стороне передается открытый ключ, который позволяет шифровать, но не расшифровывать информацию. Таким образом решается проблема симметричных систем, связанная с синхронизацией ключей.

Деятельность в области криптографии (шифрования) ограничена как при ее осуществлении на территории России, так и при ввозе и вывозе криптографических (шифровальных) средств. Регулирование деятельности в области криптографии на территории России осуществляется российскими нормативными правовыми актами, ввоз и вывоз криптографических средств регламентируется актами Евразийской экономической комиссии.

Органом, осуществляющим регулирование и контроль в сфере криптографии, является Федеральная служба безопасности (ФСБ России). Она вправе:

- осуществлять в соответствии со своей компетенцией регулирование в области разработки, производства, реализации, эксплуатации шифровальных (криптографических) средств и защищенных с использованием шифровальных средств систем и комплексов телекоммуникаций, расположенных на территории Российской Федерации, а также в области предоставления услуг по шифрованию информации в Российской Федерации, выявления электронных устройств, предназначенных для негласного получения информации, в помещениях и технических средствах;
- осуществлять государственный контроль за организацией и функционированием криптографической и инженерно-технической безопасности информационно-телекоммуникационных систем, сетей связи специального назначения и иных сетей связи, обеспечивающих передачу информации с использованием шифров, контроль за соблюдением режима секретности при обращении с шифрованной информацией в шифровальных подразделениях государственных органов и организаций на территории Российской Федерации и в ее учреждениях, находящихся за пределами Российской Федерации, а также в соответствии со своей компетенцией контроль за обеспечением защиты особо важных объектов (помещений) и находящихся в них технических средств от утечки информации по техническим каналам;

- разрабатывать, создавать и эксплуатировать информационные системы, системы связи и системы передачи данных, а также средства защиты информации, включая средства криптографической защиты.

Основной документ, регулирующий отношения, касающиеся шифрования - Приказ ФСБ РФ от 9 февраля 2005 г. "Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)"

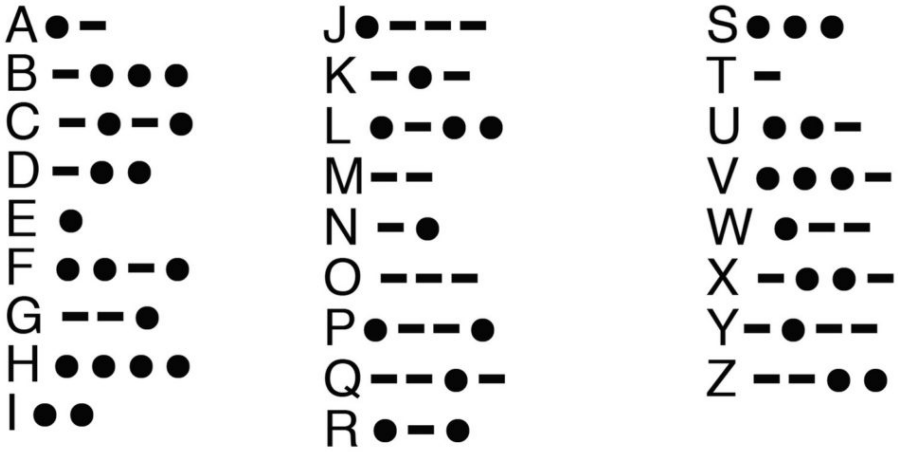
Методы шифрования. Ниже представлены некоторые методы шифрования. 1.Стеганография — это искусство скрытого письма. Этой технике даже больше лет, чем кодам и шифрованию. Например, сообщение может быть написано на бумаге, покрыто ваксой и проглочено с той целью, чтобы незаметно доставить его получателю. Другой способ — нанести сообщение на бритую голову курьера, подождать, пока волосы вырастут заново и скроют послание. Лучше всего для стеганографии использовать повседневные объекты. Когда-то в Англии использовался такой метод: под некоторыми буквами на первой странице газеты стояли крохотные точки, почти невидимые невооруженным глазом. Если читать только помеченные буквы, то получится секретное сообщение! Некоторые писали сообщение первыми буквами составляющих его слов или использовали невидимые чернила. Была распространена практика уменьшения целых страниц текста до размера буквально одного пикселя, так что их было легко пропустить при чтении чего-то относительно безобидного. Стеганографию лучше всего использовать в сочетании с другими методами шифрования, так как всегда есть шанс, что ваше скрытое послание обнаружат и прочитают.

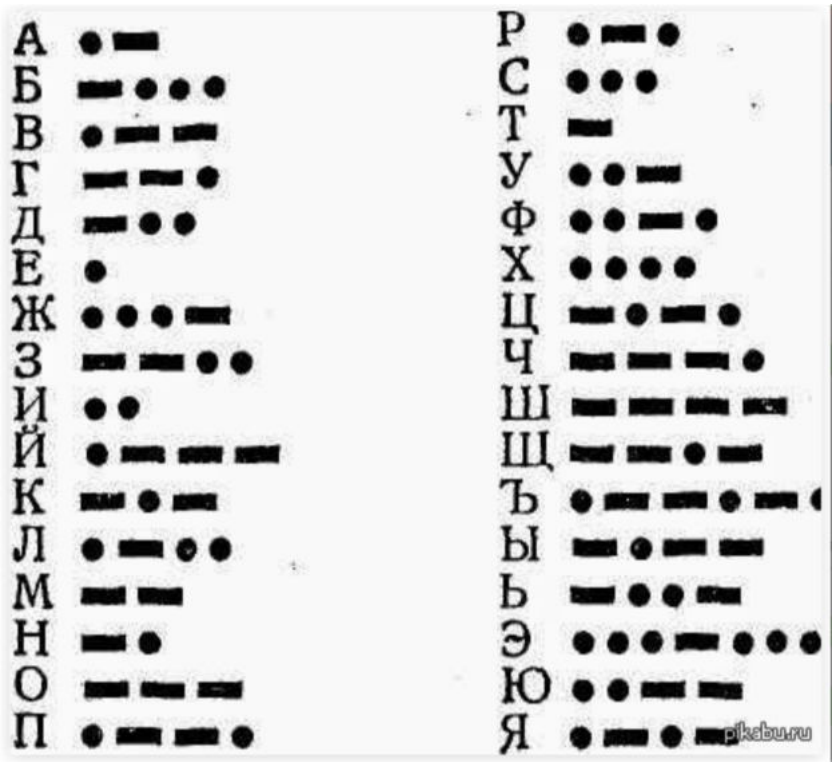
2.ROT1. Ключ прост: каждая буква заменяется на следующую за ней в алфавите. Так, A заменяется на B, B на C, и т.д. «ROT1» значит «ROTate 1 letter forward through the alphabet» (англ. «сдвиньте алфавит на одну букву вперед»). Сообщение «I know what you did last summer» станет «J lopx xibu zpv eje mbtu tvnnfs». Этот шифр весело использовать, потому что его легко понять и применять, но его так же легко и расшифровать. Из-за этого его нельзя использовать для серьезных нужд, но дети с радостью «играют» с его помощью. Задание: расшифровать следующее сообщение «mpoepo jt b dbqjubm»

3.Транспозиция. В транспозирующих шифрах буквы переставляются по заранее определенному правилу. Например, если каждое слово пишется задом наперед, то из «all the better to see you with» получается «lla eht retteb ot ees joy htiw». Другой пример — менять местами каждые две буквы. Таким образом, предыдущее сообщение станет «la tl eh eb tt re ot es ye uo iw ht». Подобные шифры использовались в Первую Мировую и Американскую Гражданскую Войну, чтобы посылать важные сообщения. Сложные ключи могут сделать такой шифр довольно сложным на первый взгляд, но многие сообщения, закодированные

подобным образом, могут быть расшифрованы простым перебором ключей на компьютере. Расшифровать: Лэ ме не ат рн о аВстно

4.Азбука Морзе. В азбуке Морзе каждая буква алфавита, все цифры и наиболее важные знаки препинания имеют свой код, состоящий из череды коротких и длинных сигналов, часто называемых «точками и тире». Так, А — это «•–», В — «–•••», и т.д. В отличие от большинства шифров, азбука Морзе используется не для затруднения чтения сообщений, а наоборот, для облегчения их передачи (с помощью телеграфа). Длинные и короткие сигналы посылаются с помощью включения и выключения электрического тока.





Расшифровать: .-. .- --.. --. .- -.. -.- .-

5.Шифр Цезаря, также известный как **шифр сдвига**, **код Цезаря** или **сдвиг Цезаря** — один из самых простых и наиболее широко известных методов шифрования.

Шифр Цезаря — это вид шифра подстановки, в котором каждый символ в открытом тексте заменяется символом, находящимся на некотором постоянном числе позиций левее или правее него в алфавите. Например, в шифре со сдвигом вправо на 3, А была бы заменена на Г, Б станет Д, и так далее. Если сопоставить каждому символу алфавита его порядковый номер (нумеруя с 0), то шифрование и дешифрование можно выразить формулами модульной арифметики[1][2]: y=(x+k) mod n x=(y-k) mod nгде x— символ открытого текста, y — символ шифрованного текста, n— мощность алфавита, а k — ключ. Пример: Шифрование с использованием ключа . Буква «Е» «сдвигается» на три буквы вперёд и становится буквой «З». Твёрдый знак, перемещённый на три буквы вперёд, становится буквой «Э», буква «Я», перемещённая на три буквы вперёд, становится буквой «В», и так далее: Исходный алфавит: А Б В Г Д Е Ё Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я

Шифрованный: Г Д Е Ё Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я А Б В

Оригинальный текст:

Съешь же ещё этих мягких французских булок, да выпей чаю.

Шифрованный текст получается путём замены каждой буквы оригинального текста соответствующей буквой шифрованного алфавита:

Фэзыя йз зьи ахлш пвёнлш чугрщцкфнлш дцосн, жг еютзм ъгб.

6.Шифр Виженера (фр. *Chiffre de Vigenère*) — метод полиалфавитного шифрования буквенного текста с использованием ключевого слова.[1]

Этот метод является простой формой многоалфавитной замены. Шифр Виженера изобретался многократно. Хотя шифр легко понять и реализовать, на протяжении трех столетий он противостоял всем попыткам его сломать; чем и заработал название **le chiffre indéchiffrable** (с французского 'неразгаданный шифр'). Многие люди пытались реализовать

схемы шифрования, которые по сути являлись шифрами Виженера.

Квадрат Виженера (рис1)

В шифре Цезаря каждая буква алфавита сдвигается на несколько позиций; например в шифре Цезаря при сдвиге +3, A стало бы D, B стало бы E и так далее. Шифр Виженера состоит из последовательности нескольких шифров Цезаря с различными значениями сдвига. Для зашифровывания может использоваться таблица алфавитов, называемая tabula recta или квадрат (таблица) Виженера (рис1). Применительно к латинскому алфавиту таблица Виженера составляется из строк по 26 символов, причём каждая следующая строка сдвигается на несколько позиций. Таким образом, в таблице получается 26 различных шифров Цезаря. На каждом этапе шифрования используются различные алфавиты, выбираемые в зависимости от символа ключевого слова. Например, предположим, что исходный текст имеет такой вид:

ATTACKATDAWN

Человек, посылающий сообщение, записывает ключевое слово («LEMON») циклически до тех пор, пока его длина не будет соответствовать длине исходного текста:

LEMONLEMONLE

Первый символ исходного текста ("A") зашифрован последовательностью L, которая является первым символом ключа. Первый символ зашифрованного текста ("L") находится на пересечении строки L и столбца A в таблице Виженера. Точно так же для второго символа исходного текста используется второй символ ключа; то есть второй символ зашифрованного текста ("X") получается на пересечении строки E и столбца T. Остальная часть исходного текста шифруется подобным способом.

Исходный текст: ATTACKATDAWN
Ключ: LEMONLEMONLE

Зашифрованный текст: LXFOPVEFRNHR

Расшифровывание производится следующим образом: находим в таблице Виженера строку, соответствующую первому символу ключевого слова; в данной строке находим первый символ зашифрованного текста. Столбец, в котором находится данный символ, соответствует первому символу исходного текста. Следующие символы зашифрованного текста расшифровываются подобным образом.

Если n — количество букв в алфавите, Mj — буквы открытого текста, Kj— буквы ключа, то шифрование Виженера можно записать следующим образом:

$$Cj=(Mj=Kj) \bmod n$$

И расшифровывание:

$$Mj=(Cj+N-Kj) \bmod n$$

В компьютере такая операция соответствует сложению кодов ASCII символов сообщения и ключа по некоторому модулю. Кажется, что если таблица будет более сложной, чем циклическое смещение строк, то шифр станет надежнее. Это действительно так, если ее менять чаще, например, от слова к слову. Но составление таких таблиц, представляющих собой латинские квадраты, где любая буква встречается в строке или столбце один раз, трудоемко и его стоит делать лишь на ЭВМ. Для ручного же многоалфавитного шифра полагаются лишь на длину и сложность ключа, используя приведенную таблицу, которую можно не держать в тайне, а это упрощает шифрование и расшифровывание.

7. **Использование кодов, таблиц соответствия**. Можно создать таблицу соответствия символов к алфавиту, содержание обеих таблиц может произвольным. Например, такую таблицу, в которой «*» означает какую-нибудь букву, например букву «Д», сочетание и варианты могут быть любыми.

Вопросы и задания к лабораторной работе. Для каждого метода шифрования придумать собственное произвольное зашифрованное сообщение. Знать принципы шифрования описанных методов.

1. Что такое шифрование?

2. Что такое кодирование?

3. В чем разница между кодированием и шифрованием?

4. Виды шифрования?

8. Учебно-методическое и информационное обеспечение дисциплины

Основная литература:

1. Башлы П.Н. Информационная безопасность и защита информации : учебное пособие / Башлы П.Н., Бабаш А.В., Баранова Е.К.. — Москва : Евразийский открытый институт, 2017. — 311 c. — ISBN 978-5-374-00301-7. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/10677.html
2. Фомин Д.В. Информационная безопасность : учебно-методическое пособие по дисциплине «Информационная безопасность» / Фомин Д.В.. — Саратов : Вузовское образование, 2018. — 54 c. — ISBN 978-5-4487-0298-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/77320.html
3. Артемов А.В. Информационная безопасность : курс лекций / Артемов А.В.. — Орел : Межрегиональная Академия безопасности и выживания (МАБИВ), 2018. — 256 c. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/33430.html

Дополнительная литература

1. Алексеев В.А. Методы и средства криптографической защиты информации : методические указания к проведению лабораторных работ по курсу «Методы и средства защиты компьютерной информации» / Алексеев В.А.. — Липецк : Липецкий государственный технический университет, ЭБС АСВ, 2019. — 16 c. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/17710.htm
2. Джонс К.Д. Инструментальные средства обеспечения безопасности : учебное пособие / Джонс К.Д., Шема М., Джонсон Б.С.. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 913 c. — ISBN 978-5-4497-0871-7. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/102011.html

9.Материально-техническое обеспечение дисциплины

Перечень материально-технических средств учебной аудитории для проведения занятий по дисциплине:

- учебная аудитория, доска;
- компьютеры с необходимым ПО;
- мультимедийный проектор;
- настенный экран.

Составитель:

Старший преподаватель кафедры «ИВТ» /М.З.Исаева/

СОГЛАСОВАНО:

Зав.кафедрой «ИВТ» / Э. Д. Алисултанова/

Директор ДУМР /Магомаева М.А./