МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования «Югорский государственный университет» (ЮГУ)
НЕФТЯНОЙ ИНСТИТУТ
(ФИЛИАЛ) ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО
ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
«ЮГОРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(НефтИн (филиал) ФГБОУ ВО «ЮГУ»)

ФИЛИАЛ ФГБОУ ВО «ЮГУ»
НЕФТЯНОЙ
ИНСТИТУТ

МДК.03.03
ФИЗИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ/ ОСНОВЫ ИНТЕЛЛЕКТУАЛЬНОГО ТРУДА

10.00.00 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
специальность 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Методические указания к выполнению практических занятий
для обучающихся 3 курса очной формы обучения
образовательных организаций
среднего профессионального образования

Нижневартовск, 2023

ББК 32.973+65.422.5
Ф 48

РАССМОТРЕНО
На заседании ПЦК «ЭТД»
Протокол № 09 от 18.11.2022 г.
Председатель Тен М.Б.

УТВЕРЖДЕНО
Председателем методического совета
НефтИн (филиала) ФГБОУ ВО «ЮГУ»
Хайбулина Р.И.
« 24 » января 2023 г.

Методические указания к выполнению практических занятий для обучающихся 3 курса очной формы обучения образовательных организаций среднего профессионального образования по МДК.03.03 Физические основы защиты информации / Основы интеллектуального труда специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем (10.00.00 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ), разработаны в соответствии с:

1. Федеральным государственным образовательным стандартом (далее – ФГОС) по специальности среднего профессионального образования (далее – СПО) 10.02.05 Обеспечение информационной безопасности автоматизированных систем;
2. Программой учебной дисциплины ПМ.03 Защита информации техническими средствами, утвержденной на методическом совете НефтИн (филиал) ФГБОУ ВО «ЮГУ» протокол № 4 от 31.08.2022 года.

Разработчик:
Садиков Денис Анифович, преподаватель НефтИн (филиал) ФГБОУ ВО «ЮГУ».

Рецензенты:
1. Тен М.Б., преподаватель НефтИн (филиал) ФГБОУ ВО «ЮГУ».
2. Третяк Б.П., ведущий специалист по ИТ ООО ЧОП «РН-Охрана».

Замечания, предложения и пожелания направлять в Нефтяной институт (филиал) федерального государственного бюджетного образовательного учреждения высшего образования «Югорский государственный университет» по адресу: 628615, Тюменская обл., Ханты-Мансийский автономный округ, г. Нижневартовск, ул. Мира, 37.

ВВЕДЕНИЕ

Методические указания к практическим занятиям по МДК.03.03 Физические основы защиты информации / Основы интеллектуального труда разработаны на основе рабочей программы в соответствии Федеральным государственным образовательным стандартом по специальности среднего профессионального образования 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Практические занятия служат важнейшим элементом учебного процесса, приобщают обучающихся к исследовательской работе, обогащают опытом и знаниями, необходимыми.

Целью методических указаний является закрепление теоретических знаний по дисциплине, развитие умения использовать приобретенные знания в профессиональной деятельности.

Методические указания рекомендованы к использованию в учебном процессе при подготовке специалистов по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем. Результат деятельности на практическом занятии – отчет о проделанной работе.

Защита: устный опрос по контрольным вопросам. Критерии оценивания: зачет/незачет.

Оценка «зачтено» выставляется, если работа выполнена в полном объеме с соблюдением необходимой последовательности. Обучающийся работает полностью самостоятельно: подбирает и применяет необходимые теоретические знания в практической деятельности. Дает правильные ответы на контрольные вопросы практической работы, делает выводы. Работа оформлена аккуратно, в наиболее оптимальной для фиксации результатов форме. Оценка «незачтено» ставится за невыполненное задание, или присутствуют существенные ошибки, неисправляемые даже с помощью преподавателя, наблюдается неумение применять знания в практической деятельности.

ТЕМАТИКА ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Номер темы	Номер и наименование занятия	Кол-во аудиторных часов	Формируемые компетенции
1.1	Практическое занятие № 1. Применение правовых основ использования организационных и технических средств защиты информации	10	ПК 3.1. - ПК 3.5., ОК 01 - ОК 10.
2.1	Практическое занятие № 2. Применение различных методов обеспечения информационной безопасности в операционных системах	4	ПК 3.1. - ПК 3.5., ОК 01 - ОК 10.
2.1	Практическое занятие № 3. Аутентификация в операционных системах	2	ПК 3.1. - ПК 3.5., ОК 01 - ОК 10.

2.1	Практическое занятие № 4. Разграничение доступа к защищаемым объектам	2	ПК 3.1. - ПК 3.5., ОК 01 - ОК 10.
2.1	Практическое занятие № 5. Аудит событий	2	ПК 3.1. - ПК 3.5., ОК 01 - ОК 10.
2.3	Практическое занятие № 6. Применение защитных мер безопасности вычислительных систем в корпоративной сети	10	ПК 3.1. - ПК 3.5., ОК 01 - ОК 10.
3.1	Практическое занятие № 7. Основные алгоритмы шифрования	8	ПК 3.1. - ПК 3.5., ОК 01 - ОК 10.
3.1	Практическое занятие № 8. Криптоанализ и атаки на криптосистемы	8	ПК 3.1. - ПК 3.5., ОК 01 - ОК 10.
3.1	Практическое занятие № 9. Управление ключами	8	ПК 3.1. - ПК 3.5., ОК 01 - ОК 10.
	Итого	54	

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ №1

ПРИМЕНЕНИЕ ПРАВОЫХ ОСНОВ ИСПОЛЬЗОВЫНИЯ ОРГАНИЗАЦИОННЫХ И ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Цель занятия: закрепление теоретических знаний в области правового обеспечения информационной безопасности.

Теоретические вопросы:

1. Понятие информационной безопасности.
2. Виды и источники угроз информационной безопасности РФ.
3. Методы обеспечения информационной безопасности РФ.
4. Основные направления обеспечения информационной безопасности.
5. Система защиты информации, содержащейся в информационной системе, защиты информации на предприятие.

Задание № 1. Разработать систему защиту информации в информационной системе на предприятии (выбор системы и предприятия произвольно).

Задание № 2. Проанализируйте Доктрину информационной безопасности Российской Федерации, утвержденной Президентом РФ от 5 декабря 2016 г. № 646 и определите основные направления обеспечения информационной безопасности в экономической сфере России.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ №2

ПРИМЕНЕНИЕ РАЗЛИЧНЫХ МЕТОДОВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗПАСНОСТИ В ОПЕРАЦИОННЫХ СИСТЕМАХ

Цель занятия: получение знаний о методах защиты информации,

которым подвергаются компьютерные системы и потерях банков.

Теоретический материал:

Одним из наиболее эффективных методов обеспечения информационной безопасности являются организационно-технические методы.

Что такое организационно-технические методы обеспечения информационной безопасности? Прежде всего, создание и совершенствование системы обеспечения информационной безопасности, разработка, использование и совершенствование СЗИ и методов контроля их эффективности.

Этот этап тесно связан с правовыми методами защиты информации, такими как лицензирование (деятельности в области защиты информации), сертификация средств защиты информации и применение уже сертифицированных, и аттестация объектов информатизации по требованиям безопасности информации.

А так же организационно технические методы связаны с экономическими, включающими в себя разработку программ обеспечения информационной безопасности Российской Федерации, определение порядка их финансирования, совершенствование системы финансирования работ, связанных с реализацией правовых и организационно-технических методов защиты информации, создание системы страхования информационных рисков.

Защита информации всегда является комплексным мероприятием. В совокупности, организационные и технические мероприятия позволяют предотвратить утечку информации по техническим каналам, предотвратить несанкционированный доступ к защищаемым ресурсам, что в свою очередь обеспечивает целостность и доступность информации при ее обработке, передаче и хранении. Так же техническими мероприятиями могут быть выявлены специальные электронные устройства перехвата информации, установленные в технические средства и защищаемое помещение.

Меры по охране конфиденциальности информации, составляющей коммерческую тайну (ФЗ 2004 г. № 98-ФЗ)

- определение перечня информации, составляющей коммерческую тайну;
- ограничение доступа к информации, составляющей коммерческую тайну,
- путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;
- учёт лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;
- регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;
- нанесение на материальные носители (документы), содержащие информацию, составляющую коммерческую тайну, грифа "Коммерческая

тайна" с указанием обладателя этой информации (для юридических лиц - полное наименование и место нахождения, для индивидуальных предпринимателей - фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).

Если говорить об экономической стороне защиты информации, всегда важно одно правило – стоимость системы защиты информации не должна превышать стоимость этой информации. Но это не единственное «но» в этом вопросе.

Нецелесообразно защищать всю информацию, какую можем, и все каналы информации какие только есть. Для этого необходимо определить объект защиты.

Основными объектами защиты являются речевая информация и информация, обрабатываемая техническими средствами. Так же информация может быть представлена в виде физических полей, информативных электрических сигналов, носителей на бумажной, магнитной, магнито-оптической и иной основе. В связи с этим защите подлежат средства и системы информатизации, участвующие в обработке защищаемой информации (ОТСС), технические средства и системы, не обрабатывающие непосредственно информацию, но размещенные в помещениях, где она обрабатывается (ВТСС) и защищаемые помещения.

Порядок выполнения работы:

1. Скопировать папку Y:\ИБ на диск S:\
2. Создать в папке S:\ИБ каталоги 1, 2, 3, 4.
3. Запустить программу ArtMasker.exe
4. В диалоговом режиме выполнить все рекомендации Мастера (в качестве файла-контейнера выбрать) S:\ИБ\фото\Sky_01.bmp, в качестве маскируемого файла выбрать S:\Virus.doc, задайте параметры скрытия как средние
5. Сохраните замаскированный файл с именем Security_1.bmp в папке S:\ИБ\1
6. Выполнить обратные действия, сохранив размаскированный файл с именем Decod_1.doc в папке S:\ИБ\1
7. Переписать в тетрадь текст по описанию ArtMasker:

ArtMasker - эта программа может прятать информацию в рисунки (BMP 8bit, 16bit, 32bit) и музыкальные файлы (WAV 8bit 16bit). Уникальная возможность этой программы - установка параметров скрытия. Файл-контейнер не меняет своего размера. Имеется поддержка мультиязычности.

1. Запустить программу SimPass. Создать 5 паролей при помощи генератора, количество букв в пароле 10 (использовать специальные символы и латинские буквы). Выбрать любой понравившийся пароль и скопировать его в буфер.
2. Запустить программу Secret BMP (в качестве пароля использовать пароль – результат работы генератора паролей)
3. Создать **небольшой!!!!** растровый рисунок компьютерного вируса в

редакторе PAINT, сохранив его с именем S:\ИБ\2\Pic.bmp

4. Скрыть файл Pic.bmp в файле S:\ИБ\фото\Sky_02.bmp, сохранив новый файл с именем Security_2.bmp в папке S:\ИБ\2 (использовать сгенерированный пароль)

5. Выполнить обратные действия, сохранив извлеченный файл с именем Decod_2.bmp в папке S:\ИБ\2

6. Переписать в тетрадь текст по описанию Secret BMP и Simple Passwords:

Secret BMP - реализация методов стеганографии и криптографии для защиты данных, хранящихся в файлах любого формата. Методы стеганографии применяются для скрытия секретных данных внутри файла-контейнера. В качестве файла контейнера используются файлы растровых изображений формата bmp. Перед скрытием файла в файле-контейнере (bmp-картинке) файл шифруется с использованием метода гаммирования. Для получения гаммы в работе используется 32-разрядный генератор случайных чисел, который программно реализуем и позволяет получать псевдослучайное число.

Simple Passwords - программа для генерирования одновременно нескольких паролей из случайных символов. Позволяет выбрать символы, из которых должен состоять пароль - английские и русские, строчные и прописные, цифры и специальные. Можно указать количество символов в пароле и общее количество генерируемых паролей.

1. Запустить программу CriptograFF для реализации криптозащиты из файла в файл

2. Открыть файл для шифрования S:\ИБ\VIP.txt

3. Зашифровать данный файл, присвоив ему имя S:\ИБ\3\Security_3.scr

4. Выполнить обратные действия, сохранив расшифрованный файл с именем Decod_3.txt в папке S:\ИБ\3

5. Выполнить криптозащиту открытых файлов

6. В окне программы набрать текст, где перечислить программно-технические средства защиты информации

7. Зашифровать открытый файл с именем S:\ИБ\3\Metod.txt

8. Переписать в тетрадь текст по описанию CriptograFF

CriptograFF - шифрует текстовые файлы криптографическим методом. Предназначена для шифрования текстовых файлов по алгоритму RC4. Особенности данного алгоритма - большая скорость, возможность потокового шифрования, практическая невозможность вскрытия зашифрованного файла.

1. Запустить программу Signature Cryptographer

2. Зашифруйте файл S:\ИБ\фото\Sky_04.bmp, выбрав в качестве файла-ключа любой свой файл

3. Сохраните этот файл с именем S:\ИБ\\4\Security_4

4. Выполнить обратные действия, сохранив извлеченный файл с именем Decod_4.bmp в папке S:\ИБ\\4

5. Переписать в тетрадь текст по описанию Signature Cryptographer:

Signature Cryptographer - программа защиты информации в важных файлах от несанкционированного доступа. Шифровальщик использует в качестве ключа содержимое файлов вместо строки пароля. Таким образом, длина пароля может достигать гигантских размеров или вовсе быть больше длины шифруемого файла, что делает зашифрованный файл теоретически не взламываемым. Вместо длинных строк пароля запомнить нужно только имя файла, используемого для пароля.

1. Показать работу преподавателю, получить оценку, удалить с диска S:\ИБ

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ №3

АУТЕНТИФИКАЦИЯ В ОПЕРАЦИОННЫХ СИСТЕМАХ

Цель занятия: провести идентификацию и аутентификацию

Теоретический материал:

Аутентификация (Authentication) - процедура проверки подлинности заявленного пользователя, процесса или устройства. Эта проверка позволяет достоверно убедиться, что пользователь (процесс или устройство) является именно тем, кем себя объявляет. При проведении аутентификации проверяющая сторона убеждается в подлинности проверяемой стороны, при этом проверяемая сторона тоже активно участвует в процессе обмена информацией. Обычно пользователь подтверждает свою идентификацию, вводя в систему уникальную, неизвестную другим пользователям информацию о себе (например, пароль или сертификат).

Идентификация и аутентификация являются взаимосвязанными процессами распознавания и проверки подлинности субъектов (пользователей). Именно от них зависит последующее решение системы, можно ли разрешить доступ к ресурсам системы конкретному пользователю или процессу. После идентификации и аутентификации субъекта выполняется его авторизация.

Авторизация (Authorization) - процедура предоставления субъекту определенных полномочий и ресурсов в данной системе. Иными словами, авторизация устанавливает сферу действия субъекта и доступные ему ресурсы. Если система не может надежно отличить авторизованное лицо от неавторизованного, конфиденциальность и целостность информации в ней могут быть нарушены. Организации необходимо четко определить свои требования к безопасности, чтобы принимать решения о соответствующих границах авторизации.

С процедурами аутентификации и авторизации тесно связана процедура администрирования действий пользователя.

Пароль — это то, что знает пользователь и что также знает другой

участник взаимодействия. Для взаимной аутентификации участников взаимодействия может быть организован обмен паролями между ними

Инструкция по организации парольной защиты автоматизированной системы:

Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в автоматизированной системе ОРГАНИЗАЦИИ (АС ОРГАНИЗАЦИИ), а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

1. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах АС ОРГАНИЗАЦИИ и контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на сотрудников службы обеспечения безопасности информации (СОБИ) - администраторов средств защиты, содержащих механизмы идентификации и аутентификации (подтверждения подлинности) пользователей по значениям паролей.

2. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями автоматизированной системы самостоятельно с учетом следующих требований:

- длина пароля должна быть не менее 8 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях;
- личный пароль пользователь не имеет права сообщать никому.

Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

3. В случае, если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на уполномоченных сотрудников СОБИ. Для генерации «стойких» значений паролей могут применяться специальные программные средства. Система централизованной генерации и распределения паролей должна исключать возможность ознакомления самих уполномоченных сотрудников СОБИ, а также ответственных за информационную безопасность в подразделениях с паролями других сотрудников подразделений ОРГАНИЗАЦИИ (исполнителей).

4. При наличии в случае возникновении нештатных ситуаций, форс-

мажорных обстоятельств и т.п. технологической необходимости использования имен и паролей некоторых сотрудников (исполнителей) в их отсутствие, такие сотрудники обязаны сразу же после смены своих паролей их новые значения (вместе с именами соответствующих учетных записей) в запечатанном конверте или опечатанном пенале передавать на хранение ответственному за информационную безопасность подразделения (руководителю своего подразделения). Опечатанные конверты (пеналы) с паролями исполнителей должны храниться в сейфе. Для опечатывания конвертов (пеналов) должны применяться личные печати владельцев паролей (при их наличии у исполнителей), либо печать уполномоченного представителя службы обеспечения безопасности информации (СОБИ).

5. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в месяц.

6. Внеплановая смена личного пароля или удаление учетной записи пользователя автоматизированной системы в случае прекращения его полномочий (увольнение, переход на другую работу внутри территориального органа ОРГАНИЗАЦИИ и т.п.) должна производиться уполномоченными сотрудниками СОБИ – администраторами соответствующих средств защиты немедленно после окончания последнего сеанса работы данного пользователя с системой.

7. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри территориального органа ОРГАНИЗАЦИИ и другие обстоятельства) администраторов средств защиты и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой подсистем АС.

8. В случае компрометации личного пароля пользователя автоматизированной системы должны быть немедленно предприняты меры в соответствии с п.6 или п.7 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

9. Хранение сотрудником (исполнителем) значений своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у ответственного за информационную безопасность или руководителя подразделения в опечатанном личной печатью пенале (возможно вместе с персональными ключевыми дискетами и идентификатором Touch Memory).

10. Повседневный контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на ответственных за информационную безопасность в подразделениях (руководителей подразделений), периодический контроль – возлагается на сотрудников СОБИ – администраторов средств парольной защиты.

Контрольные вопросы:

1. Перечислить виды паролей.

2. От чего зависит надежность пароля?
3. Что такое парольная политика?

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ №4

РАЗГРАНИЧЕНИЕ ДОСТУПА К ЗАЩИЩАЕМЫМ ОБЪЕКТАМ

Цель занятия: ознакомиться с принципами построения VPN на базе программного обеспечения

Теоретические сведения:

VPN (англ. Virtual Private Network — виртуальная частная сеть) — обобщённое название технологий, позволяющих обеспечить одно или несколько сетевых соединений (логическую сеть) поверх другой сети (например, интернет).

Виртуальная частная сеть базируется на трех методах реализации:

Туннелирование;

Шифрование;

Аутентификация.

Hamachi— это программа, позволяющая создать виртуальную частную сеть (VPN) через Интернет и объединить в ней несколько компьютеров. После создания такой сети пользователи могут устанавливать VPN-сессии между собой и работать в этой сети точно так же, как в обычной локальной (LAN) сети с возможностью обмена файлами, удаленного администрирования компьютеров и т.д. Преимущество VPN-сети заключается в том, что она полностью защищена от несанкционированного вмешательства и невидима из Интернета, хотя и существует в нем.

Программа Hamachi должна быть установлена на всех компьютерах, которые предполагается объединить в виртуальную частную сеть.

Виртуальная сеть создается с помощью специализированного сервера Hamachi в Интернете.

После того как с помощью сервера Hamachi создается виртуальная сеть между выбранными компьютерами, обмен информацией между клиентами VPN-сети происходит уже напрямую, то есть без участия сервера Hamachi. Для обмена данными между клиентами VPN-сети используется протокол UDP.

Порядок выполнения работы:

1. Загрузить программу "LogMeIn Hamachi" с сайта http://hamachi.ru.softonic.com/ на оба компьютера будущей сети.
2. Создать сеть, пользуясь подсказками на сайте http://hamachiinfo.ru/nastrojka.html
3. Объединить в сеть принтер, камеру или другое устройство либо развернуть в сети какое-либо программное обеспечение (например, игру).

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ №5

АУДИТ СОБЫТИЙ

Цель занятия:

1. получить навыки по планированию аудита, определив какие события необходимо отслеживать;

2. научиться настраивать аудит для файлов, папок и принтеров;

3. научиться использовать оснастку Просмотр событий для выполнения различных заданий, связанных с просмотром журнала аудита и содержимым файлов журнала безопасности, а также для поиска определенных событий в файлах журналов.

Теоретические сведения:

Аудит позволяет проследить как действия пользователей, так и действия Windows, называемые событиями (events). С помощью аудита можно заставить Windows регистрировать события в журнале безопасности. Журнал безопасности (security log) поддерживает запись успешных и безуспешных попыток входа в систему и событий, связанных с созданием, открытием или удалением файлов, или других объектов. Запись аудита в журнале безопасности содержит следующую информацию: – выполненное действие; – имя пользователя, выполнившего действие; – успех или неудачу события, и указание, когда оно произошло.

Политика аудита (audit policy) определяет типы событий безопасности, которые Windows записывает в журнал безопасности на каждом компьютере. Журнал безопасности позволяет проследить события выборочно. Windows записывает событие в журнал безопасности на том компьютере, где оно произошло: например, каждый раз, когда кто-то пытается войти в систему, и это не удается.

Можно определить политику аудита для компьютера, чтобы:

– отследить успех и неудачу событий, таких как попытки входа пользователей, попытки определенного пользователя прочитать какой-либо файл, изменения учетной записи пользователя или членства в группах, изменения параметров безопасности;

– устранить или свести к минимуму риск несанкционированного использования ресурсов.

Для просмотра событий, записанных Windows в журнале безопасности, используется оснастка Event Viewer (**Просмотр событий**). Можно также архивировать журналы для отслеживания загрузки принтеров, открытия файлов, попыток несанкционированного использования ресурсов и др.

Планировать политику аудита — значит определиться, какие события нужно отслеживать, и на каких компьютерах следует конфигурировать аудит.

Можно отслеживать следующие типы событий:

– доступ к файлам и папкам;

– вход и выход из системы;

– выключение и перезагрузку компьютера;

– изменение учетных записей пользователей и групп;

– попытки изменять объекты в Active Directory (только в том случае, если компьютер с Windows входит в домен).

Отслеживание неудачных событий может предупредить о возможных, нарушениях безопасности. Например, если отмечено сразу несколько неудачных попыток входа в систему под определенной учетной записью пользователя, особенно, если это происходит в нерабочее время, то можно сделать вывод, что в систему пытается проникнуть злоумышленник.

Существуют следующие основные направления политики аудита.

– Определитесь, нужно ли отслеживать тенденции использования системы. Если да, то планируйте архивировать журналы событий. Это позволит, например, просмотреть, как используются системные ресурсы, и запланировать своевременное их расширение.

– Чаще просматривайте журналы безопасности. Вы должны составить расписание и регулярно следовать ему.

– Формируйте эффективную и хорошо управляемую политику аудита. Всегда ведите аудит использования конфиденциальных данных. Одновременно, отслеживайте только те события, которые дадут вам нужную информацию о сети. Это сведет к минимуму использование компьютерных ресурсов и облегчит поиск нужной информации. Тотальный аудит отрицательно отразится на производительности системы.

– Отслеживайте доступ к ресурсам участников группы Everyone (Все), а не только Users (Пользователи). Это гарантирует, что вы проверите каждого, кто может подключиться к сети, а не только пользователей, для которых созданы учетные записи в домене.

Настройка политики аудита.

Сначала надо выбрать типы наблюдаемых событий. Для каждого наблюдаемого события укажите, какие попытки нужно отслеживать

— успешные или неудачные. Эти параметры задают в окне Local Security Settings (Локальная политика безопасности), которое открывается выбором пункта Local Security Policy в меню Administrative Tools (Администрирование).

Аудит доступа к файлам и папкам.

Если вам необходимо контролировать нарушения безопасности, вы можете назначить аудит для файлов и папок в разделах NTFS. Для этого следует сначала определить политику аудита для доступа к объектам, включающим файлы и папки. Затем нужно активизировать аудит для конкретных файлов и папок и определить, какие типы доступа каких пользователей или групп отслеживать. Действуйте следующим образом.

1. На вкладке Security (Безопасность) окна свойств файла или папки щелкните кнопку Advanced (Дополнительно).

2. На вкладке Auditing (Аудит) щелкните кнопку Add (Добавить), выберите учетные записи пользователей, для которых надо контролировать доступ к файлам или папкам, и щелкните ОК.

3. В окне Audit Entry (Элемент аудита) пометьте флажок Successful (Успех) или Failed (Отказ) для событий, которые хотите отслеживать Щелкните ОК, чтобы вернуться в окно Access Control 'Settings. По умолчанию все изменения аудита, которые вы вносите в родительскую папку, применяются также ко всем дочерним папкам и всем файлам в родительских и дочерних папках.

4. Чтобы не допустить применение изменений, сделанных в родительской папке, к выбранным дочерним файлу или папке, сбросьте флажок Allow Inheritable Auditing Entries From Parent To Propagate To This Object (Переносить наследуемый от родительского объекта аудит на этот объект).

6. Щелкните ОК.

Аудит доступа к принтерам.

Для наблюдения доступа к принтерам, настройте политику аудита для доступа к объектам, включающим принтеры. Затем активизируйте аудит для конкретных принтеров и определите, какие типы доступа нужно отслеживать, и какие пользователи будут иметь такой доступ. После выбора принтера повторите те же самые шаги, что и для настройки аудита файлов и папок. Назначьте аудит для принтера следующим образом.

1. В окне свойств принтера перейдите на вкладку Security (Безопасность) и щелкните кнопку Advanced (Дополнительно).

2. На вкладке Auditing (Аудит). щелкните кнопку Add (Добавить), выберите соответствующих пользователей или группы, для которых вы хотите проверять доступ к принтеру, затем щелкните ОК.

3. В списке Apply Onto (Применять) окна Auditing Entry (Элемент аудита) выберите, где применяются параметры аудита.

4. В списке Access (Доступ) пометьте флажком Successful (Успех) или Failed (Отказ) события, которые хотите отслеживать.

Использование оснастки.

Просмотр событий Event Viewer используется для просмотра информации, содержащейся в журналах Windows. По умолчанию имеется три журнала доступных для просмотра

Журналы, поддерживаемые Windows.

Application log (Приложение) Содержит ошибки, предупреждения или информационные сообщения, связанные с работой некоторых программ, например, базы данных или электронной почты. Какие события будут отслеживаться, определяет разработчик программы.

Security log (Безопасность)Содержит информацию об успехе или неудаче отслеживаемых действий. Сюда записываются события согласно вашей политики аудита.

System log (Система) Содержит ошибки, предупреждения и информационные сообщения, генерируемые Windows.

Просмотр журналов безопасности.

Журнал безопасности содержит информацию о событиях, которые отслеживаются политикой аудита, например, успешные и неудачные попытки входа в систему. Вы можете просмотреть журнал безопасности следующим образом.

1. Раскройте меню Start\Programs\Administrative Tools (Пуск\Программы\Администрирование) и щелкните значок Event Viewer (Просмотр событий).

2. В дереве консоли выберите Security Log (Безопасность).

На правой панели окна Event Viewer появятся записи журнала и сводная информация для каждой из них. Успешные события помечены значком ключа, а неудачные — значком замка. Прочая информация включает дату и время, когда произошло событие, категорию события и учетную запись пользователя, вызвавшего событие.

Категория указывает тип события: например, доступ к объекту, управление учетными записями, доступ к службе каталогов или события входа.

Для просмотра дополнительной информации щелкните интересующее вас событие и в меню Action (Действие) выберите команду Properties (Свойства).

Windows записывает событие в журнал безопасности на компьютере, где произошло событие. Вы можете просмотреть эти события с любого компьютера, если имеете права администратора для этого компьютера. Для просмотра журнала безопасности на удаленном компьютере запустите MMC и создайте специальную консоль, куда добавьте оснастку Event Viewer (Просмотр событий), ссылающуюся на удаленный компьютер.

Поиск событий.

Когда вы впервые запускаете Event Viewer (Просмотр событий), автоматически отображаются все события, записанные в выбранном журнале. Для изменения появляющихся в журнале событий задействуйте команду Filter (Фильтр). Вы также можете вести поиск выбранных событий, используя команду Find (Поиск). Для сортировки или поиска событий запустите Event Viewer и выберите в меню View (Вид) команду Filter (Фильтр) или Find (Поиск).

Управление журналами аудита.

Вы можете отследить тенденции использования Windows путем архивирования журналов событий и сравнения журналов за разные периоды.

Это поможет планировать и контролировать использование ресурсов. Windows позволяет регулировать размер журналов и определять действия, предпринимаемые после заполнения журнала. Вы можете конфигурировать свойства каждого индивидуального журнала аудита. Для этого откройте окно свойств журнала в Event Viewer.

Используйте окно свойств для каждого типа журнала аудита, чтобы контролировать:

– размер журнала, который может варьироваться от 64 Кб до 4 194 240

Кб (4 Гб); по умолчанию он равен 512 Кб;

– действия, которые предпринимает Windows, когда журнал заполняется, путем изменения значений параметров Архивирование журналов безопасности позволяет вести хронику событий, связанных с безопасностью. Многие организации практикуют хранение архивов журналов в течение определенного периода времени для отслеживания информации, связанной с безопасностью.

Порядок выполнения работы:

Спланируйте политику аудита для вашего компьютера. Затем активизируйте аудит конкретных событий. Назначьте аудит файла и принтера. Просмотрите файл журнала безопасности и задайте параметры в окне Event Viewer (Просмотр событий) для перезаписи журнала событий после его заполнения. Спланируете политику аудита для вашего компьютера. Вы должны определить следующее:

– какие типы событий отслеживать;

– отслеживать успех события, неудачу, или и то, и другое.

Действуйте следующим образом:

– записывайте неудачные попытки регистрации в системе;

– записывайте попытки несанкционированного доступа к файлам из вашей БД;

– отслеживайте использование цветного принтера;

– отслеживайте все попытки вмешательства в аппаратное обеспечение компьютера;

– храните запись действий, выполняемых администратором для отслеживания неразрешенных изменений;

– отслеживайте процедуры резервного копирования для предотвращения кражи данных;

– отслеживайте неразрешенный доступ к важным объектам Active Directory.

Запишите ваши решения в следующую таблицу.

Отслеживаемое действие	**Успешное**	**Неудачное**
Вход в систему		
Управление учетными записями		
Доступ к службе каталогов		
События входа в систему		
Доступ к объектам		
Изменение политики		
Использование привилегий		
Отслеживание процессов		
Системные события		

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ №6

ПРИМЕНЕНИЕ ЗАЩИТНЫХ МЕР БЕЗОПАСНОСТИ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ В КОРПОРАТИВНОЙ СЕТИ

Цель занятия: изучить порядок вычисления и проверки ЭЦП (электронной цифровой подписи)

Теоретические сведения:

Программно-аппаратные средства защиты информации — это сервисы безопасности, встроенные в сетевые операционные системы. К сервисам безопасности относятся: идентификация и аутентификация, управление доступом, протоколирование и аудит, криптография, экранирование

В настоящее время повсеместное внедрение информационных технологий отразилось и на технологии документооборота внутри организаций и между ними, между отдельными пользователями. Все большее значение в данной сфере приобретает электронный документооборот, позволяющий отказаться от бумажных носителей (или снизить их долю в общем потоке) и осуществлять обмен документами между субъектами в электронном виде. Однако переход от бумажного документооборота к электронному ставит ряд проблем, связанных с обеспечением целостности (подлинности) передаваемого документа и аутентификации подлинности его автора.

Следует отметить, что известные в теории информации методы защиты сообщений, передаваемых по каналам связи, от случайных помех не работают в том случае, когда злоумышленник преднамеренно реализует угрозу нарушения целостности информации. Например, контрольные суммы, используемые для этой цели передатчиком и приемником, могут быть пересчитаны злоумышленником так, что приемником изменение сообщения не будет обнаружено. Для обеспечения целостности электронных документов и установления подлинности авторства необходимо использовать иные методы, отличные от контрольных сумм. Для решения данных задач используют технологию электронно-цифровой подписи.

Электронно-цифровая подпись (ЭЦП) сообщения является уникальной последовательностью, связываемой с сообщением, подлежащей проверке на принимающей стороне с целью обеспечения целостности передаваемого сообщения и подтверждения его авторства.

Процедура установки ЭЦП использует секретный ключ отправителя сообщения, а процедура проверки ЭЦП – открытый ключ отправителя сообщения (рис. 1). Здесь М – электронный документ, Е – электронно-цифровая подпись.

В технологии ЭЦП ведущее значение имеют однонаправленные функции хэширования. Использование функций хэширования позволяет формировать криптографически стойкие контрольные суммы передаваемых сообщений.

Функцией хэширования H называют функцию, сжимающую

сообщение произвольной длины M, в значение фиксированной длины H(M) (несколько десятков или сотен бит), и обладающую свойствами необратимости, рассеивания и чувствительности к изменениям. Значение H(M) обычно называют дайджестом сообщения M.

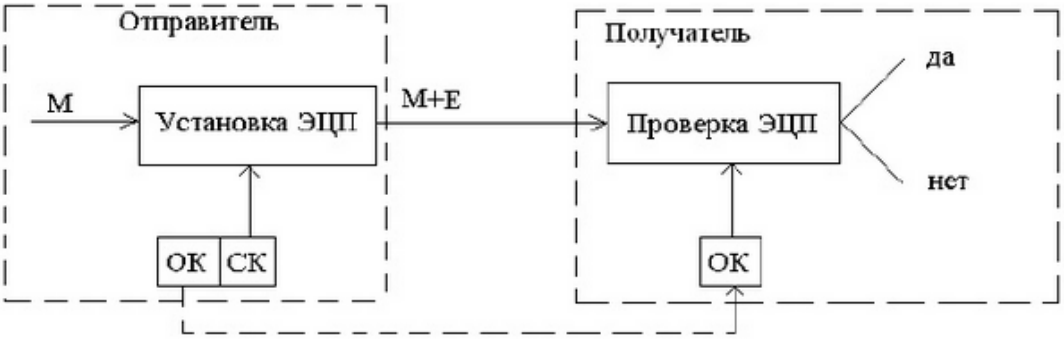

Рисунок 1 – Схема использования ЭЦП

Схема установки ЭЦП (рис. 2):

1. Для документа M формируется дайджест H с помощью заданного алгоритма хэширования.

2. Сформированный дайджест H шифруют на секретном ключе отправителя сообщения. Полученная в результате шифрования последовательность и есть ЭЦП.

3. Сообщение M и его ЭЦП передаются получателю сообщения.

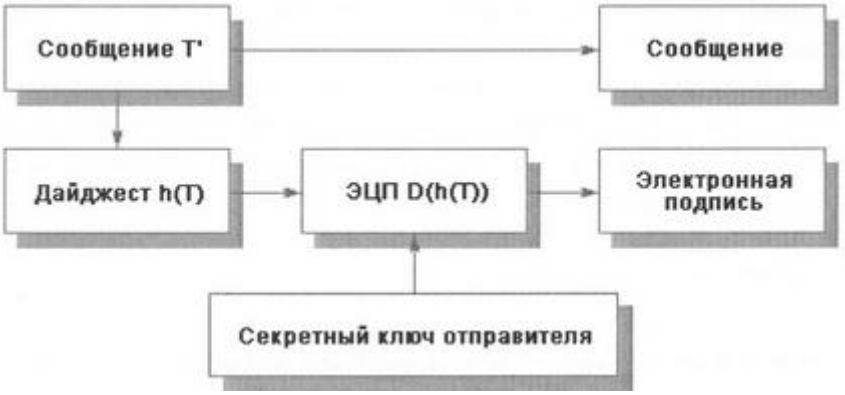

Рисунок 2 – Схема установки ЭЦП

Схема проверки ЭЦП (рис. 3):

1. Получатель для проверки ЭЦП должен иметь доступ к самому сообщению M и его ЭЦП.

2. Зная алгоритм хэширования, который был использован при установке ЭЦП, получатель получает дайджест H1 присланного сообщения M.

3. Зная открытый ключ отправителя, получатель дешифрует ЭЦП, в результате чего получает дайджест H2, сформированный на этапе установки ЭЦП.

4. Критерием целостности присланного сообщения M и подтверждения его автора является совпадение дайджестов H1 и H2. Если это равенство не выполнено, то принимается решение о некорректности ЭЦП.

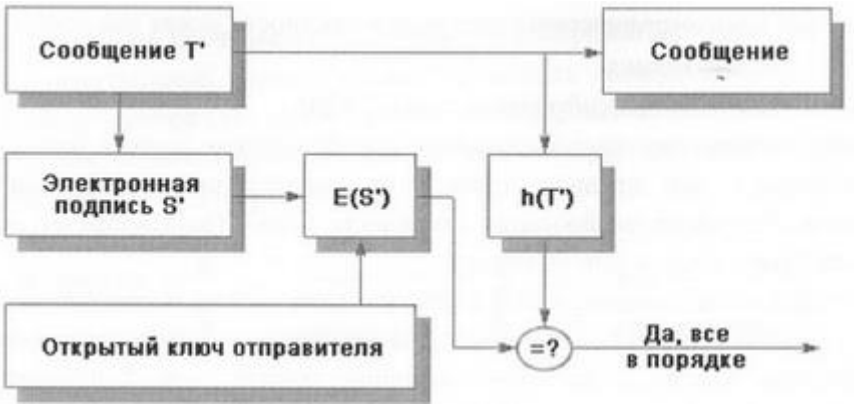

Рисунок 3 – Схема проверки ЭЦП

Задание. Сформировать ЭЦП к сообщению M' (см. вариант) и произвести проверку целостности принятого сообщения.

Порядок выполнения работы:

1. Разделить лист на две части: слева – сторона отправителя сообщения, справа – получателя.

2. На стороне отправителя выполнить следующие действия:

1. Записать сообщение M (см. вариант).

2. Сформировать профиль сообщения M’ с помощью упрощенной функции хэширования h(M’) – перемножения всех цифр кроме нуля этого сообщения.

3. Создать ЭЦП шифрованием профиля сообщения h(M’) закрытым ключом отправителя Da (значение ключа (d, n) см. в таблице с вариантами задания), т.е. Da (h(M’)) (см. вариант).

3. На стороне получателя выполнить следующие действия:

1. Записать сообщение M (его получает получатель вместе с ЭЦП) и ЭЦП Da (h(M’)).

2. Сформировать профиль принятого сообщения, M’ с помощью той же функции хэширования h(M’) – перемножения всех цифр кроме нуля этого сообщения (Получателю известен алгоритм хэширования, применяемый на стороне отправителя).

3. Создать профиль дешифрованием ЭЦП открытым ключем отправителя (Ea (Da (h(M’)) = h(M’)) (значение ключа (e, n) см. в таблице с вариантами задания).

4. Сравнить два профиля сообщения h(M’) (п.3.2 и 3.3). Убедиться в их совпадении.

Вариант – номер по списку в журнале.

Номер варианта	p	q	e	d	M
1	**2**	**3**	**4**	**5**	**6**
1	3	11	7	3	5523
3	17	11	7	23	8866
3	13	7	5	29	3565
4	101	113	3533	6597	6546
5	3	11	7	3	8562

1	2	3	4	5	6
6	17	11	7	23	9795
7	13	7	5	29	8462
8	17	11	7	23	7785
9	13	7	5	29	2123
10	101	113	3533	6597	3145
11	7	11	37	13	2566
12	101	113	3533	6597	3782
13	3	11	7	3	3465
14	17	11	7	23	3895
15	13	7	5	29	4132
16	17	11	7	23	5123
17	13	7	5	29	4416
18	101	113	3533	6597	7895
19	3	11	7	3	7459
20	17	11	7	23	5654
21	13	7	5	29	2456
22	17	11	7	23	3585
23	13	7	5	29	2652
24	101	113	3533	6597	5656
25	3	11	7	3	6685
26	17	11	7	23	5566
27	13	7	5	29	4652
28	17	11	7	23	8666
29	13	7	5	29	4556
30	101	113	3533	6597	9266

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ №7

ОСНОНЫЕ АЛГОРИТМЫ ШИФРОВАНИЯ

Цель занятия: изучить протоколирование и аудит, а также криптографические методы защиты. Показать их место в общей архитектуре безопасности.

Теоретические сведения:

Криптография – обеспечивает сокрытие смысла сообщения с помощью шифрования и открытия его расшифровкой, которые выполняются по специальным алгоритмам с помощью ключей.

Ключ – конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор только одного варианта из всех возможных для данного алгоритма.

Криптоанализ – занимается вскрытием шифра без знания ключа (проверка устойчивости шифра).

Кодирование – (не относится к криптографии) – система условных обозначений, применяемых при передаче информации. Применяется для увеличения качества передачи информации, сжатия информации и для

уменьшения стоимости хранения и передачи.

Криптографические преобразования имеют цель обеспечить недоступность информации для лиц, не имеющих ключа, и поддержание с требуемой надежностью обнаружения несанкционированных искажений.

Большинство средств защиты информации базируется на использовании криптографических шифров и процедур шифрования-расшифровки. В соответствии со стандартом ГОСТ 28147-89 под шифром понимают совокупность обратимых преобразований множества открытых данных на множество зашифрованных данных, задаваемых ключом и алгоритмом преобразования.

В криптографии используются следующие основные алгоритмы шифрования:

- алгоритм замены (подстановки) – символы шифруемого текста заменяются символами того же или другого алфавита в соответствии с заранее обусловленной схемой замены;
- алгоритм перестановки – символы шифруемого текста переставляются по определенному правилу в пределах некоторого блока этого текста;
- гаммирование – символы шифруемого текста складываются с символами некоторой случайной последовательности;
- аналитическое преобразование – преобразование шифруемого текста по некоторому аналитическому правилу (формуле).

Процессы шифрования и расшифровки осуществляются в рамках некоторой криптосистемы. Для симметричной криптосистемы характерно применение одного и того же ключа как при шифровании, так и при расшифровке сообщений. В асимметричных криптосистемах для шифрования данных используется один (общедоступный) ключ, а для расшифровки – другой (секретный) ключ.

Симметричные криптосистемы

Шифры перестановки

В шифрах средних веков часто использовались таблицы, с помощью которых выполнялись простые процедуры шифрования, основанные на перестановке букв в сообщении. Ключом в данном случае является размеры таблицы. Например, сообщение “Неясное становится еще более непонятным” записывается в таблицу из 5 строк и 7 столбцов по столбцам:

Н	О	Н	С	Б	Н	Я
Е	Е	О	Я	О	Е	Т
Я	С	В	Е	Л	П	Н
С	Т	И	Щ	Е	О	Ы
Н	А	Т	Е	Е	Н	М

Для получения шифрованного сообщения текст считывается по

строкам и группируется по 5 букв:

НОНСБ НЯЕЕО ЯОЕТЯ СВЕЛП НСТИЩ ЕОЫНА ТЕЕНМ

Несколько большей стойкостью к раскрытию обладает метод одиночной перестановки по ключу. Он отличается от предыдущего тем, что столбцы таблицы переставляются по ключевому слову, фразе или набору чисел длиной в строку таблицы. Используя в качестве ключа слово «ЛУНАТИК», получим следующую таблицу:

Л	У	Н	А	Т	И	К			А	И	К	Л	Н	Т	У
4	7	5	1	6	2	3			1	2	3	4	5	6	7
Н	О	Н	С	Б	Н	Я			С	Н	Я	Н	Н	Б	О
Е	Е	О	Я	О	Е	Т			Я	Е	Т	Е	О	О	Е
Я	С	В	Е	Л	П	Н			Е	П	Н	Я	В	Л	С
С	Т	И	Щ	Е	О	Ы			Щ	О	Ы	С	И	Е	Т
Н	А	Т	Е	Е	Н	М			Е	Н	М	Н	Т	Е	А

До перестановки После перестановки

В верхней строке левой таблицы записан ключ, а номера под буквами ключа определены в соответствии с естественным порядком соответствующих букв ключа в алфавите. Если в ключе встретились бы одинаковые буквы, они бы нумеровались слева направо. Получается шифровка:

СНЯНН БОЯЕТ ЕООЕЕ ПНЯВЛ СЩОЫС ИЕТЕН МНТЕА

Для обеспечения дополнительной скрытности можно повторно шифровать сообщение, которое уже было зашифровано. Для этого размер второй таблицы подбирают так, чтобы длины ее строк и столбцов отличались от длин строк и столбцов первой таблицы. Лучше всего, если они будут взаимно простыми.

Кроме алгоритмов одиночных перестановок применяются алгоритмы двойных перестановок. Сначала в таблицу записывается текст сообщения, а потом поочередно переставляются столбцы, а затем строки. При расшифровке перестановки проводятся в обратном порядке. Например, сообщение “Приезжаю_шестого” можно зашифровать следующим образом:

	2	4	1	3			1	2	3	4			1	2	3	4
4	П	Р	И	Е		4	И	П	Е	Р		1	А	З	Ю	Ж
1	З	Ж	А	Ю		1	А	З	Ю	Ж		2	Е	_	С	Ш
2	_	Ш	Е	С		2	Е.	_	С	Ш		3	Г	Т	О	О
3	Т	О	Г	О		3	Г	Т	О	О		4	И	П	Е	Р

Двойная перестановка столбцов и строк

В результате перестановки получена шифровка АЗЮЖЕ_СШГТООИ-ПЕР. Ключом к шифру служат номера столбцов 2413 и номера строк 4123 исходной таблицы.

Число вариантов двойной перестановки достаточно быстро возрастает с увеличением размера таблицы: для таблицы 3 х 3 их 36, для 4 х 4 их 576, а для 5*5 их 14400.

В средние века для шифрования применялись и магические квадраты. Магическими квадратами называются квадратные таблицы с вписанными в их клетки последовательными натуральными числами, начиная с единицы, которые дают в сумме по каждому столбцу, каждой строке и каждой диагонали одно и то же число. Для шифрования необходимо вписать исходный текст по приведенной в квадрате нумерации и затем переписать содержимое таблицы по строкам. В результате получается шифротекст, сформированный благодаря перестановке букв исходного сообщения.

16	3	2	13			О	И	Р	Т
5	10	11	8			З	Ш	Е	Ю
9	6	7	12			_	Ж	А	С
4	15	14	1			Е	Г	О	П

П	Р	И	Е	З	Ж	А	Ю	_	Ш	Е	С	Т	О	Г	О
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Число магических квадратов очень резко возрастает с увеличением размера его сторон: для таблицы 3*3 таких квадратов -1; для таблицы 4*4 - 880; а для таблицы 5*5-250000.

Шифры простой замены

Система шифрования Цезаря - частный случай шифра простой замены. Метод основан на замене каждой буквы сообщения на другую букву того же алфавита, путем смещения от исходной буквы на К букв.

Известная фраза Юлия Цезаря VENI VINI VICI – пришел, увидел, победил, зашифрованная с помощью данного метода, преобразуется в SBKF SFAF SFZF (при смещении на 4 символа).

Греческим писателем Полибием за 100 лет до н.э. был изобретен так называемый полибианский квадрат размером 5*5, заполненный алфавитом в случайном порядке. Греческий алфавит имеет 24 буквы, а 25-м символом является пробел. Для шифрования на квадрате находили букву текста и записывали в шифротекст букву, расположенную ниже ее в том же столбце. Если буква оказывалась в нижней строке таблицы, то брали верхнюю букву из того же столбца.

Шифры сложной замены

Шифр Гронсфельда состоит в модификации шифра Цезаря числовым

ключом. Для этого под буквами сообщения записывают цифры числового ключа. Если ключ короче сообщения, то его запись циклически повторяют. Шифротекст получают примерно также, как в шифре Цезаря, но отсчитывают не третью букву по алфавиту (как в шифре Цезаря), а ту, которая смещена по алфавиту на соответствующую цифру ключа.

Пусть в качестве ключа используется группа из трех цифр – 314, тогда

Сообщение: СОВЕРШЕННО СЕКРЕТНО

Ключ: 3143143143143143143

Шифровка: ФПИСЬИОССАХИЛФИУСС

В шифрах многоалфавитной замены для шифрования каждого символа исходного сообщения применяется свой шифр простой замены (свой алфавит):

	АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_
А	АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_
Б	_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ
В	Я_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮ
Г	ЮЯ_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭ
.	……
Я	ВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_АБ
_	БВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_А

Каждая строка в этой таблице соответствует одному шифру замены аналогично шифру Цезаря для алфавита, дополненного пробелом. При шифровании сообщения его выписывают в строку, а под ним ключ. Если ключ оказался короче сообщения, то его циклически повторяют. Шифротекст получают, находя символ в колонке таблицы по букве текста и строке, соответствующей букве ключа. Например, используя ключ АГАВА, из сообщения ПРИЕЗЖАЮ ШЕСТОГО получаем следующую шифровку:

Сообщение	ПРИЕЗЖАЮ_ШЕСТОГО
Ключ	АГАВААГАВААГАВАА
Шифровка	ПНИГЗЖЮЮЮАЕОТМГО

Гаммирование

Процесс шифрования заключается в генерации гаммы шифра и наложении этой гаммы на исходный открытый текст. Перед шифрованием открытые данные разбиваются на блоки $T(0)_i$ одинаковой длины (по 64 бита).

Гамма шифра вырабатывается в виде последовательности блоков $Г(ш)_i$ аналогичной длины ($Т(ш)_i$=$Г(ш)_i$+$Т(0)_i$, где + - побитовое сложение, i =1-m).

Процесс расшифровки сводится к повторной генерации шифра текста и наложение этой гаммы на зашифрованные данные $Т(0)_i$=$Г(ш)_i$+$Т(ш)_i$.

Асимметричные криптосистемы

Схема шифрования Эль Гамаля

Алгоритм шифрования Эль Гамаля основан на применении больших чисел для генерации открытого и закрытого ключа, криптостойкость же обусловлена сложностью вычисления дискретных логарифмов.

Последовательность действий пользователя:

1. Получатель сообщения выбирает два больших числа P и G, причем P G.

2. Получатель выбирает секретный ключ - случайное целое число X P.

3. Вычисляется открытый ключ $Y= G^x \bmod P$.

4. Получатель выбирает целое число K, 1P-1.

5. Шифрование сообщения (M): $a= G^K \bmod P$, $b=Y^K M \bmod P$, где пара чисел (a,b) является шифротекстом.

Криптосистема шифрования данных RSA

Предложена в 1978 году авторами Rivest, Shamir и Aldeman и основана на трудности разложения больших целых чисел на простые сомножители.

Алгоритм создания, открытого и секретного ключей:

1. Получатель выбирает 2 больших простых целых числа p и q, на основе которых вычисляет n=p*q и функцию Эйлера $\varphi(n)$=(p-1)(q-1).

2. Получатель выбирает целое число e (1e $\varphi(n)$), взаимно простое со значением функции $\varphi(n)$.

Пара чисел (e,n) публикуется в качестве открытого ключа.

1. Получатель вычисляет целое число d, которое отвечает условию: e*d=1(mod $\varphi(n)$).

Пара чисел (d,n) является секретным ключом.

Шифрование сообщения с использованием открытого ключа:

Если m – сообщение (сообщениями являются целые числа в интервале от 0 до n-1), то зашифровать это сообщение можно как $c=m^e \bmod(n)$.

Дешифрование сообщения с использованием секретного ключа:

Получатель расшифровывает, полученное сообщение c: $m=c^d \bmod (n)$.

Порядок выполнения работы:

Часть 1:

1. Используя один из алгоритмов симметричного шифрования (см. вариант), зашифровать свои данные: фамилию, имя, отчество.

2. Выполнить проверку, расшифровав полученное сообщение.

Часть 2:

1. Написать программу, реализующую алгоритм шифрования и дешифрования сообщения RSA. Входные данные: открытый и секретный ключи (значения n, e, d) и сообщение (m).

2. Используя заданные значения p, q, e, d (см. вариант) зашифровать и

дешифровать сообщения m_1, m_2, m_3 (см. вариант).

Вариант – номер по списку в журнале.

Номер варианта	Исходные данные							
	Часть 1	Часть 2						
	Алгоритм шифрования	p	q	e	d	$_1$	m_2	3
1	Простая перестановка	3	1	7	3	9	12	3
3	Одиночная перестановка	7	1	7	3	8	15	5
3	Двойная перестановка	3	7	5	9	3	16	5
4	Магический квадрат	01	13	533	597	6	19	3
5	Шифр Цезаря	7	1	7	3	8	18	1
6	Полибианский квадрат	7	7	5	7	9	11	6
7	Шифр Гронсфельда	3	1	7	3	8	13	5
8	Многоалфавитная замена	7	1	7	3	7	14	7
9	Простая перестановка	3	7	5	9	2	17	5
10	Одиночная перестановка	7	1	7	3	3	20	1
11	Двойная перестановка	3	7	5	9	2	12	5
12	Магический квадрат	01	13	533	597	3	15	6
13	Шифр Цезаря	7	1	7	3	3	16	4
14	Полибианский квадрат	7	7	5	7	3	19	6
15	Шифр Гронсфельда	3	1	7	3	4	18	5
16	Многоалфавитная замена	7	1	7	3	5	11	4
17	Простая перестановка	01	13	533	597	4	13	1
18	Одиночная перестановка	7	1	7	3	7	14	4
19	Двойная перестановка	7	7	5	7	7	17	3
20	Магический квадрат	3	1	7	3	5	20	3
21	Шифр Цезаря	7	1	7	3	2	11	5
22	Полибианский квадрат	3	7	5	9	3	13	7
23	Шифр Гронсфельда	7	1	7	3	2	14	9
24	Многоалфавитная замена	3	7	5	9	5	17	6
25	Простая перестановка	01	13	533	597	6	20	2

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ №8

КРИПТОАНАЛИЗ И АТАКИ КРИПТОСИСТЕМЫ

Цель занятия: изучить методы криптоанализа шифров перестановки.

Теоретические сведения:

Шифры перестановки, или транспозиции, изменяют только порядок следования символов или других элементов исходного текста. Классическим примером такого шифра является система, использующая карточку с отверстиями – решетку Кардано, которая при наложении на лист бумаги оставляет открытыми лишь некоторые его части. При зашифровке буквы сообщения вписываются в эти отверстия. При расшифровке сообщение вписывается в диаграмму нужных размеров, затем накладывается решетка, после чего на виду оказываются только буквы открытого текста. Решетки можно использовать двумя различными способами.

В первом случае зашифрованный текст состоит только из букв исходного сообщения. Решетка изготавливается таким образом, чтобы при ее последовательном использовании в различных положениях каждая клетка лежащего под ней листа бумаги оказалась занятой. Если такую решетку последовательно поворачивать на 90° после заполнения всех открытых при данном положении клеток, то при возврате решетки в исходное положение все клетки окажутся заполненными. Числа, стоящие в клетках, облегчают изготовление решетки. В каждом из концентрических окаймлений должна быть вырезана только одна клетка из тех, которые имеют одинаковый номер.

Второй, стеганографический метод использования решетки позволяет скрыть факт передачи секретного сообщения. В этом случае заполняется только часть листа бумаги, лежащего под решеткой, после чего буквы или слова исходного текста окружаются ложным текстом. Рассмотрим усложненную перестановку по таблице. Таблица представляет собой матрицу размерностью 6 х 6, в которую построчно вписывается искомое сообщение. При считывании информации по столбцам в соответствии с последовательностью чисел ключа получается шифротекст. Усложнение заключается в том, что некоторые ячейки таблицы не используются. При зашифровании сообщения КОМАНДОВАТЬ ПАРАДОМ БУДУ Я получим: ОЬБНАОДКДМУМВ АУ ОТР ААПДЯ, При расшифровании буквы шифротекста записываются по столбцам в соответствии с последовательностью чисел ключа, после чего исходный текст считывается по строкам. Для удобства запоминания ключа применяют перестановку столбцов таблицы по ключевому слову или фразе, всем символам которых ставятся в соответствие номера, определяемые порядком соответствующих букв в алфавите. Например, при выборе в качестве ключа слова ИНГОДА последовательность использования столбцов будет иметь вид 462531. Также возможны и другие варианты шифра перестановки, например, шифры столбцовой и двойной перестановки.

Порядок выполнения работы:

1.Дешифровать сообщение: Бирои имч еыеес витсч арзки танет есарл лпюсп мотоо еипнф кйаои крслт мн

2. Дешифровать сообщение: тиооско нцрпоед иявдттж афэелиа ткокнбв еапанъг уитриоб

3. Дешифровать сообщение: икинорткелэоидаржделлок

Контрольные вопросы.

1.Оценить надежность шифрования перестановкой

2.От чего зависит возможность успешного проведения криптоанализа шифров перестановки.

3. Насколько увеличивается сложность криптоанализа двойной перестановки.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ №9

УПРАВЛЕНИЕ КЛЮЧАМИ

Цель занятия: изучить алгоритм Диффи-Хелмана. Освоить методы генерации больших простых чисел и методы проверки больших чисел на простоту. Научиться строить первообразные корни по модулю n.

Теоретические сведения:

Генерация большого простого числа. Любая криптосистема основана на использовании ключей. Если для обеспечения конфиденциального обмена информацией между двумя пользователями процесс обмена ключами тривиален, то в системе, в которой количество пользователей составляет десятки и сотни, управление ключами – серьёзная проблема. Если не обеспечено достаточно надёжное управление ключевой информацией, то, завладев ею, злоумышленник получает неограниченный доступ ко всей информации. В этом случае необходимо введение какой-либо случайной величины в процесс шифрования. В частности, для реализации алгоритма RSA требуются большие простые числа. Считается, что вероятность выбора двумя людьми одного и того же большого простого числа пренебрежимо мала.

Существуют различные вероятностные проверки чисел на простоту, определяющие с заданной степенью достоверности, является ли число простым. При условии, что эта степень достоверности велика, такие способы достаточно хороши. Такие простые числа часто называют «промышленными простыми», т.е. они просты с контролируемой возможностью ошибки. В 1976 году американцы Уитфилд Диффи и Мартин Хеллман (Diffi W., Hellman M.) предложили новый принцип построения криптосистем. По их задумке, передачу от Алисы к Бобу сообщения можно было осуществить без передачи ключей, более того, не было необходимости скрывать метод шифрования. Предложенный принцип, в итоге, преобразовался в отдельную классификацию алгоритмов шифрования - шифрование с открытым ключом.

В поисках способов реализовать свою идею, Диффи и Хеллман пришли к использованию односторонних функций, т.е. функций, в которых получить исходное значение практически невозможно. Одна из таких функций в математике – вычисление по модулю.

Перейдем к рассмотрению самого алгоритма. Принцип простой. Сначала Алиса и Боб вместе выбирают большие простые числа n и g так, чтобы работало следующее соотношение: gxmod n. Эти два числа не нужно хранить в секрете, поэтому об использовании этих чисел Алиса и Боб могут договориться как им удобно (даже прийти в гости к Еве и выбрать эти числа при ней). Потом выполняются следующие действия:

1) Алиса выбирает случайное целое большое число x и присылает Бобу число X, полученное по формуле X = gxmod n.

2) Боб выбирает случайно целое большое число y и присылает Алисе

число Y, которое считается как Y = gymod n.

3) Алиса вычисляет число k1 = Yxmod n.

4) Боб вычисляет число k2 = Xymod n.

Нетрудно заметить, что и k1, и k2 равны gxymod n. Но ни Ева, ни кто-нибудь еще, кто прослушивал канал, не знают этого значения. Им известны только n, g, X и Y. Теоретически, Ева знает функцию и может вычислить k1 или k2, но, к сожалению для нее, эта функция является односторонней, и если Алиса и Боб могут выполнить обратное преобразование, поскольку обладают всеми необходимыми числами, то Еве будет очень сложно сделать тоже самое, а учитывая, что работа ведется с большими числами, - почти невозможно. Есть, конечно, одно «но». Выбор n и g довольно сильно влияет на безопасность системы. Следует выбирать n такое, чтобы (n-1)/2 было также простым, и, самое главное, чтобы n было большим: безопасность заключается в сложности разложения на множители чисел того же размера, что и n. Требования к выбору g не такие строгие, главное требование – оно должно быть примитивом mod n. В остальном же, оно может быть хоть одноразрядным простым числом.

Следует добавить, что алгоритм Диффи-Хеллмана успешно работает с тремя и более участниками, секретный ключ, после всех вычислений будет иметь вид k = gn1*n2*…*nNmod n, где n1..nN – переменные, закрепленные за каждым участником (x,y, z и т.д.). Алгоритм, как видно из заголовка, является алгоритмом обмена ключами, а не шифрования.

Порядок выполнения работы:

Произвести расчет ключа.

1. Совместно с удалённой стороной устанавливить открытые параметры p и g (обычно значения p и g генерируются на одной стороне и передаются другой), где p является случайным простым числом (p-1)/2 также должно быть случайным простым числом (для повышения безопасности) g является первообразным корнем по модулю p

2. Вычислить открытый ключ A, используя преобразование над закрытым ключом A = ga mod p для каждого студента.

3. Обменяться открытыми ключами с удалённой стороной

4. Вычислить общий секретный ключ K, используя открытый ключ удаленной стороны B и свой закрытый ключ a K = Ba mod p K получается равным с обеих сторон, потому что: B a mod p = (gb mod p)a mod p = g ab mod p = (ga mod p)b mod p = Ab mod p

5. Сравнить общие ключи.

Контрольные вопросы:

1. Для чего применяется алгоритм Диффи-Хеллмана?

2. Что такое модулярная математика?

3. Чем обеспечивается секретность получаемого ключа?

ПЕРЕЧЕНЬ РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

1. Белов Е. Б. Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студ. учреждений сред. проф. образования – М.: Издательский центр «Академия», 2017. – 336 с.

2. Баранова, Е. К. Информационная безопасность. История специальных методов криптографической деятельности: Учебное пособие / Баранова Е.К., Бабаш А.В., Ларин Д.А. - Москва: ИЦ РИОР, НИЦ ИНФРА-М, 2019. [Электронный ресурс; Режим доступа http://znanium.com]

3. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов; ответственный редактор Т. А. Полякова, А. А. Стрельцов. — Москва: Издательство Юрайт, 2022. — 325 с. — (Профессиональное образование). [Электронный ресурс; Режим доступа https://www.biblio-online.ru]

СОДЕРЖАНИЕ

МДК.03.03
ФИЗИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ/ ОСНОВЫ ИНТЕЛЛЕКТУАЛЬНОГО ТРУДА

10.00.00 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
специальность 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Методические указания к выполнению практических занятий для обучающихся 3 курса очной формы обучения образовательных организаций среднего профессионального образования

Методические указания
разработал преподаватель: Садиков Денис Анифович

Подписано к печати ***24.01.2023 г.*** Объем ***1,9*** п.л.
Формат 60х84/16 Заказ
Тираж ***1*** *экз.*

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования «Югорский государственный университет» (ЮГУ)
НЕФТЯНОЙ ИНСТИТУТ
(ФИЛИАЛ) ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «ЮГОРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
628615 Тюменская обл., Ханты-Мансийский автономный округ,
г. Нижневартовск, ул. Мира, 37.