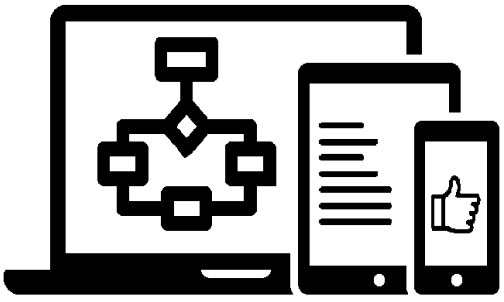
МЕЖГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«БЕЛОРУССКО-РОССИЙСКИЙ УНИВЕРСИТЕТ»

Кафедра «Программное обеспечение информационных технологий»

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Методические рекомендации к практическим занятиям для студентов специальности 1-28 01 02 «Электронный маркетинг» дневной и заочной форм обучения



Могилев 2023

УДК 004.4
ББК 32.973-018.2
О75

Рекомендовано к изданию
учебно-методическим отделом
Белорусско-Российского университета

Одобрено кафедрой «Программное обеспечение информационных технологий» «28» марта 2023 г., протокол № 9

Составители: доц. В. В. Кутузов;
ст. преподаватель Е. А. Зайченко

Рецензент доц. С. К. Крутолевич

Даны методические указания по выполнению практических работ по дисциплине «Основы информационной безопасности», а также приведены задания к ним и список литературы для подготовки.

Учебное издание

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Ответственный за выпуск	В. В. Кутузов
Корректор	Т. А. Рыжикова
Компьютерная верстка	Н. П. Полевничая

Подписано в печать . Формат 60×84/16. Бумага офсетная. Гарнитура Таймс.
Печать трафаретная. Усл. печ. л. . Уч.-изд. л. . Тираж 21 экз. Заказ №

Издатель и полиграфическое исполнение:
Межгосударственное образовательное учреждение высшего образования
«Белорусско-Российский университет».
Свидетельство о государственной регистрации издателя,
изготовителя, распространителя печатных изданий
№ 1/156 от 07.03.2019.
Пр-т Мира, 43, 212022, г. Могилев.

Содержание

1 Практическая работа № 1. Изучение законодательных и правовых основ информационной безопасности

Цель работы: ознакомление с законодательными правовыми актами по информационной безопасности.

Порядок выполнения работы

1 Изучить основные законодательные и правовые акты по информационной безопасности, сделав необходимые выписки в конспект.

2 Оформить отчет.

Основные теоретические положения

Конституция Республики Беларусь [1].

Концепция национальной безопасности Республики Беларусь [2].

Закон «Об информации, информатизации и защите информации» [3].

Закон «О государственных секретах» [4].

ТР 2013/027/BY «Информационные технологии. Средства защиты информации. Информационная безопасность» [5].

Закон «О защите персональных данных» [6].

Рекомендации Коллегии Евразийской экономической комиссии «Перечень стандартов и рекомендаций в области информационной безопасности, применяемых в рамках реализации цифровой повестки Евразийского экономического союза» [7] и многие другие законодательные акты, нормативные документы и распоряжения.

Практическое задание

Изучить основные законодательные и правовые акты по информационной безопасности.

Вопросы для контроля

1 Назовите основные законы по информационной безопасности.

2 Назовите основные приказы по информационной безопасности.

3 Как регулируются вопросы информационной безопасности в РБ?

2 Практическая работа № 2. Изучение законодательства Республики Беларусь о персональных данных

Цель работы: ознакомление с законодательными правовыми актами по персональным данным.

Порядок выполнения работы

1 Изучить Закон Республики Беларусь 7 мая 2021 г. № 99-З «О защите персональных данных».

2 Оформить отчет.

Основные теоретические положения

Закон «О защите персональных данных» [6].

Практическое задание

Изучить Закон Республики Беларусь 7 мая 2021 г. № 99-З «О защите персональных данных» (https://pravo.by/upload/docs/op/H12100099_1620939600.pdf).

Дать ответы на вопросы согласно варианту, выданному преподавателем (таблица 2.1). Ответ должен быть развернутым и обоснованным, в скобках необходимо указать ссылку на статью и пункт Закона № 99-З, например, (Ст. 4 п.7).

1 Что относится к персональным данным (ПД), согласно Закону № 99-З?
2 Кем распространяются общедоступные ПД?
3 Какие бывают виды ПД?
4 Что относится к биометрическим ПД?
5 В чем отличие биометрических и генетических ПД?
6 В чем отличие биометрических и специальных ПД?
7 В чем отличие блокирования и обезличивания ПД?
8 Включает ли обработка ПД их обезличивание?
9 В чем отличие удаления и обезличивания ПД?
10 Включает ли обработка ПД их удаление?
11 В чем отличие предоставления и распространения ПД?
12 Может ли быть субъектом ПД юридическое лицо?
13 Как может быть идентифицировано физическое лицо при отсутствии идентификационного номера?
14 Кто может быть уполномоченным лицом?
15 Может ли быть уполномоченным лицом физическое лицо?
16 Может ли быть уполномоченным лицом юридическое лицо?
17 Какие действия выполняет оператор ПД?
18 Кто может быть оператором?
19 Может ли быть оператором физическое лицо?
20 На какого рода отношения по защите ПД при их обработке регулирует Закон?

21 Распространяется ли Закон на защиту государственных секретов?

22 Чему должна быть соразмерна обработка ПД?

23 Требуется ли согласие субъекта ПД на их обработку?

24 Допустимо ли изменение в течение времени целей обработки ПД?

25 Допустим ли сбор ПД с избытком, «про запас»?

26 Что понимается под «прозрачностью» ПД?

27 Каким образом обеспечивается достоверность ПД?

28 Какое время должны храниться ПД в форме, позволяющей идентифицировать их субъекта?

29 Каким образом должно быть получено согласие субъекта ПД?

30 Всегда ли достаточно СМС-сообщения на согласие обработки ПД?

31 Всегда ли необходима письменная форма согласия на обработку ПД?

32 Всегда ли необходима электронная форма согласия на обработку ПД?

33 На кого возлагается обязанность доказать наличие согласия на обработку ПД?

34 Можно ли отозвать согласие на обработку ПД?

35 Перечислите пять случаев, когда согласие субъекта ПД на обработку не требуется.

36 Должны ли быть определены в договоре между оператором и уполномоченным лицом цели обработки ПД?

37 Должен ли быть определен в договоре между оператором и уполномоченным лицом перечень действий с ПД?

38 Должны ли быть определены в договоре между оператором и уполномоченным лицом обязанности по соблюдению конфиденциальности ПД?

39 Должны ли быть определены в договоре между оператором и уполномоченным лицом меры по обеспечению защиты ПД?

40 Должен ли субъект ПД обосновывать отзыв согласия на обработку ПД?

41 В какой форме субъект ПД должен обосновывать отзыв согласия на обработку ПД?

42 В какой срок субъект ПД должен обосновывать отзыв согласия на обработку ПД?

43 В какой срок оператор должен осуществить удаление ПД?

44 Какие действия должен предпринять оператор, если невозможно удаление ПД?

45 В какой срок оператор должен осуществить блокирование ПД?

46 Какие действия должен предпринять оператор после окончания срока действия договора, в соответствии с которым осуществлялась обработка ПД?

47 Если субъект ПД забыл, на какой срок он дал согласие на обработку ПД, как он может это узнать?

48 Может ли субъект ПД узнать, из какого источника оператор получил его ПД и на какой срок?

49 Может ли оператор отказаться сообщить субъекту ПД, из какого источника получены его ПД?

50 Что делать субъекту ПД, если его ПД изменились?

51 В какой срок после получения заявления субъекта оператор должен уведомить субъекта ПД об изменении или отказе?

52 Какие меры оператор обязан принимать по обеспечению защиты ПД?

53 Должна ли осуществляться криптографическая защита ПД?

54 Должен ли быть предоставлен доступ к документам, определяющим политику оператора через Интернет?

Таблица 2.1 – Вопросы по вариантам

Номер варианта	Номера вопросов
1	1, 2, 10, 21, 23, 29, 35, 36, 40, 47, 52
2	1, 3, 11, 20, 22, 30, 35, 37, 41, 48, 53
3	1, 4, 12, 21, 24, 31, 35, 38, 42, 49, 54
4	1, 5, 13, 20, 25, 32, 35, 39, 43, 50, 52
5	1, 6, 14, 21, 26, 33, 35, 36, 44, 51, 53
6	1, 7, 15, 20, 27, 34, 35, 37, 45, 47, 54
7	1, 8, 16, 21, 28, 29, 35, 38, 46, 48, 52
8	1, 2, 17, 20, 23, 30, 35, 39, 46, 49, 53
9	1, 3, 18, 21, 24, 31, 35, 36, 45, 50, 54
10	1, 4, 12, 20, 25, 32, 35, 37, 44, 51, 52
11	1, 5, 19, 21, 26, 33, 35, 38, 43, 47, 53
12	1, 6, 11, 20, 27, 34, 35, 39, 42, 48, 54
13	1, 7, 13, 21, 28, 33, 35, 36, 41, 49, 52
14	1, 8, 17, 20, 22, 32, 35, 37, 40, 50, 53
15	1, 9, 16, 21, 24, 33, 35, 38, 45, 51, 54

Вопросы для контроля

1 Кого касаются требования Закона № 99-З «О защите персональных данных»?

2 Необходимо ли получать от работников обязательство о неразглашении персональных данных?

3 Какая предусмотрена ответственность за нарушение законодательства о защите персональных данных?

4 Дайте определение терминов «субъект ПД», «оператор», «уполномоченное лицо».

3 Практическая работа № 3. Оценка рисков информационной безопасности организаций в соответствии с требованиями СТБ 34.101.70–2016

Цель работы: получение практических навыков по оценке рисков информационной безопасности в соответствии с требованиями СТБ 34.101.70–2016.

Порядок выполнения работы

1 Изучить основные теоретические положения СТБ 34.101.70–2016.

2 Получить задание у преподавателя, выполнить типовые задания.

3 Проанализировать возможные угрозы информационной безопасности, осуществить оценку рисков.

4 Оформить отчет.

Основные теоретические положения

Стандарт СТБ 34.101.70–2016 *Информационные технологии. Методы и средства безопасности. Методика оценки рисков информационной безопасности в информационных системах* устанавливает требования по выполнению процедуры оценки рисков информационной безопасности. Он содержит описание процесса оценки рисков информационной безопасности в информационных системах, рекомендации по выбору методов оценки рисков информационной безопасности, пример оценки рисков.

Для оценки рисков информационной безопасности рисков, кроме СТБ 34.101.70–2016, используются специализированные интернет-ресурсы, представленные в таблице 3.1.

Таблица 3.1 – Источники информации по теме работы

Документ, сайт	Описание
СТБ 34.101.70–2016 *Информационные технологии. Методы и средства безопасности. Методика оценки рисков информационной безопасности в информационных системах*	Представлена методика оценки рисков информационной безопасности в информационных системах. В приложении А СТБ 34.101.70–2016 приведен пример отчета оценки рисков информационной безопасности представлен
Система для корпоративных служб информационной безопасности. Реестр типов активов (https://service.securitm.ru/assettypes)	Реестр активов, угроз уязвимостей, описаний угроз, причин уязвимостей, источников уязвимостей
SECURITM система для корпоративных служб информационной безопасности (https://service.securitm.ru/)	Активы Угрозы Риски Уязвимости Защитные меры от угроз

Окончание таблицы 3.1

Документ, сайт	Описание
Банк данных угроз безопасности информации (https://bdu.fstec.ru/)	Представлены список угроз, описание угроз, источники угроз, объекты воздействия, последствия реализации угроз, объекты атак
Банк данных угроз безопасности информации. Модернизированный раздел угроз (https://bdu.fstec.ru/threat-section)	Перечень угроз безопасности информации
Банк данных угроз безопасности информации. Группы мер защиты информации (https://bdu.fstec.ru/threat-section/defenses)	Группы мер защиты информации
Банк данных угроз безопасности информации. Список уязвимостей (https://bdu.fstec.ru/vul?size=100)	Список уязвимостей в программном обеспечении
Банк данных угроз безопасности информации. Типовые уязвимости веб-приложений (https://bdu.fstec.ru/webvulns)	BDU:W01 – уязвимости, связанные с недостатками проверки вводимых данных BDU:W02 – уязвимости, связанные с недостатками управления доступом и защиты данных BDU:W03 – уязвимости, связанные с недостатками работы со структурами данных BDU:W04 – уязвимости, связанные с недостатками проверки подлинности BDU:W05 – уязвимости, связанные с недостатками управления ресурсами

Практическое задание

1 Осуществить оценку рисков информационной безопасности в информационных системах отдела предприятия или предприятия в целом в соответствии с требованиями СТБ 34.101.70–2016.

2 Оформить отчет в соответствии с примером оценки рисков информационной безопасности представленном в приложении А СТБ 34.101.70–2016.

Вопросы для контроля

1 Что такое риск информационной безопасности и как он может повлиять на организацию?

2 Какие примеры нарушений безопасности данных вы можете привести?

3 Какие меры следует принять, чтобы защитить конфиденциальность информации?

4 Каковы последствия нарушения информационной безопасности для бизнеса и как их можно предотвратить?

4 Практическая работа № 4. Хеширование информации

Цель работы: ознакомление с понятием хеширования, изучение криптографических хеш-функций.

Порядок выполнения работы

1 Изучить основные теоретические сведения об алгоритмах хеширования, их областях применения, достоинствах и недостатках.

2 Рассмотреть примеры применения хеширования в реальных системах.

3 Ознакомиться с популярными онлайн-сервисами для работы с хеш-функциями.

4 Произвести хеширование текста с использованием различных алгоритмов хеширования и оценить их стойкость.

5 Сделать выводы по результатам исследований.

6 Оформить отчет.

Основные теоретические положения

Понятие хеширования. Хеширование – преобразование входного массива данных в короткое число фиксированной длины (которое называется хешем или хеш-кодом) таким образом, чтобы, с одной стороны, это число было значительно короче исходных данных, а с другой – с большой вероятностью однозначно им соответствовало. Преобразование выполняется при помощи хеш-функции (рисунок 4.1). Ясно, что в общем случае однозначного соответствия между исходными данными и хеш-кодом быть не может. Обязательно будут возможны массивы данных, дающие одинаковые хеш-коды, но вероятность таких совпадений в каждой конкретной задаче должна быть сведена к минимуму выбором хеш-функции.

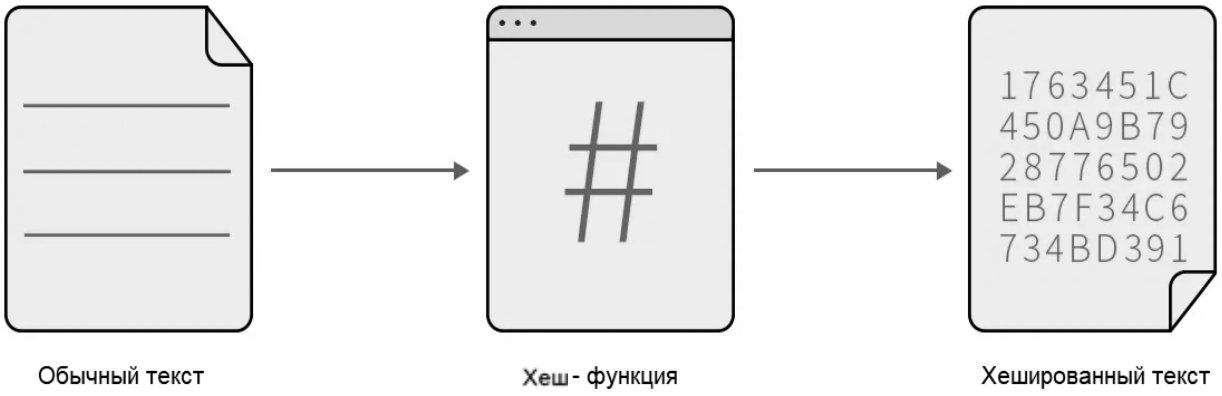


Рисунок 4.1 – Пример работы функции хеширования текст

Хеширование применяется для сравнения данных: если у двух массивов хеш-коды разные, массивы гарантированно различаются; если одинаковые – массивы, скорее всего, одинаковы. В общем случае однозначного соответствия

между исходными данными и хеш-кодом нет в силу того, что количество значений хеш-функций меньше, чем вариантов входного массива; существует множество массивов, дающих одинаковые хеш-коды – так называемые коллизии. Вероятность возникновения коллизий играет немаловажную роль в оценке качества хеш-функций.

Существует множество алгоритмов хеширования с различными характеристиками (разрядность, вычислительная сложность, криптостойкость и т. п.). Выбор той или иной хеш-функции определяется спецификой решаемой задачи.

Простым примером хеширования может служить нахождение циклической контрольной суммы или *CRC*, когда берётся текст (или другие данные) и суммируются коды входящих в него символов, а затем отбрасываются все цифры за исключением нескольких последних. Полученное число может являться примером хеш-кода исходного текста.

Контрольные суммы – несложные, крайне быстрые и легко реализуемые аппаратные алгоритмы, используемые для защиты от непреднамеренных искажений, в том числе ошибок аппаратуры.

По скорости вычисления они в десятки и сотни раз быстрее, чем криптографические хеш-функции, и значительно проще в аппаратной реализации.

Платой за столь высокую скорость является отсутствие криптостойкости, возможность подогнать сообщение под заранее известную сумму. Также обычно разрядность контрольных сумм (типичное число 32 бита) ниже, чем криптографических хешей (типичные числа 128, 160 и 256 бит), что означает возможность возникновения непреднамеренных коллизий.

Простейшим случаем такого алгоритма являются деление сообщения на 32- или 16-битные слова и их суммирование, что применяется, например, в *TCP/IP*.

Как правило, к такому алгоритму предъявляются требования отслеживания типичных аппаратных ошибок, таких как несколько подряд идущих ошибочных бит до заданной длины. Семейство алгоритмов так называемых «циклических избыточных кодов» удовлетворяет этим требованиям. К ним относится, например, *CRC32*, применяемый в аппаратуре *Ethernet* и в формате упакованных файлов *ZIP*.

Криптографические хеш-функции. Среди множества существующих хеш-функций принято выделять криптографически стойкие, применяемые в криптографии. Для того чтобы хеш-функция H считалась криптографически стойкой, она должна удовлетворять основным требованиям, на которых основано большинство применений хеш-функций в криптографии:

– необратимости (невозможность вычислить исходные данные по результату преобразования): для заданного значения хеш-функции m должно быть вычислительно неосуществимо найти блок данных X, для которого $H(X) = m$;

– стойкости к коллизиям (два различных набора данных должны иметь различные результаты преобразования): для заданного сообщения M должно быть вычислительно неосуществимо подобрать другое сообщение N, для которого $H(N) = H(M)$.

Следует отметить, что не доказано существование необратимых хеш-

функций, для которых вычисление какого-либо прообраза заданного значения хеш-функции теоретически невозможно. Обычно нахождение обратного значения является лишь вычислительно сложной задачей.

Применение хеш-функций. Хеш-функции также используются в некоторых структурах данных – хеш-таблицах, фильтрах Блума и декартовых деревьях. Требования к хеш-функции в этом случае другие: хорошая перемешиваемость данных; быстрый алгоритм вычисления.

Сверка данных. Это применение можно описать как проверку некоторой информации на идентичность оригиналу без использования оригинала. Для сверки используется хеш-значение проверяемой информации. Различают три основных направления этого применения: проверку на наличие ошибок; проверку парольной фразы; ускорение поиска данных.

Проверка на наличие ошибок. Например, контрольная сумма может быть передана по каналу связи вместе с основным текстом. На приёмном конце контрольная сумма может быть рассчитана заново, и её можно сравнить с переданным значением. Если будет обнаружено расхождение, то это значит, что при передаче возникли искажения и можно запросить повтор.

Хеширование используется в различных системах для обеспечения безопасности данных и защиты от несанкционированного доступа. **Областями применения хеширования могут быть следующие.**

1 Аутентификация пользователей: при регистрации пользователя в системе его пароль хешируется и сохраняется в базе данных. При последующей аутентификации система проверяет введенный пользователем пароль, хеширует его и сравнивает с сохраненным хеш-кодом.

2 Хранение паролей: хеширование используется для защиты паролей пользователей в базе данных. Это обеспечивает безопасность в случае утечки базы данных, т. к. злоумышленник не сможет получить исходные пароли.

3 Проверка целостности данных: хеширование применяется для проверки целостности данных, таких как файлы, сообщения и т. д. Если хеш-коды данных не совпадают, значит, данные были изменены.

4 Цифровая подпись: для защиты цифровых подписей от подделки используется хеширование. Хеш-код документа хешируется, а затем шифруется с использованием приватного ключа подписанта. Полученная цифровая подпись вместе с хеш-кодом документа позволяют проверить подлинность документа.

5 Криптовалюты: хеширование используется в блокчейн-технологии для обеспечения безопасности транзакций. Каждый блок содержит хеш-код предыдущего блока, что позволяет защитить цепочку блоков от изменений.

6 Защита программного обеспечения: хеширование используется для защиты программного обеспечения от несанкционированного доступа. Хешируется исполняемый файл программы, и если он изменен, программа перестает работать.

7 Безопасность интернет-соединений: хеширование используется в протоколах безопасности, таких как SSL/TLS, для защиты интернет-соединений и обеспечения конфиденциальности передаваемых данных.

8 Контроль доступа: хеширование используется для контроля доступа к ре-

сурсам, например, к файлам или к базе данных. Хеш-коды пользовательских паролей могут использоваться для определения прав доступа к конкретным ресурсам.

9 Хранение ключей: хеширование используется для защиты ключей шифрования и других конфиденциальных данных. Хеш-коды ключей могут быть использованы для защиты от их утечки или несанкционированного доступа.

10 Поиск данных: хеширование используется для быстрого поиска данных в больших базах данных. Хеш-коды данных могут быть использованы для быстрого определения, содержит ли база данных нужную информацию.

11 Защита от DoS-атак: хеширование используется для защиты от DoS-атак (атак, связанных с отказом в обслуживании), например, для защиты от атак на DNS-серверы. Хеш-коды запросов к серверу могут быть использованы для быстрой фильтрации нежелательного трафика.

12 Идентификация устройств: хеширование может быть использовано для идентификации устройств, например, в системах аутентификации Wi-Fi. Хеш-коды уникальных идентификаторов устройств могут быть использованы для проверки прав доступа к сети.

13 Поиск дубликатов: хеширование используется для быстрого поиска дубликатов файлов в больших коллекциях данных, таких как фотографии или музыкальные файлы. Хеш-коды файлов могут быть использованы для быстрого сравнения и определения, являются ли файлы идентичными.

14 Фильтрация спама: хеширование используется для фильтрации спама в электронной почте или на форумах. Хеш-коды сообщений могут быть использованы для быстрого определения, содержит ли сообщение спам или нет.

15 Контроль целостности системных файлов: хеширование используется для контроля целостности системных файлов в операционных системах. Хеш-коды файлов могут быть использованы для определения, были ли системные файлы изменены злоумышленниками.

16 Защита от подделки: хеширование используется для защиты от подделки документов, фотографий или других файлов. Хеш-коды файлов могут быть использованы для определения, является ли файл подлинным или был подделан.

17 Криптография: хеширование используется в криптографии для создания цифровых подписей и обеспечения непрерывности данных. Хеш-коды сообщений или данных могут быть использованы для создания цифровых подписей, которые обеспечивают подлинность и целостность данных.

18 Контроль версий: хеширование используется для контроля версий кода в системах контроля версий, таких как Git. Хеш-коды коммитов и файлов могут быть использованы для определения, были ли изменения внесены в код.

19 Анализ данных: хеширование используется для анализа больших объемов данных в различных областях, таких как медицинская диагностика, финансовый анализ и машинное обучение. Хеш-коды данных могут быть использованы для ускорения процесса анализа данных.

20 Децентрализованные сети: хеширование используется в децентрализованных сетях, таких как блокчейн. Хеш-коды транзакций могут быть использованы для создания блоков, которые затем добавляются в блокчейн.

21 Вычислительные системы: хеширование используется в вычислительных

системах для оптимизации производительности и ускорения вычислений. Хеш-таблицы могут быть использованы для быстрого поиска и доступа к данным.

22 Резервное копирование: хеширование используется для создания резервных копий данных и файлов. Хеш-коды файлов могут быть использованы для проверки целостности данных при восстановлении из резервной копии.

Наиболее известными алгоритмами хеширования являются: MD2 (Message Digest 2), MD5 (Message-Digest Algorithm 5), MD6 (MixHash6), SHA-1 (Secure Hash Algorithm 1), SHA-2 (Secure Hash Algorithm 2), SHA-3 (Secure Hash Algorithm 3), RIPEMD-160 (RACE Integrity Primitives Evaluation Message Digest 160), Whirlpool, BLAKE2, Bcrypt, Argon2, PBKDF2 (Password-Based Key Derivation Function 2), HMAC (Hash-based Message Authentication Code), GOST R 34.11-2012, Tiger, CRC (Cyclic Redundancy Check), IP Internet Checksum.

В системах аутентификации и идентификации обычно применяются криптографические алгоритмы хеширования для генерации хеш-кодов, которые используются для проверки целостности и подлинности данных, а также для хранения паролей и других конфиденциальных сведений без их фактического раскрытия. Некоторые из наиболее распространенных алгоритмов хеширования, используемых в системах аутентификации и идентификации, включают SHA-2 (Secure Hash Algorithm 2), bcrypt, PBKDF2 (Password-Based Key Derivation Function 2), scrypt, Argon2.

В настоящее время наиболее безопасными алгоритмами для хеширования паролей считаются Argon2, bcrypt и scrypt. Эти алгоритмы были разработаны специально для хеширования паролей и предлагают дополнительные механизмы защиты от атак типа словарного перебора, такие как использование соли, адаптивное время работы и комбинация хеш-функций и алгоритмов шифрования. SHA-2 и PBKDF2 также широко используются для хеширования паролей, но они не обладают некоторыми дополнительными механизмами безопасности, которые предлагают Argon2, bcrypt и scrypt.

В любом случае для обеспечения безопасности паролей необходимо также следовать другим безопасным практикам, таким как использование длинных и сложных паролей, регулярное изменение паролей, использование механизмов двухфакторной аутентификации и т. д.

В финансовой сфере применяются различные алгоритмы хеширования для обеспечения безопасности данных и защиты от несанкционированного доступа. Некоторые из наиболее распространенных алгоритмов хеширования, используемых в финансовой сфере, включают SHA-2 (Secure Hash Algorithm 2), HMAC (Hash-based Message Authentication Code), RSA (Rivest-Shamir-Adleman), AES (Advanced Encryption Standard), SHA-3 (Secure Hash Algorithm 3).

Эти алгоритмы используются в различных аспектах финансовой сферы, включая онлайн-банкинг, электронные платежи, торговлю ценными бумагами и другие операции, связанные с обработкой финансовых данных.

Онлайн-сервисы для работы с хеш-функциями

1 All Hash Generator (NTLM, MD2, MD4, MD5, MD6-128, MD6-256, MD6-512, RipeMD-128, RipeMD-160, RipeMD-256, RipeMD-320, SHA1, SHA3-224,

SHA3-256, SHA3-384, SHA3-512, SHA-224, SHA-256, SHA-384, SHA-512, CRC16, CRC32, Adler32, Whirlpool) – https://www.browserling.com/tools/all-hashes.

2 Online Hach Generator (Hash, CRC-16, CRC-32, MD2, MD4, MD5, SHA1, SHA224, SHA256, SHA384, SHA512, SHA512/224, SHA512/256, SHA3-224, SHA3-256, SHA3-384, SHA3-512, Keccak-224, Keccak-256, Keccak-384, Keccak-512, Shake-128, Shake-256) – https://emn178.github.io/online-tools/.

3 Online hash calculator (md2, md4, md5, sha1, sha224, sha256, sha384, sha512, ripemd128, ripemd160, ripemd256, ripemd320, whirlpool, tiger128,3, tiger160,3, tiger192,3, tiger128,4, tiger160,4, tiger192,4, snefru, snefru256, gost, gost-crypto, adler32, crc32, crc32b, fnv132, fnv1a32, fnv164, fnv1a64, joaat, haval128,3, haval160,3, haval192,3, haval224,3, haval256,3, haval128,4, haval160,4, haval192,4, haval224,4, haval256,4, haval128,5, haval160,5, haval192,5, haval224,5, haval256,5) – https://www.tools4noobs.com/online_tools/hash/.

4 Преобразование строк в хеш-функции (MD5, SHA1, SHA256, SHA384, SHA512, RIPE MD160) – https://convertstring.com/ru/Hash.

Онлайн-сервисы для поиска исходного текста по хешу.

1 Reverse hash decoder (md2, md4, md5, sha1, sha224, sha256, sha384, sha512, ripemd128, ripemd160, ripemd256, ripemd320, whirlpool, tiger128, tiger160, tiger192, tiger128.3, tiger160.3, tiger192.3, tiger128.4, tiger160.4, tiger192.4, snefru, snefru256, gost, adler32, crc32, crc32b, crc32b, fnv132, fnv164, fnv1a32, fnv1a52, fnv1a64, fnv1a128, fnv1a512, fnv1a1024, joaat, murmur3, djb2, sdbm, loselose, pearson, farmHashFingerprint32, farmHashFingerprint64, haval128.3, haval160.3, haval192.3, haval224.3, haval256.3, haval 128.4, haval160.4, haval192.4, haval224.4, haval256.4, haval128.5, haval160.5, haval192.5, haval224.5, haval256.5, md5x2, md5x3, md5x4, md5x5, base64 and other) – https://md5hashing.net.

2 Hashes. Поиск хешей для расшифровки (MD5, SHA1, MySQL, NTLM, SHA256, SHA512 и т. д.) – https://hashes.com/ru/decrypt/hash.

3 CMD5 encryption and decryption services (MD5, sha1, mysql, sha256) – https://www.cmd5.org.

Практическое задание

1 Выберите любой текстовый фрагмент (может быть статья, песня или абзац из книги).

2 Воспользуйтесь одним из предложенных онлайн-сервисов для генерации хешей различных алгоритмов хеширования (MD5, SHA-1, SHA-256 и SHA-512).

3 Запишите полученные хеш-коды и сравните их длину и уникальность.

4 Используйте онлайн-сервис для поиска исходного текста по хешу. Оцените стойкость разных алгоритмов хеширования к обратному преобразованию.

Вопросы для контроля

1 Что такое хеш-функция?

2 Когда хеш-функция является криптографически стойкой?

3 В чем состоит алгоритм контрольной суммы?

4 Перечислите требования к криптостойким хеш-функциям.

5 Назовите области применения хеш-функций.

6 Назовите алгоритмы хеширования, применяемые в финансовой сфере.

7 Назовите алгоритмы хеширования, применяемые в системах аутентификации и идентификации.

8 Расскажите про семейство алгоритмов хеширования MD (MD2, MD5, MD6).

9 Расскажите про семейство алгоритмов хеширования SHA (SHA-1, SHA-2, SHA-3).

5 Практическая работа № 5. Средства защиты документов Microsoft Office

Цель работы: изучение методов защиты документов MS Office, правил создания сложных паролей.

Порядок выполнения работы

1 Изучить основные теоретические положения, сделав необходимые выписки в конспект.

2 Получить задание у преподавателя, выполнить типовые задания.

3 Сделать выводы по результатам исследований.

4 Оформить отчет.

Основные теоретические положения

Начиная с версии 2007 в пакете офисных программ компании Microsoft введена функция «Центр управления безопасностью», доступ к которой осуществляется через меню «Файл» – «Параметры» – «Центр управления безопасности». Т. к. лента выглядит похоже во всех программах Office, действия, которые нужно выполнить, чтобы найти центр управления безопасностью, одинаковы для всех программ. Параметры, доступные в центре управления безопасностью, позволяют делиться документами с другими людьми, а также находить и удалять скрытые данные, которые вы не хотите сообщать другим.

Защита документа в Microsoft Word.

При работе в Microsoft Word существуют следующие возможностей ограничения изменений в документе:

- назначение пароля для открытия документа;
- назначение пароля разрешения записи;
- рекомендация доступа только для чтения;
- подготовка документа к проверке;
- защита полей электронной формы от изменения;
- назначение пароля разрешения записи;
- назначение документу пароля, предотвращающего открытие документа пользователем, не имеющим соответствующих полномочий.

Если открыть документ как файл, предназначенный только для чтения, и внести в него изменения, сохранить этот файл можно только под другим именем. Если после присвоения пароля он будет забыт, невозможно будет ни открыть документ, ни снять с него защиту, ни восстановить данные из него. Поэтому следует составить список паролей и соответствующих им документов и хранить его в надежном месте.

Назначение пароля для открытия документа.

Создайте документ Word. Выберите команду «Сохранить как» в меню Файл, выберите путь, куда сохранить файл (например, в папку Документы). Введите имя файла (любое), снизу на вкладке Сервис выберите Общие параметры. В поле Пароль для открытия файла введите пароль, а затем подтвердите пароль и нажмите кнопку OK. Нажмите кнопку Сохранить.

Назначение пароля разрешения записи.

Откройте документ. Выберите команду Сохранить как в меню Файл. Нажмите кнопку Параметры. В поле Пароль разрешения записи введите пароль, а затем нажмите кнопку OK. Затем введите тот же пароль еще раз и нажмите кнопку OK. Нажмите кнопку Сохранить.

Рекомендация доступа только для чтения.

Откройте документ. Выберите команду Сохранить как в меню Файл. Нажмите кнопку Параметры. Установите флажок «Рекомендовать доступ только для чтения» и нажмите кнопку OK. Нажмите кнопку Сохранить.

При рассылке документа для проверки можно запретить другим пользователям вносить любые изменения, кроме примечаний и записанных исправлений. Выберите команду Ограничить редактирование в меню Рецензирование, а затем в открывшемся справа меню поставить метку во втором пункте «Ограничения на редактирование» в раскрывающемся окне выбрать «Записи исправлений». Чтобы разрешить только вставку примечаний, выберите параметр Примечания.

Работа со скрытым текстом.

Порой требуется скрыть часть данных, содержащихся в документе, например, записанные исправления, примечания и скрытый текст.

Введите некоторый абзац текста, затем выделите его, затем правой кнопкой щелкните по выделению и выберете меню «Шрифт», поставьте метку в поле напротив «Скрытый». Чтобы увидеть скрытый текст, нажмите кнопку «Отобразить все знаки» в меню Главная.

Перед тем как предоставить другим лицам копию документа, целесообразно просмотреть скрытые данные и решить, что из них следует оставить их в документе. Например, может потребоваться временно скрыть часть данных при печати документа или удалить все скрытые данные из документа перед его распространением средствами электронной почты.

Если документ слишком велик, чтобы проверять его на наличие скрытых элементов вручную, можно воспользоваться встроенным инспектором документов. Для этого откройте меню Файл в нем Сведения, кликом по блоку «Поиск проблем» вызовите дополнительное меню, а в нем выберите опцию «Поиск скрытых свойств и персональных данных…». При этом редактор попросит вас

сохранить документ, после чего откроется окно инспектора, в котором вам нужно будет указать, какие именно элементы нужно искать. Перед тем как удалять скрытые элементы с помощью инспектора документов, создайте на всякий случай резервную копию файла, т. к. восстановить их вы уже не сможете.

Как быть, если документ со скрытым текстом нужно распечатать на принтере или преобразовать в PDF таким образом, чтобы он стал видимым? Ведь даже если вы отобразите его, на печать он все равно выведен не будет. Чтобы иметь возможность распечатывать скрытый текст, перейдите по цепочке Файл – Параметры – Экран и установите галочку «Печатать скрытый текст». Если открыть документ, сохраненный в режиме быстрого сохранения, как текстовый файл, в нем можно найти ранее удаленные данные. Это происходит потому, что при быстром сохранении вносимые изменения (в том числе удаление данных) дописываются в конец документа, не отражаясь в самом документе. Для окончательного удаления удаленных данных закройте текстовый файл и откройте документ как обычный документ Word. Выберите команду Сохранить как в меню Файл, а затем нажмите кнопку Сохранить. Чтобы вообще отключить быстрое сохранение, выберите команду Параметры в меню Файл, а затем снимите флажок Разрешить быстрое сохранение на вкладке Сохранение.

Для того чтобы предотвратить просмотр версий распространяемого документа достаточно выполнить следующее. Если нужно сохранить предыдущие версии, сохраните текущую версию как отдельный документ. Если не требуется сохранения предыдущих версий, удалите ненужные версии, а затем сохраните оставшийся документ.

Сохранение данных и восстановление утерянных документов.

Защитить себя от возможной потери результатов труда из-за сбоя в программе или отключения электричества можно с помощью автосохранения. Оно обеспечивает периодическое сохранение копий документа в процессе работы над ним или сохранение резервной копии документа при каждом сохранении конечного варианта. Чем чаще производится сохранение документа, тем большую часть его удастся восстановить в случае, если при работе в Word произойдет сбой в программе или падение напряжения в сети. Чтобы иметь возможность восстановить введенные данные после падения напряжения или сбоя в программе, необходимо заранее установить флажки Автосохранение каждые ... минут и/или Всегда сохранять резервную копию на вкладке Сохранение диалогового окна Параметры (меню Файл). Если необходимо, можно установить интервал для автоматического сохранения, меньший 10 мин. Чтобы иметь возможность восстановить данные после случайного удаления или повреждения документа, необходимо заранее установить флажок Всегда сохранять резервную копию. Кроме того, это позволит открыть и восстановить текст случайно поврежденного документа.

Использование автосохранения не избавляет от необходимости сохранять открытый документ обычным способом; временные файлы удаляются при закрытии или сохранении документа. В случае падения напряжения или после перезагрузки компьютера, если файл не был закрыт или сохранен, временные файлы сохраняются. При повторном запуске Word автоматически открываются

все временные файлы, и их можно сохранить. Если временный файл не сохранить, он удаляется.

Чтобы иметь возможность восстановить предыдущую версию документа после внезапного падения напряжения или другой аналогичной аварии, необходимо заранее установить флажок Всегда создавать резервную копию на вкладке Сохранение в диалоговом окне Параметры (меню Файл). Кроме того, перед этим документ должен быть сохранен хотя бы один раз.

Практическое задание

Откройте через «Файл» – «Параметры» – «Центр управления безопасностью» – «Параметры центра управления безопасностью» средство безопасности согласно варианту (таблица 5.1) и изучите справку (F1). Подготовьте документ «Отчет», в котором будут подробно описаны возможные настройки и назначение этого средства безопасности.

Добавьте в документ скрытый текст.

Установите на документ пароль, обеспечивающий заданный по варианту вид ограничения доступа. Не забудьте записать пароль в тетрадь, он понадобится при защите работы преподавателю.

Таблица 5.1 – Варианты индивидуальных заданий

Вариант	Средство безопасности	Вид ограничения доступа к документу
1	Надежные издатели	Пароль на открытие
2	Надежные расположения	Пароль на разрешение записи
3	Надежные документы	Пароль на открытие
4	Надстройки	Пароль на разрешение записи
5	Параметры ActiveX	Пароль на открытие
6	Параметры макросов	Пароль на разрешение записи
7	Защищенный просмотр	Пароль на открытие
8	Параметры блокировки файлов	Пароль на разрешение записи
9	Параметры конфиденциальности	Пароль на открытие
10	Параметры макросов	Пароль на разрешение записи

Вопросы для контроля

1 Какие возможности ограничения изменений в документе существуют в Microsoft Word?

2 Как выполнить проверку документа на наличие скрытого текста, свойств и персональных данных?

3 Как запретить другим пользователям вносить любые изменения в документ, кроме примечаний и записанных исправлений?

4 Как установить время автосохранения документа? На что оно влияет?

5 Как обеспечить возможность восстановления предыдущей версии документа в случае аварии или сбоя?

6 Практическая работа № 6. Архивирование и резервное копирование данных

Цель работы: ознакомление студентов с основными технологиями архивирования и резервного копирования данных, их преимуществами и недостатками, а также получение умений применять эти технологии в практических задачах.

Порядок выполнения работы

1 Изучить основные теоретические основы архивирования и резервного копирования данных.

2 Получить задание у преподавателя, выполнить типовые задания.

3 Сделать выводы по результатам исследований.

4 Оформить отчет.

Основные теоретические положения

В настоящее время вопросы защиты данных от несанкционированного доступа, модификации или уничтожения актуальны в связи с широким и повсеместным использованием средств вычислительной техники. Стоимость информации, хранящейся и обрабатываемой на компьютерах, может многократно превышать стоимость используемой вычислительной техники.

Стоимость информации, хранящейся в современных компьютерных системах, может многократно превышать стоимость самих компьютеров и программного обеспечения, необходимого для работы вычислительных машин, поэтому вопросам защиты информации в настоящее время уделяется особое внимание. Рассматривая проблемы надежной защиты данных, выделим две группы вопросов.

К первой группе отнесем вопросы обеспечения защиты от несанкционированного доступа к данным. Комплексное решение вопросов этой группы позволит обеспечить надежную защиту от злоумышленников, пытающихся получить доступ к защищаемой от них информации. Несанкционированное распространение закрытой информации, внесение изменений в наборы данных – все это может привести к возникновению серьезных проблем у предприятия, на котором произошел инцидент. В зависимости от степени серьезности инцидента могут иметь место как незначительные репутационные проблемы и финансовые потери, так и серьезнейшие проблемы, приводящие к негативному развитию ситуации вплоть до закрытия предприятия.

Актуальны вопросы защиты данных и для пользователей домашних компьютеров, которые в настоящее время практически все используют ресурсы сети Интернет (в виде постоянного или периодического подключения). В боль-

шинстве своем пользователи достаточно хорошо представляют себе угрозы, связанные с тем, что кто-то чужой получит доступ к компьютеру (человек-злоумышленник, атакующий выбранный им сетевой хост, или вирус, не нацеленный именно на этот конкретный компьютер, но заражающий исполняемые файлы, выполняемые под управлением той или иной операционной системы).

Как правило, на каждом компьютере установлена антивирусная программа, например, это может быть бесплатное решение Microsoft Security Essentials (для Windows 7) или Защитник Windows (Windows 8, Windows RT, Windows 8.1, Windows RT 8.1, Windows 10). Пользователь может использовать более сложную систему защиты, включающую в себя не только антивирусный функционал, но и средства, обеспечивающие безопасное подключение к компьютерным сетям, анализ входящего и исходящего трафика и т. д. В качестве примера отметим Kaspersky Internet Security для всех устройств – надежное и удобное решение для защиты, совместимое с операционными системами (ОС) Windows, Mac и Android. Используемая проактивная облачная защита в составе данного решения надежно защищает от вирусов, троянских и других вредоносных программ, от взаимодействия с опасными веб-сайтами, а также блокирует навязчивую баннерную рекламу и спам. Для малого бизнеса может использоваться программа Kaspersky Small Office Security. Программы Kaspersky Security и Dr.Web Enterprise Security Suite хорошо подходят для решений среднего и крупного бизнеса.

Заметим, что использование самого современного антивирусного решения само по себе не может полностью гарантировать безопасность данных. Если злоумышленник не получает доступа к данным, то это не значит, что данные не могут быть утрачены.

Вторая группа вопросов, которые обязательно должны быть рассмотрены и реализованы в полной мере для обеспечения защиты данных, – резервное копирование и восстановление данных из архивных копий. Если отсутствуют резервные копии, то данные могут быть безвозвратно утрачены в любой момент времени по самым разным причинам. Наиболее часто встречающиеся действия – выход из строя жестких дисков, на которых записана информация, а также неправильные действия самого пользователя, ошибочно удаляющего без возможности восстановления или перезаписывающего файлы с нужной для него информацией.

Отмечено, что, хотя пользователи компьютеров в большинстве своем хорошо знают о необходимости создания резервных копий файлов, но большинство из них такие копии не делают или делают, но недостаточно часто. Возможность восстановления информации со старой копии может быть практически бесполезна для пользователя, т. к. информация, которую можно восстановить, сильно устарела, а новой копии с актуальной информацией у пользователя нет.

Назовем наиболее часто встречающиеся причины, по которым созданию резервных копий уделяется недостаточное внимание.

1 Выход из строя информационных носителей. Надежность современных носителей информации весьма высока, поэтому пользователи недооценивают

возможность выхода информационных носителей из строя. Если носитель функционирует, т. е. с него можно считывать и на него можно записывать данные, то это без дополнительной информации по данному носителю свидетельствует только о том, что устройство исправно. О надежности, которая проявляется во времени, сказать ничего нельзя. Как правило, время безотказной работы современных жестких дисков составляет несколько лет, поэтому такое событие, как выход из строя жесткого диска, происходит достаточно редко, и пользователь не рассматривает вероятность его возникновения как существенную. Однако, если событие все же произошло, может быть полностью и безвозвратно утрачена информация за несколько лет работы. Пользователи недооценивают и вероятность собственных ошибок, которые могут привести к утрате всей или части информации (например, ошибочно отформатировать жесткий диск, перезаписать или удалить нужный файл).

2 Отсутствие свободного места на носителях данных для создания резервных копий. Данный фактор объясняет, почему пользователи игнорируют действия по созданию резервных копий, которые необходимо регулярно создавать. Очевидно, что для сохранения архивов необходимо свободное место, и если его нет, то или надо покупать накопители или арендовать ресурсы для хранения данных (многие облачные провайдеры за относительно невысокую плату предоставляют услуги архивирования информации в облако с поддержкой средств программной автоматизации).

3 Необходимость выделять время и ресурсы на создание резервных копий. Для проведения операции резервного копирования необходимо время – может потребоваться несколько часов. Во время создания резервных копий на обеспечение процедуры затрачивается процессорное время, производительность системы, на которой запущен процесс архивирования, снижается. Несмотря на возможности теневого копирования, пользователи предпочитают не создавать архивные копии в то время, когда работают с данными. Отметим, что нежелательно создавать новые папки, удалять существующие или перемещать их на новое место, если данные операции затрагивают носители, для которых создаются резервные копии.

4 Соблюдение графика создания архивных копий. Если начало операции резервного копирования должно инициироваться вручную или если требуется трудоемкая настройка работы программного обеспечения для создания архивных копий по расписанию, то все это не способствует своевременному созданию архивов.

Отсутствие архивов с актуальной информацией не позволяет относительно быстро и без потерь восстановить данные в случае их утраты по основному месту размещения. Утрата данных возможна не только в том случае, когда вообще не создаются резервные копии, но и тогда, когда процесс архивирования организован неправильно. Например, копируется не вся необходимая информация, архивные копии хранятся на ненадежных носителях, что не позволяет выполнить восстановление информации в полном объеме, архивные копии хранятся в том же самом месте, где и основные носители, что приводит к полной утрате информации в случае чрезвычайных ситуациях (пожары, наводнения и пр.).

Существует множество программ для архивирования данных, некоторые из них: WinZip, 7-Zip, WinRAR, PeaZip, Bandizip, FreeArc, Keka, The Unarchiver, Ark, File Roller.

Это малый список из доступных программ для архивирования данных. Выбор конкретной программы зависит от потребностей и предпочтений пользователя. Из наиболее распространенных выделяют Zip, Rar и 7z-архивы.

Создание резервных копий по средством архивирования является самым простым и понятным способом сохранения данных. Обычно выполняется архивирование данных с разной периодичностью и хранением на внешних носителях или в облачных хранилищах (таблица 6.1).

Таблица 6.1 – Бесплатные облачные хранилища

Облако	Бесплатные Гб	URL
Google Drive	15	https://www.google.com/drive/
Яндекс.Диск	10	https://disk.yandex.ru/client/disk
Облако Mail.ru	8	https://cloud.mail.ru/home/
Degoo	100	https://cloud.degoo.com/
MEGA	50	https://mega.nz/
MEGA	20	https://mega.io/
Blomp	20…200	https://www.blomp.com/
Box	10	https://www.box.com/home
Icedrive	10	https://icedrive.net/
Koofr	10	https://koofr.eu
MediaFire	10	https://www.mediafire.com/
Mimedia	10	http://www.mimedia.com/
pCloud	10	https://my.pcloud.com/
NextCloud	8	https://nextcloud.com/
Amazon Drive	5	https://www.amazon.com/clouddrive
iCloud (Apple)	5	https://www.apple.com/in/icloud/
OpenDrive	5	https://www.opendrive.com/
Sync.com	5	https://www.sync.com/
Dropbox	2	https://www.dropbox.com/ru/
TeraBox	2	https://www.terabox.com/

Кроме простого варианта создания архивов файлов и папок и хранения их в облаках, существуют специализированные программные продукты, позволяющие выполнять резервные копии информации. В качестве примера можно привести EaseUS Todo Backup, Acronis Cyber Backup, Acronis True Image, rsync, Кибер Бэкап, CloudBerry Backup, Macrium Reflect, Backup and Sync от Google, BorgBackup, Restic, Paragon Backup & Recovery Free, AOMEI Backupper Standard, Time Machine и др.

Это малый перечень программ для резервного копирования.

Практическое задание

1 Создать папку и скопировать в нее несколько файлов.

2 Заархивировать данную папку архиватором Rar или Zip. К названию архива обязательно добавить текущую дату.

3 Выполнить аналогичное архивирование, дополнительно установив пароль на архив.

4 Проверить целостность данных распаковав полученные архивы.

5 Создать профиль в сервисе Яндекс.Диск, Гугл.Диск, Mail.ru.Облако или аналогичных сервиса.

6 На облаке создать папку «Резервная копия данных».

7 Скопировать архивный файл на облако в созданную папку.

8 В интернете найти информацию о трех программах для резервного копирования и сравнить их возможности.

9 При возможности установки программ на персональном компьютере скачать и установить одну из программ для резервного копирования. Попробовать сделать резервную копию любой папки с компьютера.

Вопросы для контроля

1 Какие две большие группы вопросов рассматриваются для обеспечения безопасности данных?

2 Почему обеспечение безопасности данных не сводится только к вопросам предотвращения несанкционированного доступа к данным со стороны злоумышленников?

3 Перечислите основные причины, почему пользователи не любят создавать архивные копии.

4 В каких случаях архивные копии создавать не требуется? Приведите примеры.

5 Какие существуют онлайн-сервисы для хранения данных?

7 Практическая работа № 7. Исследование надежности паролей и их восстановление

Цель работы: получение практических навыков по оценке надежности и восстановлению паролей.

Порядок выполнения работы

1 Изучить основные теоретические парольной защиты файлов.

2 Изучить основные программные продукты и онлайн-сервисы по восстановлению паролей.

3 Выполнить работу по восстановлению паролей.

4 Оформить отчет.

Основные теоретические положения

Пароль – это строка символов, которая используется для проверки подлинности пользователя и предоставления доступа к защищенному ресурсу или информации. Он представляет собой секретную комбинацию символов, которая известна только пользователю, имеющему право доступа.

Пароли широко применяются в компьютерной безопасности и используются в различных областях, включая следующие.

1 Пользовательские учетные записи. Пароли используются для защиты учетных записей пользователей, чтобы предотвратить несанкционированный доступ к личной информации или ресурсам.

2 Управление доступом. Пароли используются для управления доступом к помещениям, зданиям, офисам и другим объектам, чтобы предотвратить несанкционированный доступ.

3 Электронная почта. Пароли используются для защиты электронных почтовых ящиков от несанкционированного доступа и для защиты личной информации, содержащейся в письмах.

4 Онлайн-банкинг. Пароли используются для защиты банковских аккаунтов и предотвращения несанкционированных транзакций.

5 Социальные сети. Пароли используются для защиты профилей в социальных сетях и предотвращения несанкционированного доступа к личной информации.

6 Файлы и документы. Пароли могут использоваться для защиты файлов и документов, содержащих конфиденциальную информацию.

7 Wi-Fi-сети. Пароли используются для защиты беспроводных сетей Wi-Fi и предотвращения несанкционированного доступа к сети.

Важно использовать надежные пароли и не использовать один и тот же пароль для нескольких учетных записей, чтобы предотвратить несанкционированный доступ и сохранить конфиденциальность личной информации.

Надежность пароля – это показатель эффективности пароля против угадывания или атак методом перебора. В своей обычной форме он оценивает, сколько попыток потребуется злоумышленнику, у которого нет прямого доступа к паролю, в среднем, чтобы правильно его угадать. Надежность пароля зависит от длины, сложности и непредсказуемости.

Использование надежных паролей снижает общий риск нарушения безопасности, но надежные пароли не заменяют необходимость в других эффективных средствах контроля безопасности.

Скорость, с которой злоумышленник может передавать системе угаданные пароли, является ключевым фактором в определении безопасности системы. Некоторые системы устанавливают тайм-аут в несколько секунд после небольшого числа (например, трех) неудачных попыток ввода пароля. При отсутствии других уязвимостей такие системы могут быть эффективно защищены относительно простыми паролями. Однако система должна хранить информацию о паролях пользователя в той или иной форме, и если эта информация будет

украдена, скажем, путем нарушения безопасности системы, пароли пользователя могут оказаться под угрозой.

Существуют требования к надежности паролей. Пароль должен быть таким, чтобы его нельзя было легко раскрыть. Для этого при выборе и использовании пароля рекомендуется руководствоваться следующими правилами:

1) пароль не должен содержать личных данных пользователя (таких как фамилия, имя, серия или номер паспорта либо другого документа, удостоверяющего личность, дата рождения, адрес и т. п.);

2) пароль не должен быть словом из какого-либо словаря (входить в какой-либо тезаурус), т. к. перебор слов заданного словаря – технически достаточно простая задача;

3) пароль не должен быть слишком коротким (подобрать сочетание символов в этом случае также не представляет сложности);

4) пароль не должен состоять из повторяющихся букв или фрагментов текста;

5) пароль не должен состоять из символов, соответствующих подряд идущим клавишам на клавиатуре (например, «QWERTY» – образец недопустимого пароля);

6) желательно включать в пароль символы в разных регистрах (прописные и строчные буквы, кириллицу и латиницу), знаки препинания, цифры и др.

Следующие меры предосторожности помогут гарантировать безопасность при использовании пароля:

– используйте надежные пароли. Пароли должны быть достаточно длинными и сложными, чтобы их было трудно угадать или взломать. Используйте сочетание букв, цифр и специальных символов;

– не используйте один и тот же пароль для всех аккаунтов. Если пароль взломается, злоумышленники смогут получить доступ ко всем вашим аккаунтам. Используйте уникальные пароли для каждого аккаунта;

– не сообщайте пароли другим людям. Никогда не сообщайте свои пароли другим людям, даже друзьям или близким. Это может привести к несанкционированному доступу к вашим личным данным;

– не используйте общедоступные компьютеры для ввода паролей: избегайте ввода паролей на общедоступных компьютерах, таких как в интернет-кафе или библиотеках. Кто-то может установить программное обеспечение для перехвата паролей;

– используйте двухфакторную аутентификацию. Это обеспечивает дополнительный уровень безопасности для ваших аккаунтов. Помимо пароля, вам потребуется ввести дополнительный код, который будет отправлен на ваш мобильный телефон;

– регулярно меняйте пароли. Регулярно меняйте свои пароли, чтобы повысить безопасность своих аккаунтов. Меняйте пароли, если считаете, что они могут быть скомпрометированы;

– устанавливайте пароли большой длинны. Длинные пароли тяжело подбирать. Установка длинных паролей, как показывает практика, даже более эффективны чем постоянная смена паролей;

– следите за безопасностью своих паролей. Используйте надежные менеджеры паролей для хранения ваших паролей и следите за безопасностью своих аккаунтов.

Существует несколько способов оценки надежности пароля. Вот несколько из них:

– длина пароля. Чем длиннее пароль, тем более безопасным он является. Используйте пароли, состоящие как минимум из восьми символов;

– сложность пароля. Используйте сочетание букв, цифр и специальных символов, чтобы сделать пароль более сложным для угадывания или взлома. Избегайте использования простых слов и фраз, которые могут быть легко угаданы;

– использование менеджера паролей. Многие менеджеры паролей могут оценить надежность пароля и рекомендовать более надежные пароли;

– использование методов восстановления паролей. Можно использовать программы для восстановления паролей или словарные атаки, чтобы узнать, насколько легко пароль может быть взломан;

– использование онлайн-сервисов. Некоторые онлайн-сервисы могут оценить надежность пароля, например, проверка пароля на сайте «How Secure Is My Password?».

Для проверки надежностей паролей более детально рассмотрим онлайн-сервисы, которые могут помочь оценить надежность пароля. Вот несколько популярных сервисов.

1 «Kaspersky Password Check» – сервис проверяет надежность пароля на основе различных факторов, таких как длина, сложность и использование разных типов символов (https://password.kaspersky.com/ru/).

2 «How Secure Is My Password?» – сервис оценивает сложность пароля и сообщает, насколько сложно его будет взломать. Сайт также предлагает рекомендации по улучшению пароля (https://howsecureismypassword.net).

3 «How Secure is Your Password?» – сервис проверяет пароль методом перебора и наличия пароля в базах стандартных паролей (https://www.passwordmonster.com/).

4 «The Password Meter» – сервис проверяет надежность пароля на основе длины, сложности и разнообразия символов. Он также предоставляет рекомендации по улучшению пароля (http://www.passwordmeter.com).

5 «How Secure Is My Password?» – сервис проверки пароля методом перебора (https://www.security.org/how-secure-is-my-password/).

6 «Have I Been Pwned» – сервис проверяющий пароль по базе украденных паролей в интернете (https://haveibeenpwned.com/Passwords).

При работе на компьютере пользователь использует пароли для входа в операционную систему, для работы с электронной почтой, интернет-мессенджерами, документами, архивами. Почти на все файлы можно установить пароли, а также при необходимости их восстановить, если пароль забыт. Программы по восстановлению паролей находятся в Яндексе или Гугле по следующим ключевым словам «RAR password recovery», «ZIP password recovery», «Word

password recovery», «Excel password recovery», «Office password recovery» или «PDF password recovery» и так далее по аналогии.

Для восстановления забытых паролей существуют специализированные программные продукты. Для каждого типа файлов существуют сбои программы.

Для восстановления паролей в архивах RAR: RAR Password Unlocker, Free RAR Password Recovery, Free KRyLack RAR Password Recovery, RAR Password Cracker, Accent RAR Password Recovery, KRyLack RAR Password Recovery, Password Recovery Bundle, Advanced Archive Password Recovery Professional, Advanced RAR Password Recovery, RAR Password Unlocker, Any RAR Password Recovery, PassFab for RAR и др.

Для восстановления паролей в архивах Zip: Zip Password Cracker Pro, KRyLack ZIP Password Recovery, Ultimate ZIP Cracker, Zip Password Recovery Tool, Passware Kit, Accent ZIP Password Recovery, Zip Password Recovery Master, Elcomsoft Distributed Password Recovery и др.

Для восстановления паролей в документах Office: Free Word and Excel Password Recovery Wizard, Appnimi All-In-One Password Unlocker, PassFab for Office, GuaWord, Elcomsoft Advanced Office Password Recovery, Advanced Office Password Recovery Pro, Appnimi Word Password Recovery, Elcomsoft Advanced PDF Password Recovery, Password Recovery Bundle и др.

Для каждого типа файла существуют свои программы, а также имеются специализированные онлайн-сервисы для восстановления забытых паролей, например:

LostMyPass.com – сервис восстанавливающий пароли в файлах архивов zip, rar, 7z, файлах word, excel, powerpoint и pdf (https://www.lostmypass.com/ru/try/).

Password-online – это еще один онлайн-инструмент для восстановления паролей doc, docx, xls, xlsx, ppt, mdb, pdf, rar, zip, 7zip, eoc и т.д. В настоящее время восстановление паролей стало платным (https://www.password-online.com).

Online Password Remover – сервис удаления паролей с документов Excel, Word и PowerPoint (https://www.password-find.com).

PassFab – сервис с информацией по восстановлению паролей с любых документов (https://www.passfab.ru).

Кроме данных сервисов, в интернете есть очень много аналогичных.

Практическое задание

1 Изучите теоретический материал.

2 Придумайте пароль.

3 В поисковой системе Яндекс или Гугл введите «Список самых распространенных паролей» или «Стандартные пароли» и проверьте, есть ли ваш пароль в данном списке.

4 Используя онлайн сервис проверки надежности пароля, проверьте ваш пароль.

5 Создайте документ Word, Excel и архив Zip и установите простой пароль из не более трех символов.

6 Восстановите пароль ваших файлов, используя специализированные онлайн сервисы восстановления паролей или специализированного программного обеспечения при возможности установить его на ваш компьютер.

Вопросы для контроля

1 Что такое пароль?

2 Перечислите минимальные требования к выбору пароля.

3 Как определить вероятность подбора пароля злоумышленником в течение срока его действия?

4 Выбором каких параметров можно повлиять на уменьшение вероятности подбора пароля злоумышленником?

5 Какие онлайн-сервисы по проверке надежностей паролей существуют?

8 Практическая работа № 8. Основы криптографии и шифрования

Цель работы: изучение основ криптографии и шифрования.

Порядок выполнения работы

1 Изучить основные теоретические положения, сделав необходимые выписки в конспект.

2 Получить задание у преподавателя, выполнить типовые задания.

3 Сделать выводы по результатам исследований.

4 Оформить отчет.

Основные теоретические положения

Как и любая наука, криптография опирается на базовые понятия и определения. Рассмотрим основные из них.

Криптография (от др.-греч. κρυπτός (криптос) – тайный, скрытый и γράφω (графо) – пишу) – наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним) и аутентичности (целостности и подлинности авторства, а также невозможности отказа от авторства) информации.

Изначально криптография изучала методы шифрования информации – обратимого преобразования открытого (исходного) текста на основе секретного алгоритма и/или ключа в шифрованный текст (шифротекст). Традиционная криптография образует раздел симметричных криптосистем, в которых зашифрование и расшифрование проводится с использованием одного и того же секретного ключа. Помимо этого раздела, современная криптография включает в себя асимметричные криптосистемы, системы электронной цифровой подписи, хеш-функции, управление ключами, получение скрытой информации, квантовую криптографию.

Криптография не занимается защитой от обмана, подкупа или шантажа законных абонентов, кражи ключей и других угроз информации, возникающих в защищенных системах передачи данных.

Шифр (от арабского sifr «ноль», откуда французское chiffre «цифра»; родственно слову «цифра») – это совокупность условных знаков (условная азбука из цифр или букв) для секретной переписки дипломатических представителей со своими правительствами, а также в вооруженных силах для передачи текста секретных документов по техническим средствам связи.

Открытый (исходный) текст – данные (текстовые или иного вида), передаваемые без использования криптографии.

Шифротекст, шифрованный (закрытый) текст – данные, полученные после применения криптосистемы (обычно с некоторым указанным ключом).

Код – это совокупность алгоритмов криптографических преобразований (шифрования), отображающих множество возможных открытых данных на множество возможных зашифрованных данных, и обратных им преобразований. Важным параметром любого шифра является ключ.

Ключ – это параметр криптографического алгоритма, обеспечивающий выбор одного преобразования из совокупности преобразований, возможных для этого алгоритма. В современной криптографии предполагается, что вся секретность криптографического алгоритма сосредоточена в ключе, но не в деталях самого алгоритма (принцип Керкгоффса).

Шифры могут использовать один ключ для шифрования и дешифрования или два различных ключа. По этому признаку различают симметричный и асимметричный шифры.

Симметричный шифр – это шифр, который использует один ключ для шифрования и дешифрования. Примерами таких систем шифрования являются Шифр Атбаш, Шифр Бэкона и Шифр Цезаря. Шифр Атбаш основан на замене букв алфавита на противоположные. Шифр Бэкона использует комбинации из пяти букв алфавита для кодирования сообщения. Шифр Цезаря сдвигает каждую букву алфавита на фиксированное число позиций, которое задается ключом.

Асимметричный шифр – это шифр, который для шифрования и дешифрования использует два различных ключа. К асимметричным шифрам относятся следующие известные шифры: RSA, Эль-Гамаля (Elgamal), Elliptic curve cryptography (ECC) – криптосистема на основе эллиптических кривых.

Шифры могут быть сконструированы так, чтобы либо шифровать сразу весь текст, либо шифровать его по мере поступления. Таким образом, существуют блочный и поточный шифры.

Блочный шифр шифрует сразу целый блок текста, выдавая шифротекст после получения всей информации.

В блочных шифрах результат зашифрования очередного блока зависит только от него самого и не зависит от других блоков шифруемого массива данных. К блочным шифрам относятся следующие известные шифры: ГОСТ 28147–89, Advanced Encryption Standard (AES), также известный как Rijndael, DES, DESX, Triple DES, CAST-128, CAST-256, Blowfish, Twofish,

IDEA, MARS, RC2, RC5, RC6, Serpent, Safer+, TEA, 3-WAY, WAKE, FROG, Skipjack.

Поточный (потоковый) шифр шифрует информацию и выдает шифротекст по мере ее поступления. За счет этого поточный шифр имеет возможность обрабатывать текст неограниченного размера, используя фиксированный объем памяти. ***Поточный шифр*** – это симметричный шифр, в котором каждый символ открытого текста преобразуется в символ шифрованного текста в зависимости не только от используемого ключа, но и от его расположения в потоке открытого. К поточным шифрам относятся следующие известные шифры: RC4, A5.

Шифрование – процесс нормального применения криптографического преобразования открытого текста на основе алгоритма и ключа, в результате которого возникает шифрованный текст.

Расшифровывание – процесс нормального применения криптографического преобразования шифрованного текста в открытый.

Одними из простых шифров для понимания можно выделить шифры Атбаш, Бэкона, Виженера и Цезаря.

Шифр Цезаря (шифр сдвига, код Цезаря) – такой простой вид шифрования текста, при котором все символы в тексте заменяются символами, сдвинутыми по алфавиту на правее или левее на постоянное количество позиций. Например, при сдвиге на 1 буква А заменяется на Б, Б на В и т. д.

Шифр Атбаш – простой шифр подстановки для алфавитного письма, в котором каждая n-я буква алфавита заменяется буквой m – n +1, где m – общее число букв в алфавите. Другими словами, первая буква заменяется на последнюю, вторая – на предпоследнюю и так далее.

Шифр Бэкона (двухлитерный шифр) – такой метод шифрования, когда буквы алфавита заменяются на символы А и В по правилам двоичного кодирования. Далее эта последовательность букв прячется в сообщении с помощью способов сокрытия сообщение. Например, печатая эти буквы курсивом или выделяя их каким-то другим способом.

Шифр Виженера представляет собой последовательность шифров Цезаря с изменяющимися коэффициентами сдвига, зависящими от ключа.

В настоящее время данные шифры не применяются, но хорошо позволяют понять методику применения систем шифрования. Сейчас в компьютерной технике в зависимости от задач используются симметричные или ассиметричные шифры. В качестве примеров симметричных шифров можно привести следующие.

AES (Advanced Encryption Standard) – это блочный шифр, который используется для защиты данных в различных приложениях, таких как банковское дело, электронная коммерция, облачные вычисления, VPN и т. д. AES считается одним из наиболее безопасных симметричных шифров в настоящее время и широко используется.

Blowfish – это блочный шифр, который используется для защиты данных в различных приложениях, таких как VPN, электронная коммерция, аутентификация и т. д. Blowfish также считается безопасным и используется в настоящее время.

DES (Data Encryption Standard) – это блочный шифр, который ранее использовался для защиты данных в различных приложениях, но сейчас считается устаревшим и небезопасным. Он был заменен на более безопасный шифр AES.

3DES (Triple Data Encryption Standard) – это блочный шифр, который используется для защиты данных в различных приложениях, таких как банковское дело, электронная коммерция. 3DES является усиленной версией DES и считается безопасным, но менее эффективным по сравнению с AES.

Serpent – это блочный шифр, который используется для защиты данных в различных приложениях, таких как VPN, электронная коммерция, аутентификация. Serpent считается безопасным и эффективным, но менее используется, чем AES и Blowfish.

RC6 (Rivest Cipher 6) – это блочный симметричный шифр, использует блоки данных размером 128 бит и ключи длиной от 128 до 256 бит. RC6 использует идеи из других шифров, таких как IDEA и AES, и имеет несколько улучшений, таких как более быстрое шифрование и более безопасное расширение ключа. Шифр RC6 используется в различных приложениях, таких как банковское дело, электронная почта, VPN. Он считается безопасным и эффективным для защиты данных.

IDEA (International Data Encryption Algorithm) – это блочный шифр, который используется для защиты данных в различных приложениях, таких как электронная почта, VPN, аутентификация. IDEA считается безопасным, но менее эффективным по сравнению с AES и другими современными шифрами.

Camellia – это блочный шифр, который используется для защиты данных в различных приложениях, таких как банковское дело, электронная коммерция, аутентификация. Camellia считается безопасным и эффективным, но менее используется, чем AES и другие шифры.

ГОСТ 28147–89 – это блочный шифр, который используется для защиты информации в России. Он используется в различных приложениях, таких как банковское дело, государственная связь, электронная почта.

Кузнечик (GOST R 34.12–2015) – это блочный шифр, который является более современной версией ГОСТ 28147–89. Он используется для защиты информации в России в различных приложениях, таких как банковское дело, государственная связь, электронная почта.

Магма (GOST 28147–89) – это блочный шифр, который также используется для защиты информации в России. Он используется в различных приложениях, таких как государственная связь, банковское дело.

В качестве примеров асимметричных шифров можно привести следующие.

RSA – это асимметричный шифр, который используется для защиты данных в различных приложениях, таких как электронная почта, электронная коммерция, VPN. RSA считается безопасным, и он широко применяется в настоящее время.

Elliptic Curve Cryptography (ECC) – это асимметричный шифр, который использует криптографию эллиптических кривых для защиты данных. Он используется в различных приложениях, таких как банковское дело, электронная

коммерция, мобильные устройств. ECC считается безопасным и устойчивым к атакам, и он широко применяется в настоящее время.

Digital Signature Algorithm (DSA) – это асимметричный шифр, который используется для создания и проверки цифровых подписей. Он используется в различных приложениях, таких как авторизация пользователей, электронная подпись документов, электронный голосовой документ. DSA считается безопасным и применяется в настоящее время.

ElGamal – это асимметричный шифр, который используется для защиты данных в различных приложениях, таких как электронная почта, электронная коммерция, VPN. ElGamal считается безопасным и широко применяется в настоящее время.

Diffie-Hellman Key Exchange (DH) – это асимметричный протокол обмена ключами, который используется для безопасного обмена ключами между двумя сторонами. Он используется в различных приложениях, таких как VPN, защита данных. DH считается безопасным и широко применяется в настоящее время.

Blowfish – это асимметричный шифр, который используется для защиты данных в различных приложениях, таких как электронная почта, файловые системы, VPN. Blowfish считается безопасным и эффективным и широко применяется в настоящее время.

Twofish – это асимметричный шифр, который используется для защиты данных в различных приложениях, таких как электронная почта, файловые системы, VPN. Twofish считается безопасным и широко применяется в настоящее время.

Camellia – это асимметричный шифр, который используется для защиты данных в различных приложениях, таких как электронная почта, файловые системы, VPN. Camellia считается безопасным и широко применяется в настоящее время.

GOST 28147–89 – это асимметричный шифр, который был разработан в СССР и используется в России для защиты государственных секретов и персональных данных. Он используется в различных приложениях, таких как электронная почта, защита данных, телекоммуникации.

КриптоПро – это семейство асимметричных шифров, разработанных в России и широко используемых в государственных и коммерческих организациях. Они используются для защиты данных в различных приложениях, таких как электронная почта, файловые системы, VPN.

Для работы с данными алгоритмами шифрования разработано большое количество программных продуктов, а также онлайн-сервисов, в качестве примеры таких сервисов можно выделить следующие.

1 AES – Symmetric Ciphers Online (AES, DES, TRIPLEDES, BLOWFISH, BLOWFISH-compat, RIJNDAEL-256, R4, SERPENT, TWOFISH) (http://aes.online-domain-tools.com).

2 Шифрование данных (Шифр Атбаш, Шифр Бэкона, Шифр Виженера, Шифр Цезаря) (https://poformule.ru/text/shifrovanie).

3 Сервис для шифрования, хеширования и расшифровки данных. Сервис не взламывает шифровки. Для шифрования и рассшифровки потребуется ключ. Поддерживаемые алгоритмы: cast-128, gost, rijndael-128, twofish, cast-256, loki97, rijndael-192, saferplus, blowfish-compat, des, rijndael-256, serpent, xtea, blowfish, rc2, tripledes, md5 (Хеш), sha1 (Хеш), base64, crc32 (Расчет контрольной суммы), Русский текст -> Транслит, ABC -> \xAA. Поддерживает бинарные и текстовые данные (https://sanstv.ru/tools/crypt/alg-des).

4 Онлайн-шифрование (Шифр Цезаря, Шифр Хилла, Шифр Виженера, Шифр Атбаш, Шифр A1Z26) (http://hostciti.net/calc/?tag=5).

5 Шифрование online (Симметричные -AES (Rijndael), DES, RC4; Асимметричные -RSA) (https://crypt-online.ru).

6 Симметричное шифрование Advanced Encryption Standard (AES) (https://torear797.github.io/PWA/?page=AES).

7 Ассиметричное шифрование RSA (Rivest-Shamir-Adleman) (https://torear797.github.io/PWA/?page=RSA).

8 DenCode (Декодирование шифрами: Цезарь, ROT13 (A-Z), ROT18 (A-Z, 0-9), ROT47 (!-~), Аффинный, Энигма, Скитейл, Ограждения рельсов; Кодирование шифром: Цезарь, ROT13 (A-Z), ROT18 (A-Z, 0-9), ROT47 (!-~), Атбаш, Аффинный, Энигма, JIS Клавиатура, Скитейл, Ограждения рельсов) (https://dencode.com/ru/cipher).

9 Шифрование данных (Шифр Цезаря, Шифр Виженера, Шифр Атбаш, Шифр Бэкона, Шифр A1Z26) (https://calculatorium.ru/cryptography/).

10 RSA Encryption Decryption (https://8gwifi.org/rsafunctions.jsp).

11 Cryptii (Enigma,Swiss-K) (https://cryptii.com/).

12 AES Encryption (https://aesencryption.net/).

13 Encipher.it (https://encipher.it/).

Практическое задание

1 Изучите теоретический материал по криптографии и шифрованию.

2 Выберите любой текстовый фрагмент (может быть статья, песня или абзац из книги).

3 Воспользуйтесь одним из предложенных онлайн-сервисов для шифрования и зашифруйте текстовый фрагмент несколькими различными алгоритмами.

4 Запишите полученные результаты и сравните их длину и уникальность.

5 Используя онлайн-сервис, произведите расшифровку полученных шифров.

Вопросы для контроля

1 Что такое криптография?

2 Что такое шифрование?

3 Что такое симметричные шифры?

4 Что такое асимметричные шифры?

5 В чем отличие симметричного от ассиметричного шифрования?

Список литературы

1 Конституция Республики Беларусь: с изм. и доп., принятыми на респ. референдумах 24 нояб. 1996 г., 17 окт. 2004 г. и 27 фев. 2022 г. – Минск: Нац. центр правовой информ. Респ. Беларусь, 2022. – 80 с.

2 Концепция национальной безопасности Респ. Беларусь [Электронный ресурс] / Нац. реестр правовых актов Респ. Беларусь, 1/9403, 2008.

3 Об информации, информатизации и защите информации: Закон Респ. Беларусь [Электронный ресурс] / Нац. реестр правовых актов Респ. Беларусь. – Минск, 2014.

4 О государственных секретах: Закон Респ. Беларусь [Электронный ресурс] / Нац. реестр правовых актов Респ. Беларусь. – Минск, 2016.

5 ТР 2013/027/BY. Информационные технологии. Средства защиты информации. Информационная безопасность. – Минск: Госстандарт, 2013. – 9с.

6 О защите персональных данных: Закон Респ. Беларусь [Электронный ресурс] / Нац. реестр правовых актов Респ. Беларусь. – Минск, 2021.

7 Перечень стандартов и рекомендаций в области информационной безопасности, применяемых в рамках реализации цифровой повестки Евразийского экономического союза: рекомендация Коллегии ЕЭК [Электронный ресурс] / Нац. реестр правовых актов Респ. Беларусь. – Минск, 2019.

8 Операционные системы. Основы UNIX: учебное пособие / А. Б. Вавренюк [и др.]. – Москва : ИНФРА-М, 2018. – 160 с.

9 Защита информации [Электронный ресурс]: учебное пособие / А. П. Жук [и др.]. – 3-е изд. – Москва: РИОР; ИНФРА-М, 2021. – 400 с. – Режим доступа: http://www.znanium.com. – Дата доступа: 05.03.2022.

10 **Ананченко, И. В.** Средства резервного копирования, восстановления, защиты данных в операционных системах Windows / И. В. Ананченко, Т. В. Зудилова, С. Э. Хоружников. – Санкт-Петербург: Университет ИТМО, 2019. – 50 с.

11 **Аверченков, В. И.** Информационная безопасность сетей и систем: учебное пособие / В. И. Аверченков, В. Т. Еременко, Е. А. Зайченко. – Могилев: Белорус.-Рос. ун-т, 2020. – 212 с.