МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

по выполнению самостоятельной работы
по дисциплине «Информационная безопасность»
для студентов направления 38.03.05 «Бизнес-информатика»
(Направленность (профиль) «Информационная бизнес-аналитика и цифровые технологии»)

Ставрополь, 2026

ВВЕДЕНИЕ

Самостоятельная работа - планируемая учебная, учебно-исследовательская, научно-исследовательская работа студентов, выполняемая во внеаудиторное (аудиторное) время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия (при частичном непосредственном участии преподавателя, оставляющем ведущую роль за работой студентов).

Самостоятельная работа студентов в ВУЗе является важным видом учебной и научной деятельности студента. Самостоятельная работа студентов играет значительную роль в рейтинговой технологии обучения.

Целью данной дисциплины является формирование набора (ПК-2) компетенций будущего бакалавра по направлению подготовки 38.03.05 «Бизнес-информатика».

Применение умений консультировать заказчиков по вопросам совершенствования управления информационной безопасностью ИТ-инфраструктуры предприятия к изучению данного курса определяет следующие его задачи:

– формирование знаний базовых положений концепции информационной безопасности;

– изучение основ классификации угроз информационной безопасности;

– приобретение студентами практических навыков оценки рисков в соответствии с концепцией обеспечения информационной безопасности.

Дисциплина относится к части, формируемой участниками образовательных отношений учебного плана 2025 года направления 38.03.05 «Бизнес-информатика».

Общая характеристика самостоятельной работы студента при изучении дисциплины «Информационная безопасность»

Целью самостоятельной работы студентов является овладение фундаментальными знаниями, профессиональными умениями и навыками деятельности по профилю, опытом творческой, исследовательской деятельности. Самостоятельная работа студентов способствует развитию самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного и профессионального уровня.

Задачами СР являются:

систематизация и закрепление полученных теоретических знаний и практических умений студентов;

углубление и расширение теоретических знаний;

формирование умений использовать нормативную, правовую, справочную документацию и специальную литературу;

развитие познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности;

формирование самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;

развитие исследовательских умений;

использование материала, собранного и полученного в ходе самостоятельных занятий на семинарах, на практических и лабораторных занятиях, при написании курсовых и выпускной квалификационной работ.

План-график выполнения самостоятельной работы

Коды реализуемых копетенций	Вид деятельности студентов	Итоговый продукт самостоятельной работы	Средства и технологии оценки	Обьем часов, в том числе		
				СРС	Контактная работа с преподавателем	Всего
4 семестр						
ПК-2	Самостоятельное решение задач	Отчет	Подготовка к зачету	34,2	3,8	38
	Лекционный материал	Конспект лекций	Собеседование	34,2	3,8	38
Итого за 4 семестр				68,4	7,6	76
Итого				68,4	7,6	76

Методические рекомендации по подготовке к лабораторным занятиям

Работа по подготовке к лабораторным занятиям и активное в них участие — одна из форм изучения программного материала курса. Она направлена на подготовку высококвалифицированных магистров. Подготовку к занятиям следует начинать с внимательного изучения соответствующих разделов учебных пособий и учебников, далее — следует изучать специальную литературу и источники, работать с картами, таблицами, схемами, наконец, написать доклад, если студент получил такое задание. Готовясь к занятиям и принимая активное участие в их работе, студент проходит школу работы над

источниками и литературой, получает навыки самостоятельной работы над письменным и устным сообщением (докладом), учится участвовать в дискуссиях, отстаивать свою точку зрения, формулировать и аргументировать выводы. Форма практических занятий во многом определяется его темой. Практика показывает, что основные формы занятий следующие: беседа на основе составленного преподавателем плана (она наиболее приемлема при обсуждении одного из теоретических вопросов по проблемам темы или монографии), коллоквиум по разделу учебника пли одной из монографий (коллоквиум предполагает прежде всего проверку знаний по определенной теме, источникам, разделу курса); подготовка письменного доклада студентом, его устный доклад и обсуждение его на занятии.

В планы лабораторных занятий включены основные вопросы общего курса. В ходе занятий возможна их конкретизация и корректировка. При подготовке сообщений и докладов следует широко использовать опубликованные источники, исследовательскую литературу. Учебники и учебные пособия студент использует по своему выбору. Каждому студенту в течение года следует прочитать не менее двух монографий (или одну монографию и одну работу мемуарного характера), которые указаны в списке литературы или рекомендовано преподавателем из числа новых публикаций, составить краткий доклад и быть готовым к беседе по ним с преподавателем.

Методические рекомендации по изучению теоретического материала

Работа с книгой

При работе с книгой необходимо подобрать литературу, научиться правильно ее читать, вести записи. Для подбора литературы в библиотеке используются алфавитный и систематический каталоги.

Важно помнить, что рациональные навыки работы с книгой - это всегда большая экономия времени и сил.

Правильный подбор учебников рекомендуется преподавателем, читающим лекционный курс. Необходимая литература может быть также указана в методических разработках по данному курсу.

Изучая материал по учебнику, следует переходить к следующему вопросу только после правильного уяснения предыдущего, описывая на бумаге все выкладки и вычисления (в том числе те, которые в учебнике опущены или на лекции даны для самостоятельного вывода).

При изучении любой дисциплины большую и важную роль играет самостоятельная индивидуальная работа.

Особое внимание следует обратить на определение основных понятий курса. Студент должен подробно разбирать примеры, которые поясняют такие определения, и уметь строить аналогичные примеры самостоятельно. Нужно добиваться точного представления о том, что изучаешь. Полезно составлять опорные конспекты. При изучении материала по учебнику полезно в тетради (на специально отведенных полях) дополнять конспект лекций. Там же следует отмечать вопросы, выделенные студентом для консультации с преподавателем.

Выводы, полученные в результате изучения, рекомендуется в конспекте выделять, чтобы они при перечитывании записей лучше запоминались.

Опыт показывает, что многим студентам помогает составление листа опорных сигналов, содержащего важнейшие и наиболее часто употребляемые формулы и понятия. Такой лист помогает запомнить формулы, основные положения лекции, а также может служить постоянным справочником для студента.

Различают два вида чтения; первичное и вторичное. *Первичное* - эти внимательное, неторопливое чтение, при котором можно остановиться на трудных местах. После него не

должно остаться ни одного непонятного олова. Содержание не всегда может быть понятно после первичного чтения.

Задача *вторичного* чтения полное усвоение смысла целого (по счету это чтение может быть и не вторым, а третьим или четвертым).

Правила самостоятельной работы с литературой

Как уже отмечалось, самостоятельная работа с учебниками и книгами (а также самостоятельное теоретическое исследование проблем, обозначенных преподавателем на лекциях) – это важнейшее условие формирования у себя научного способа познания. Основные советы здесь можно свести к следующим:

• Составить перечень книг, с которыми Вам следует познакомиться;

• Сам такой перечень должен быть систематизированным.

• Обязательно выписывать все выходные данные по каждой книге (при написании курсовых и дипломных работ это позволит очень сэкономить время).
• Разобраться для себя, какие книги (или какие главы книг) следует прочитать более внимательно, а какие – просто просмотреть.

• При составлении перечней литературы следует посоветоваться с преподавателями и научными руководителями (или даже с более подготовленными и эрудированными сокурсниками), которые помогут Вам лучше сориентироваться, на что стоит обратить большее внимание, а на что вообще не стоит тратить время...

•Естественно, все прочитанные книги, учебники и статьи следует конспектировать, но это не означает, что надо конспектировать «все подряд»: можно выписывать кратко основные идеи автора и иногда приводить наиболее яркие и показательные цитаты (с указанием страниц).

Чтение научного текста является частью познавательной деятельности. Ее цель – извлечение из текста необходимой информации. От того на сколько осознанна читающим собственная внутренняя установка при обращении к печатному слову (найти нужные сведения, усвоить информацию полностью или частично, критически проанализировать материал и т.п.) во многом зависит эффективность осуществляемого действия.

Выделяют ***четыре основные установки в чтении научного текста***:

1. информационно-поисковый (задача – найти, выделить искомую информацию)
2. усваивающая (усилия читателя направлены на то, чтобы как можно полнее осознать и запомнить как сами сведения излагаемые автором, так и всю логику его рассуждений)
3. аналитико-критическая (читатель стремится критически осмыслить материал, проанализировав его, определив свое отношение к нему)
4. творческая (создает у читателя готовность в том или ином виде – как отправной пункт для своих рассуждений, как образ для действия по аналогии и т.п. – использовать суждения автора, ход его мыслей, результат наблюдения, разработанную методику, дополнить их, подвергнуть новой проверке).

Основные виды систематизированной записи прочитанного:

1. Аннотирование – предельно краткое связное описание просмотренной или прочитанной книги (статьи), ее содержания, источников, характера и назначения;
2. Планирование – краткая логическая организация текста, раскрывающая содержание и структуру изучаемого материала;
3. Тезирование – лаконичное воспроизведение основных утверждений автора без привлечения фактического материала;
4. Цитирование – дословное выписывание из текста выдержек, извлечений, наиболее существенно отражающих ту или иную мысль автора;

5. Конспектирование – краткое и последовательное изложение содержания прочитанного.

Конспект – сложный способ изложения содержания книги или статьи в логической последовательности. Конспект аккумулирует в себе предыдущие виды записи, позволяет всесторонне охватить содержание книги, статьи. Поэтому умение составлять план, тезисы, делать выписки и другие записи определяет и технологию составления конспекта.

Методические указания по составлению конспекта

1. Внимательно прочитайте текст. Уточните в справочной литературе непонятные слова. При записи не забудьте вынести справочные данные на поля конспекта;
2. Выделите главное, составьте план;
3. Кратко сформулируйте основные положения текста, отметьте аргументацию автора;
4. Законспектируйте материал, четко следуя пунктам плана. При конспектировании старайтесь выразить мысль своими словами. Записи следует вести четко, ясно.
5. Грамотно записывайте цитаты. Цитируя, учитывайте лаконичность, значимость мысли.

В тексте конспекта желательно приводить не только тезисные положения, но и их доказательства. При оформлении конспекта необходимо стремиться к емкости каждого предложения. Мысли автора книги следует излагать кратко, заботясь о стиле и выразительности написанного. Число дополнительных элементов конспекта должно быть логически обоснованным, записи должны распределяться в определенной последовательности, отвечающей логической структуре произведения. Для уточнения и дополнения необходимо оставлять поля.

Овладение навыками конспектирования требует от студента целеустремленности, повседневной самостоятельной работы.

Список рекомендуемой литературы

Основная литература:

1. Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации / Ю.Н. Загинайлов. - М.|Берлин : Директ-Медиа, 2023. - 253 с. - ISBN 978-5-4475-3946-7

2 Кияев, В. Безопасность информационных систем / В. Кияев ; О. Граничин. - Москва : Национальный Открытый Университет «ИНТУИТ», 2016. - 192 с.

3 Скрипник, Д. А. Общие вопросы технической защиты информации : учебное пособие / Скрипник Д. А. - Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), 2020. - 424 с. - Книга находится в базовой версии ЭБС IPRbooks.

Дополнительная литература:

1 Гуляев, В. П. Анализ демаскирующих признаков объектов информатизации и технических каналов утечки информации / В.П. Гуляев. - Екатеринбург : Издательство Уральского университета, 2014. - 163 с. - ISBN 978-5-7996-1120-0

2 Нестеров С.А. Основы информационной безопасности : учебное пособие / Нестеров С.А. - Санкт-Петербург : Санкт-Петербургский политехнический университет Петра Великого, 2024. - 322 с. - Книга находится в базовой версии ЭБС IPRbooks. - ISBN 978-5-7422-4331-1

3 Сетевая защита на базе технологий фирмы Cisco Systems. Практический курс / А.Н. Андрончик. - Екатеринбург : Издательство Уральского университета, 2022. - 179 с. - ISBN 978-5-7996-1201-6

Интернет-ресурсы:

1. http://all-ib.ru - Информационная безопасность. Защита информации
2. http://bezopasnik.org/ - Информационная безопасность

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

по выполнению лабораторных работ
по дисциплине
«Информационная безопасность»
для студентов направления 38.03.05 «Бизнес-информатика»
(Направленность (профиль) «Информационная бизнес-аналитика и цифровые технологии»)

Ставрополь, 2026

Введение

Самостоятельная работа - планируемая учебная, учебно-исследовательская, научно-исследовательская работа студентов, выполняемая во внеаудиторное (аудиторное) время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия (при частичном непосредственном участии преподавателя, оставляющем ведущую роль за работой студентов).

Самостоятельная работа студентов в ВУЗе является важным видом учебной и научной деятельности студента. Самостоятельная работа студентов играет значительную роль в рейтинговой технологии обучения.

Целью данной дисциплины является формирование набора (ПК-2) компетенций будущего бакалавра по направлению подготовки 38.03.05 «Бизнес-информатика».

Задачами дисциплины «Базы данных» являются: систематизация и закрепление полученных теоретических знаний и практических умений студентов; углубление и расширение теоретических знаний; формирование умений использовать нормативную, правовую, справочную документацию и специальную литературу; развитие познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности; формирование самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации; развитие исследовательских умений; использование материала, собранного и полученного в ходе самостоятельных занятий на семинарах, на практических и лабораторных занятиях, при написании курсовых и выпускной квалификационной работ, для эффективной подготовки к итоговым зачетам и экзаменам.

Дисциплина «Информационная безопасность» входит в часть, формируемой участниками образовательных отношений учебного плана 2025 года по направлению 38.03.05 «Бизнес информатика». Ее освоение происходит в 4 семестре.

Содержание

Лабораторная работа № 1. Работа с программой вскрытия паролей AZPR

Цель: изучить возможности защиты архива паролем, научиться использовать программу вскрытия паролей Advanced ZIP Password Recovery

Формируемые компетенции или их части

№ п/п	Содержание компетенции	Шифр
1.	Способен проводить сопровождение ИТ инфраструктуры	ПК-2

Теоретическая часть
Проблема: забытые пароли

Если вы будете честно следовать правилам установки паролей, то вскоре начнёте их путать и забывать. Windows берёт часть работы на себя. Он запомнит, если вы захотите, логины и пароли на веб-сайтах, сохранит ключи шифрования, электронные сертификаты. Единственное, что вам необходимо помнить — это ваши имя пользователя и пароль. Пользователь в Windows сам управляет своими паролями. При утере пароля администратор, конечно, может присвоить новый пароль. Но при этом вы потеряете доступ ко всем вашим зашифрованным данным и сертификатам.

Если требуется восстановить утерянный пароль (либо проверить насколько уязвимым по отношению к атакам является компьютер), можно воспользоваться программами восстановления паролей. Они различаются по методам взлома (атаки со словарём, извлечение хэшей паролей из базы данных SAM или, что ещё лучше, извлечение подобной информации из памяти, грубый перебор всех вариантов) и способом работы (после загрузки с диска, после загрузки в другой операционной системе, с другого компьютера, подключённого к сети, с другого рабочего стола).

Рассмотрим пример программы для восстановления паролей

Advanced Office Password Recovery (AOPR) - программа для восстановления забытых паролей к документам Microsoft Office.

Advanced Office Password Recovery позволяет восстанавливать пароли либо обходить парольную защиту файлов и документов, созданных в продуктах семейства MS Office всех версий. В данный момент поддерживаются версии с 2.0 по 2010 включительно. Программа поддерживает документы, созданные MS Word, Excel, Access, Outlook, Project, Money, PowerPoint, Publisher, а также OneNote. Кроме перечисленного, программа позволяет получить доступ к исходным текстам VBA макросов, защищенных паролем.

Возможности Advanced Office Password Recovery

- ✓ Поддержка всех версий Microsoft Office с 2.0 по 2019
- ✓ Мгновенное восстановление отдельных паролей
- ✓ Изменение пароля на указанный пользователем
- ✓ Мгновенное снятие защиты с документов, для которых когда-либо были подобраны пароли
- ✓ Использование всех обнаруженных уязвимостей продуктов семейства MS Office для восстановления доступа к документам
- ✓ Предварительная атака с набором типичных параметров для восстановления стойких паролей
- ✓ Поддержка атаки по словарю и прямого перебора паролей с использованием шаблонов масок
- ✓ Аппаратное ускорение (подана заявка на патент) уменьшает время перебора паролей в 50 раз

- ✓ Технология аппаратного ускорения с использованием видеокарт NVIDIA или ATI
- ✓ Поддержка одновременно до 32 центральных процессоров или ядер и до 8 графических процессоров
- ✓ Оптимизация кода под современные процессоры позволяет достичь максимальной в данном классе продуктов скорости перебора паролей **Мгновенное восстановление доступа к защищенным документам**

Во многих случаях **Advanced Office Password Recovery** позволяет восстановить доступ к защищенным документам в ту же секунду. Например, старые версии MS Office используют очень простую систему шифрования, которая позволяет вычислить пароль. Также в некоторых версиях Office используются алгоритмы с ограничением длины ключа

Помимо указанных приложений, с помощью **Advanced Office Password Recovery** возможно мгновенное восстановление доступа к документам, защищенным другими версиями продуктов семейства MS Office. В частности, поддерживается возможность восстановления сохраненных паролей, используемых для авторизации через MS Passport (LiveID).

Методы восстановления пароля Предварительная атака

Если документ защищен стойким паролем, его расшифровка может занять много времени. Для удобства пользователей в программе предусмотрена предварительная атака, которая автоматически перебирает все типичные пароли и использует атаку по словарю. Также производится поиск среди паролей, которые когда-либо были восстановлены для других документов.

Перебор по маске

В случае наличия дополнительной информации о пароле (известна длина пароля в символах или любая часть пароля, либо есть информация об использовании или отсутствии в пароле определенных символов и цифр) скорость восстановления может быть существенно увеличена методом перебора по заданной маске.

Атака по словарю

Согласно статистике, существенная часть паролей, используемых для защиты офисных документов, содержит одно или несколько слов из словаря. Метод подбора паролей по словарю позволяет в десятки раз сократить время, требуемое для восстановления пароля. **Advanced Office Password Recovery** поддерживает атаку по словарю, перебирая пароли, состоящие из слов и их возможных комбинаций в разных регистрах и на нескольких языках. Поддерживается возможность подключения дополнительных словарей.

Прямой перебор

В случае полного отсутствия информации о пароле осуществляется перебор всех возможных вариантов пароля определенной длинны для восстановления доступа к документу. В **Advanced Office Password Recovery** используются новейшие методы низкоуровневой оптимизации кода под современные процессоры, позволяющие достичь высокой производительности перебора по сравнению с конкурирующими продуктами.

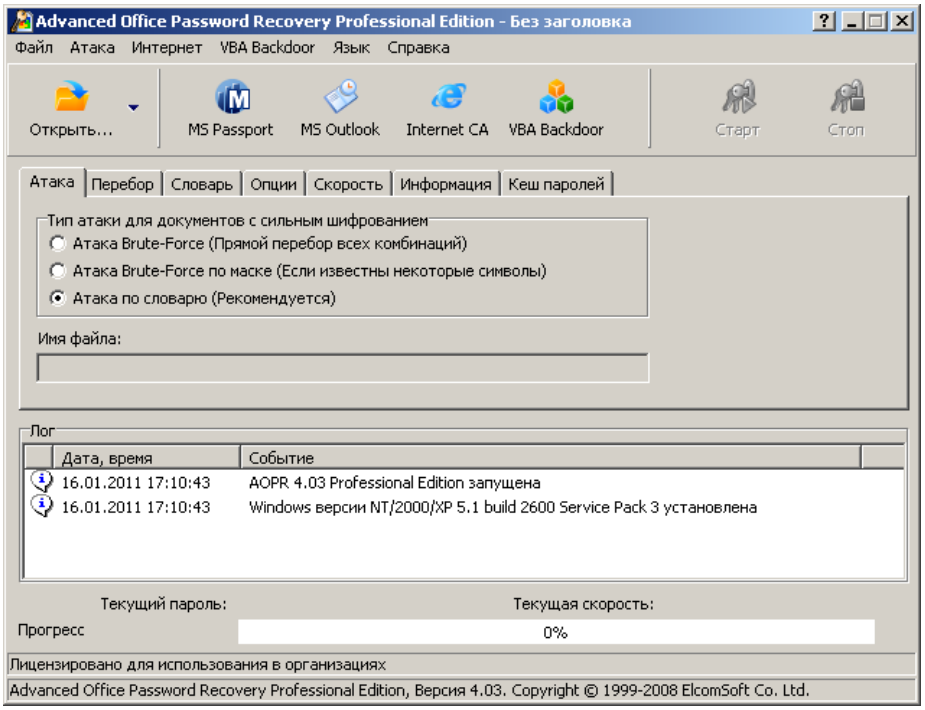


Рис. 3 Интерфейс программы

Выполнить практическое задание:

Задание 1. Восстановление пароля в документах MS Office

Указание: при выполнении задания используйте документы MS Word, MS Excel, MS Access, защищенные паролем

- ✓ Откройте программу **Advanced Office Password Recovery (AOPR)**
- ✓ В панели инструментов окна программы выберите **Открыть**
- ✓ В окне открытия файла выберите защищенный файл MS Word
- ✓ Просмотрите результат: пароль восстановлен?
- ✓ Аналогично выберите документ MS Excel, затем файл базы данных MS Access
- ✓ Изучите возможности программы

Выполнить конспект задания в тетради

Задание 2

1. Выполните поиск в сети Internet специализированных программных средств для создания, а также для восстановления паролей
2. Подготовьте сообщение по данной теме

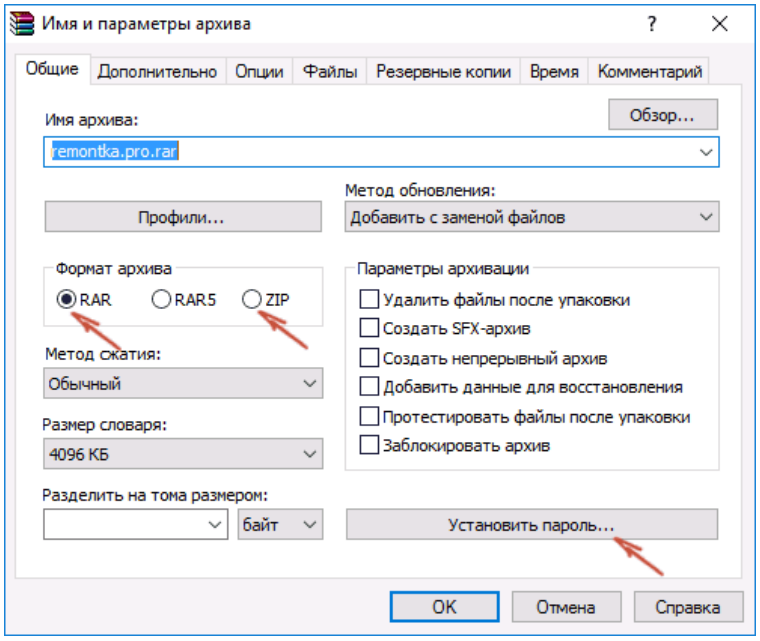
Установка пароля на архив

Создание архива с паролем, при условии, что этот пароль достаточно сложен — очень надежный способ защитить свои файлы от просмотра посторонними. Несмотря на обилие разнообразных программ **Password Recovery** для подбора паролей архивов, если он будет достаточно сложным, взломать его не получится.

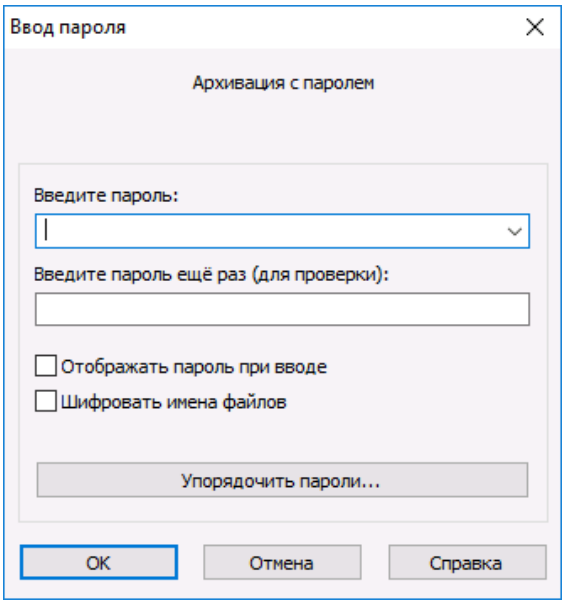
Установка пароля на архивы ZIP и RAR в программе WinRAR

В WinRAR вы можете создавать архивы RAR и ZIP, и устанавливать пароли на оба типа архива. Однако, шифрование имен файлов доступно только для RAR (соответственно, в ZIP, чтобы извлечь файлы понадобится ввести пароль, однако имена файлов будут видны и без него).

Первый способ создать архив с паролем в WinRAR — выделить все файлы и папки для помещения в архив в папке в Проводнике или на Рабочем столе, кликнуть по ним правой кнопкой мыши и выбрать пункт контекстного меню **Добавить в архив…** с иконкой WinRAR.

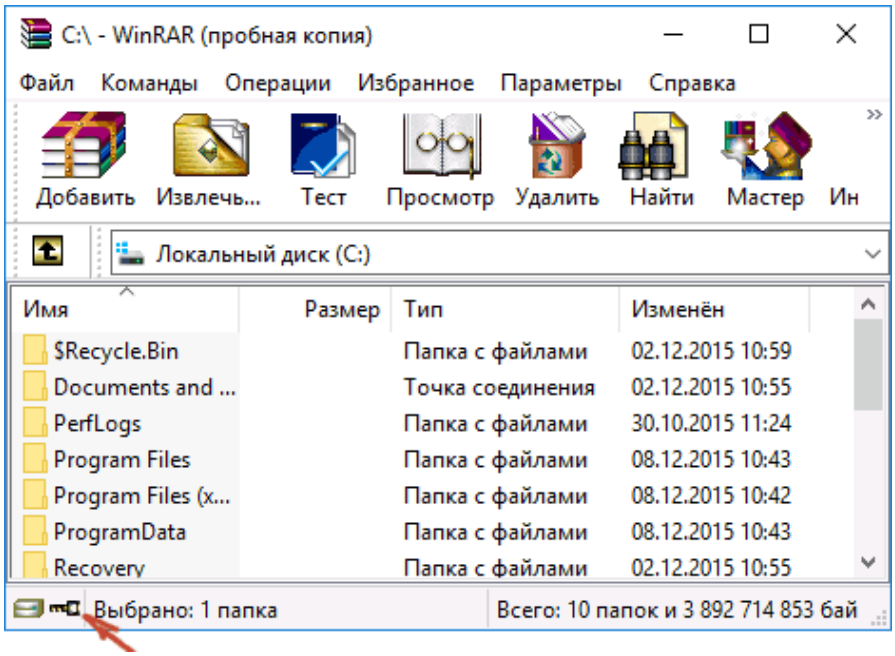


Откроется окно создания архива, в котором, помимо выбора типа архива и места его сохранения, вы можете нажать кнопку **Установить пароль**, после чего дважды ввести его, при необходимости включить шифрование имен файлов (только для RAR). После этого нажмите ОК, и еще раз ОК в окне создания архива — архив будет создан с паролем.



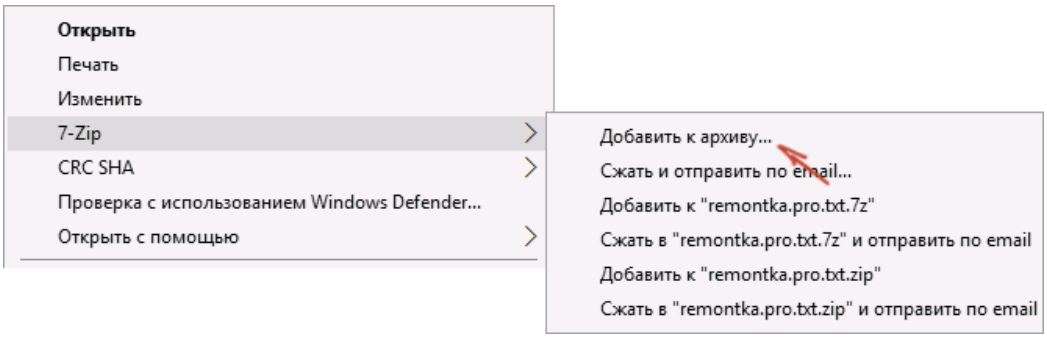
Если в контекстном меню по правому клику нет пункта для добавления в архив WinRAR, то вы можете просто запустить архиватор, выбрать файлы и папки для архивации в нем, нажать кнопку **Добавить** в панели сверху, после чего проделать те же действия по установке пароля на архив.

Второй способ поставить пароль на архив или все архивы, в дальнейшем создаваемые в WinRAR — нажать по изображению ключа слева внизу в строкесостояния и задать необходимые параметры шифрования. При необходимости установите отметку **Использовать для всех архивов**.

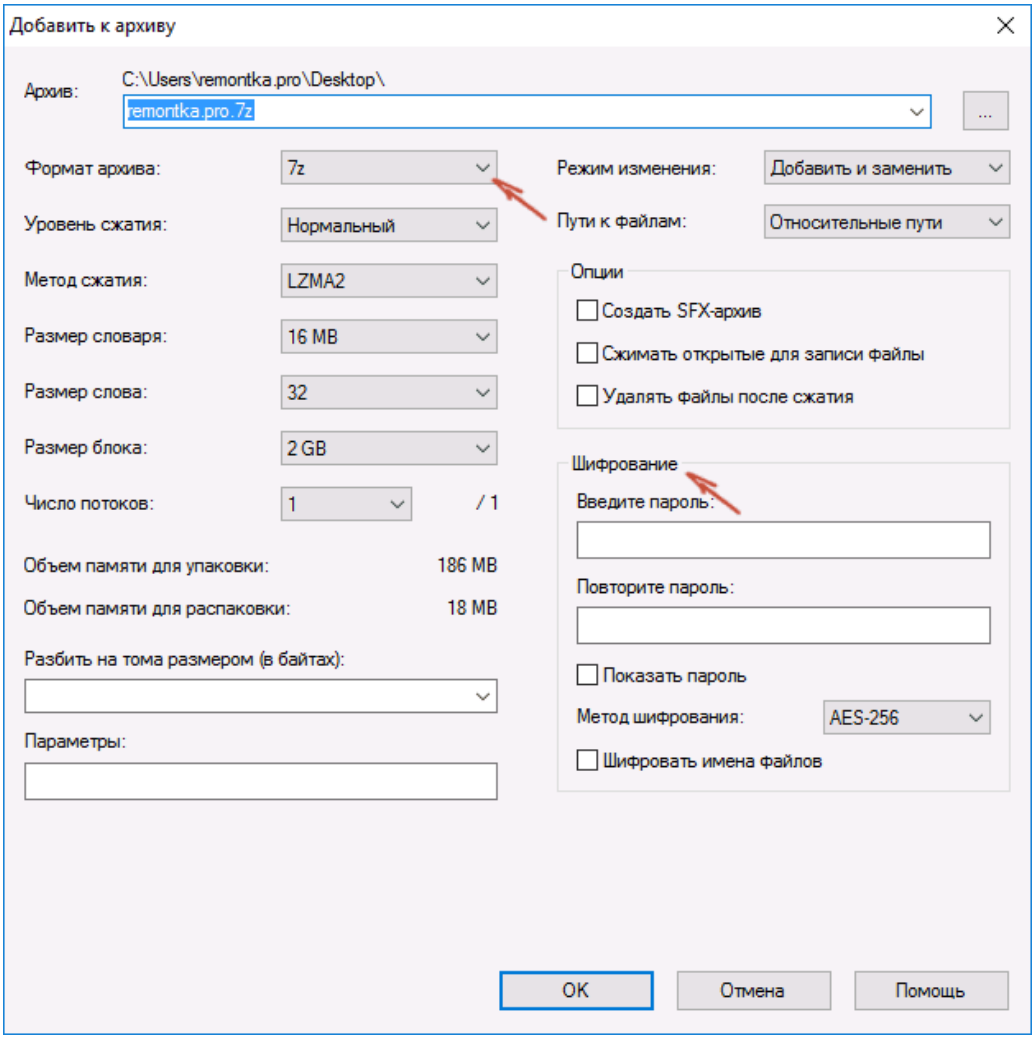


Создание архива с паролем в 7-ZIP

С помощью бесплатного архиватора 7-Zip можно создавать архивы 7z и ZIP, устанавливать на них пароль и выбирать тип шифрования (а распаковывать можно и RAR). Точнее, можно создавать и другие архивы, но установить пароль возможно лишь на два указанных выше типа.



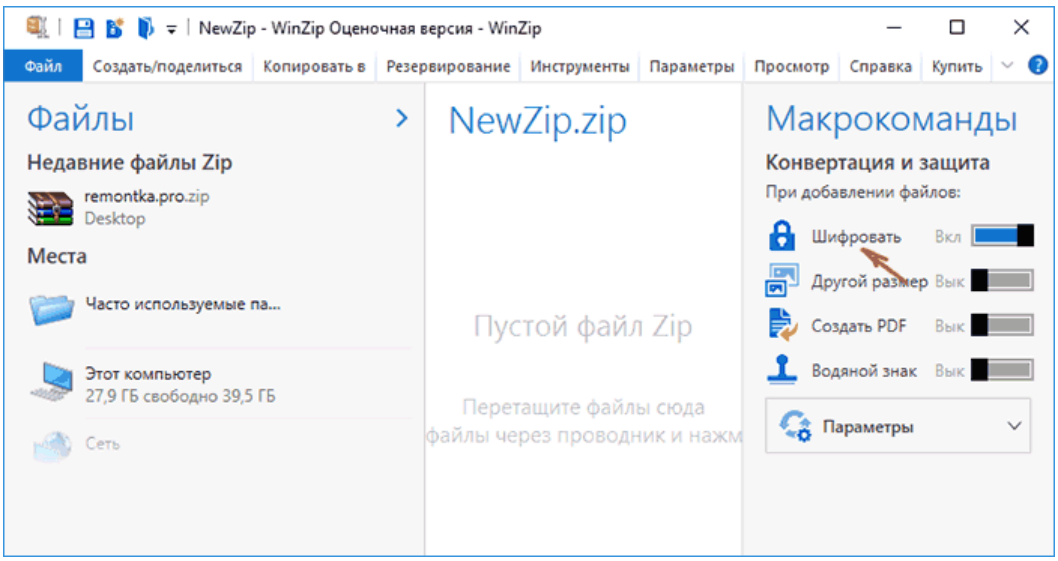
Так же, как и в WinRAR, в 7-ZIP создание архива возможно с помощью пункта контекстного меню **Добавить к архиву** в разделе **7-ZIP** или из главного окна программы с помощью кнопки **Добавить**.



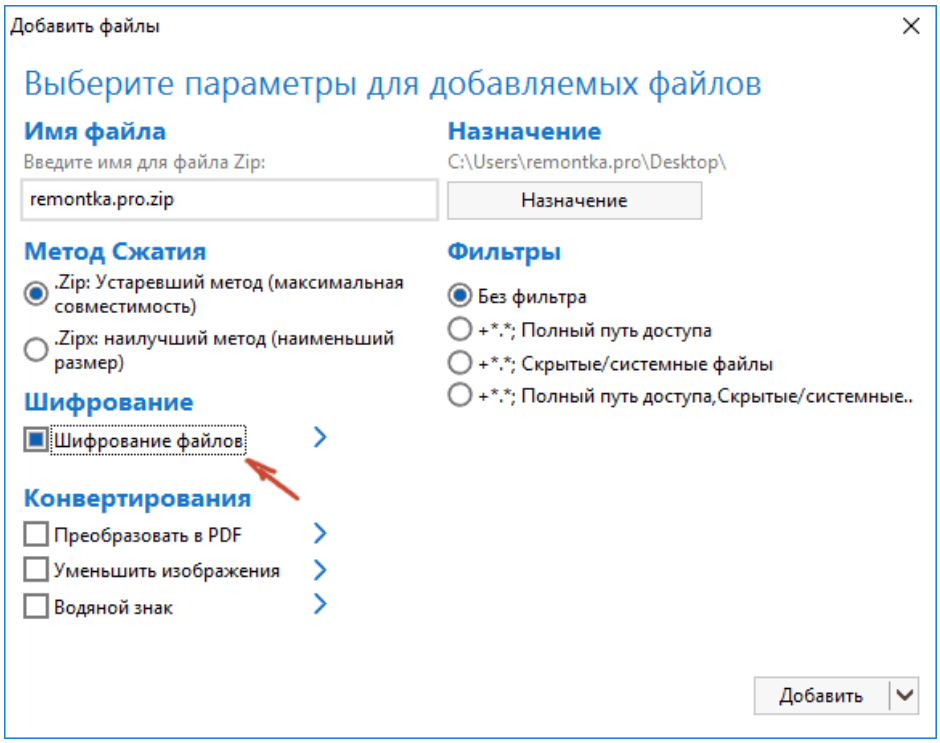
В обоих случаях вы увидите одинаковое окно добавления файлов в архив, в котором, при выборе форматов 7z (по умолчанию) или ZIP будет доступно включение шифрования, при этом для 7z доступно также и шифрование файлов. Просто задайте желаемый пароль, при желании включите скрытие имен файлов и нажмите ОК. В качестве метода шифрования рекомендованы AES-256 (для ZIP имеется также ZipCrypto).

В WinZip

С помощью WinZIP можно создать архивы ZIP (или Zipx) с шифрованием AES-256 (по умолчанию), AES-128 и Legacy (тот самый ZipCrypto). Сделать это можно в главном окне программы, включив соответствующий параметр в правой панели, а затем задав параметры шифрования ниже (если вы их не зададите, то при добавлении файлов в архив вас просто попросят указать пароль).



При добавлении файлов в архив с помощью контекстного меню проводника, в окне создания архива просто отметьте пункт **Шифрование файлов**, нажмите кнопку **Добавить** внизу и установите пароль на архив после этого.



Выполнить практическое задание:

Задание 3. Создайте 2 архива, содержащие по 3 файла. Установите пароль на каждый архив

Работа с программами взлома на примере AZPR

Программа AZPR используется для восстановления забытых паролей ZIP- архивов. На сегодняшний день существует два способа вскрытия паролей: перебор (brute force) и атака по словарю (dictionary-based attack).

Панель управления:

- ✓ кнопки **Открыть** и **Сохранить** позволяют работать с проектом, в котором указан вскрываемый файл, набор символов, последний протестированный пароль. Это позволяет приостанавливать и возобновлять вскрытие.
- ✓ кнопки **Старт** и **Стоп** позволяют соответственно начинать и заканчивать подбор пароля.
- ✓ кнопка **Набор** позволяет задать свое множество символов, если известны символы, из которых состоит пароль.
- ✓ кнопка **Справка** выводит помощь по программе.
- ✓ кнопка **О AZPR** выводит информацию о программе.
- ✓ кнопка **Выход** позволяет выйти из программы

Рассмотрим возможности программы:

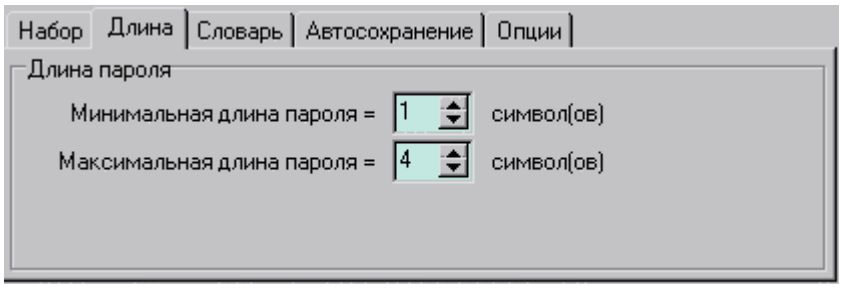
Выбирается архив для вскрытия и тип атаки (см. рис).

Выбираются параметры работы:

✓ Закладка **Набор**

Программа позволяет выбрать область перебора (набор символов). Это значительно сокращает время перебора. Можно использовать набор пользователя, заданный с помощью кнопки Набор. Можно ограничить количество тестируемых паролей, задав начальный пароль. В случае если известна часть пароля, очень эффективна атака по маске. Нужно выбрать соответствующий тип атаки, после этого станет доступным поле маска. В нем нужно ввести известную часть пароля в виде **P?s?W?r?** , где на месте неизвестных символов нужно поставить знак вопроса. Можно использовать любой другой символ, введя его в поле символ маски.

✓ Закладка **Длина -** позволяет выбрать длину пароля



✓ Закладка **Словарь**

Позволяет выбрать файл-словарь. Выбирайте файл **English.dic**, он содержит набор английских слов и наборы символов, наиболее часто использующиеся в качестве паролей.

✓ Закладка **Автосохранение**

Можно выбрать имя файла для сохранения результатов работы и интервал автосохранения.

✓ Закладка **Опции**

Выбирается приоритет работы (фоновый или высокий), интервал обновления информации о тестируемом в данный момент пароле. Увеличение интервала повышает быстродействие, но снижает информативность. Также можно установить режим ведения

протокола работы и возможность минимизации программы в **tray** (маленькая иконка рядом с часами).

Выполнить практическое задание:

Задание 4. Вскрытие пароля архива

Используются архивы с паролями из задания 3.

Проведение атаки перебором (bruteforce attack)

1. Используя программу для вскрытия паролей произвести атаку на зашифрованные архивный файлы созданный вами (не менее 5 файлов). Используйте при создания паролей разное сочетание допустимых символов алфавита, но не более 4 символов. Зафиксируйте время нахождения пароля в каждом случае. Сделайте выводы, как от сложности пароля зависит время вскрытия пароля.
2. Выполнив пункт 1, сократить область перебора до фактически используемого (например если пароль 6D1A – то выбрать прописные английские буквы и цифры). Провести повторное вскрытие. Сравнить затраченное время.

Проведение атаки по словарю (dictionary attack)

1. Сжать какой-либо небольшой файл, выбрав в качестве пароля английское слово длиной до 5 символов (например love, god, table, admin и т.д.). Провести атаку по словарю. Для этого выбрать вид атаки и в закладке Словарь выбрать файл English.dic. Он содержит набор английских слов и наборы символов, наиболее часто использующиеся в качестве паролей.
2. Попытаться определить пароль методом прямого перебора. Сравнить затраченное время.

Оформить конспект работы в тетради Контрольные вопросы:

1. Какие виды атак на пароль Вы знаете?
2. Что такое плохой пароль?
3. Как можно противостоять атаке полным перебором?
4. Как длина пароля влияет на вероятность раскрытия пароля?
5. Какие рекомендации по составлению паролей Вы можете дать?

Лабораторная работа № 2. Исследование и настройка межсетевого экрана

Цель: изучение механизмов работы средств обеспечения и поддержки сетевой защиты – брандмауэра и сетевого сканера; практическое ознакомление с работой сетевого сканера XSpider и межсетевого экрана Outpost

Формируемые компетенции или их части

№ п/п	Содержание компетенции	Шифр
1.	Способен проводить сопровождение ИТ инфраструктуры	ПК-2

Теоретическая часть

Теоретические сведения к практической работе

Интенсивная информатизация государственных и муниципальных управленческих структур, промышленных предприятий и корпораций, силовых ведомств, научных, медицинских и других учреждений выдвинула на первый план вопросы безопасности информационных ресурсов.

Среди угроз безопасности информации значительное место занимает автоматическое внедрение в компьютеры программных закладок, способных скрыто отслеживать и передавать злоумышленнику данные о функционировании компьютера, обрабатываемой на нем информации, а также о всей компании в целом. Кроме того, проблемы компьютерным сетям предприятий создают факты проникновения компьютерных хулиганов, которые, взломав систему сетевой защиты компании, могут завладеть конфиденциальной информацией или нанести физический вред оборудованию, используя специализированное вредоносное ПО.

Подобные ситуации возникают из-за уязвимостей в системе корпоративной защиты компании, в основном связанные с открытыми портами неиспользуемых сервисов, работающих вхолостую. Как правило, через «дыры» в данных сервисах осуществляется большая часть удачных атак извне, которые, зачастую, кончаются потерей компанией секретных данных.

Ярким примером наличия подобных уязвимостей могут послужить популярные операционные системы WindowsXP и FreeBSD. Так, в MS Windows, по умолчанию, работает довольно много неиспользуемых сервисов, которые в большинстве своем связаны с открытыми портами, через которые злоумышленник может провести атаку. Всем, наверное, известен факт, когда множество «автономных» пользовательских компьютеров пострадали во всем мире в результате атаки на порт 135 (RPC). Что касается FreeBSD, то здесь также после стандартной установки в системе работают демоны, которые в обычных случаях не требуются, а значит, являются дополнительными источниками уязвимостей в компьютере. Атаки на почтовый сервер sendmail приводят к полному получению злоумышленником контроля над хостом. Откуда sendmail, спросите вы? Да, иногда, в UNIX-системах, в том числе адаптированных для
работы в качестве рабочей станции, в конфигурации «по-умолчанию» можно встретить и такие сервисы…

Необходимо отметить, что на сегодняшний день работы по проникновению злоумышленников через «дыры» в защите на 90% автоматизированы. Поэтому, «самостоятельное» появление вредоносного ПО на вашем компьютере, которое встречается сегодня очень часто, связано в большинстве случаев с наличием непреднамеренных лазеек в неиспользуемых, а значит, не обновляющихся, службах.

Тем не менее, при использовании специальных средств защиты, подобных нежелательных событий можно, как правило, избежать.

Основными средствами защиты на сегодняшней день являются две категории специализированных программ:

- Межсетевые экраны (брандмауэры, FireWall, МСЭ);
- Сканеры (сканеры открытых портов и сервисов).

Следует сказать, что брандмауэр – основной механизм в сети программной и аппаратной защиты рабочих станций и серверов от атак извне и изнутри.

Сканер – это вспомогательный программный инструмент, позволяющий провести групповое тестирование параметров хостов сети, а также определить наличие и правильность настройки в них МСЭ.

Эти два класса систем в комплексе позволяют построить эффективную эшелонированную систему защиты компании, значительно снизив тем самым вероятность вторжения в сеть злоумышленников.

Системы программной и аппаратной защиты рабочих станций – брандмауэры (FireWalls)

Архитектура firewall

Firewall — это шлюз сети, снабженный правилами защиты. Он может быть аппаратным или программным. В соответствии с заложенными правилами обрабатывается каждый пакет, проходящий наружу или внутрь сети, причем процедура обработки может быть задана для каждого правила. Производители программ и машин, реализующих firewall-технологии, обеспечивают различные способы задания правил и процедур. Обычно firewall создает контрольные записи, детализирующие причину и обстоятельства возникновения внештатных ситуаций. Анализируя такие контрольные записи, администраторы часто могут обнаружить источники атаки и способы ее проведения.

Фильтрация пакетов (packet filtering firewalls)

Каждый IP-пакет проверяется на совпадение заложенной в нем информации с допустимыми правилами, записанными в firewall.

Параметры, которые могут проверяться:

- физический интерфейс движения пакета;
- адрес, с которого пришел пакет (источник);
- адрес, куда идет пакет (получатель);
- тип пакета (TCP, UDP, ICMP);
- порт источника;
- порт получателя.

Механизм фильтрации пакетов не имеет дела с их содержанием. Это позволяет использовать непосредственно ядро операционной системы для задания правил. В сущности, создаются два списка: отрицание (deny) и разрешение (permit). Все пакеты должны пройти проверку по всем пунктам этого списка. Далее используются следующие методы:

- если никакое правило соответствия не найдено, то удалить пакет из сети;
- если соответствующее правило найдено в списке разрешений, то пропустить пакет;
- если соответствующее правило найдено в списке отрицаний, то удалить пакет из сети.

В дополнение к этому firewall, основанный на фильтрации пакетов, может изменять адреса источников пакетов, выходящих наружу, чтобы скрыть тем самым топологию сети (метод address translation), плюс осуществляет условное и безусловное перенаправление пакетов на другие хосты. Отметим преимущества firewall, основанного на фильтрации пакетов:

- фильтрация пакетов работает быстрее других firewall-технологий, потому что используется меньшее количество проверок;
- этот метод легко реализуем аппаратно;
- одно-единственное правило может стать ключевым при защите всей сети;
- фильтры не требуют специальной конфигурации компьютера;

- метод address translation позволяет скрыть реальные адреса компьютеров в сети.

Однако имеются и недостатки:

- нет проверки содержимого пакетов, что не дает возможности, например, контролировать, что передается по FTP. В этом смысле application layer и circuit level firewall гораздо практичнее;
- нет информации о том, какой процесс или программа работали с этим пакетом, и сведений о сессии работы;
- работа ведется с ограниченной информацией пакета;
- в силу «низкоуровневости» метода не учитывается особенность передаваемых данных;
- слабо защищен сам компьютер, на котором запущен firewall, то есть предметом атаки может стать сам этот компьютер;
- нет возможности сигнализировать о внештатных ситуациях или выполнять при их возникновении какие-либо действия;
- возможно, что большой объем правил будет тормозить проверку.

Firewall цепного уровня (circuit level firewalls)

Поскольку при передаче большой порции информации она разбивается на маленькие пакеты, целый фрагмент состоит из нескольких пакетов (из цепи пакетов). Firewall цепного уровня проверяет целостность всей цепи, а также то, что она вся идет от одного источника к одному получателю, и информация о цепи внутри пакетов (а она там есть при использовании TCP) совпадает с реально проходящими пакетами. Причем цепь вначале собирается на компьютере, где установлен firewall, а затем отправляется получателю. Поскольку первый пакет цепи содержит информацию о всей цепи, то при попадании первого пакета создается таблица, которая удаляется лишь после полного прохождения цепи. Содержание таблицы следующее:

- уникальный идентификатор сессии передачи, который используется для контроля;
- состояние сессии передачи: установлено, передано или закрыто;
- информация о последовательности пакетов;
- адрес источника цепи;
- адрес получателя цепи;
- физический интерфейс, используемый для получения цепи;
- физический интерфейс, используемый для отправления цепи.

Эта информация применяется для проверки допустимости передачи цепи. Правила проверки, как и в случае фильтрации пакетов, задаются в виде таблиц в ядре. Основные преимущества firewall цепного уровня:

- firewall цепного уровня быстрее программного, так как производит меньше проверок;
- firewall цепного уровня позволяет легко защитить сеть, запрещая соединения между определенными адресами внешней и внутренней сети;
- возможно скрытие внутренней топологии сети. Недостатки firewall цепного уровня:
- нет проверки пакетов на программном уровне;
- слабые возможности записи информации о нештатных ситуациях, кроме информации о сессии передачи;
- нет проверки передаваемых данных;
- трудно проверить разрешение или отрицание передачи пакетов.

Firewall программного уровня

Помимо целостности цепей, правильности адресов и портов, проверяются также сами данные, передаваемые в пакетах. Это позволяет проверять целостность данных и отслеживать передачу таких сведений, как пароли. Вместе с firewall программного уровня используется proxy-сервис, который кэширует информацию для более быстрой ее

обработки. При этом возникают такие новые возможности, как, например, фильтрация URL и установление подлинности пользователей. Все соединения внутренней сети с внешним миром происходят через proxy, который является шлюзом. У proxy две части: сервер и клиент. Сервер принимает запросы, например на telnet-соединение из внутренней сети с внешней, обрабатывает их, то есть проверяет на допустимость передачи данных, а клиент работает с внешним компьютером от имени реального клиента. Естественно, вначале все пакеты проходят проверку на нижних уровнях. Достоинства proxy:

- понимает и обрабатывает протоколы высокого уровня типа HTTP и FTP;
- сохраняет полную информацию о сессии передачи данных как низкого, так и высокого уровня;
- возможен запрет доступа к некоторым сетевым сервисам;
- есть возможность управления пакетами данных;
- есть сокрытие внутренних адресов и топологии сети, так как proxy является фильтром;
- остается видимость прямого соединения сетей;
- proxy может перенаправлять запросы сетевых сервисов на другие компьютеры;
- есть возможность кэширования http-объектов, фильтрации URL и установления подлинности пользователей;
- возможно создание подробных отчетных записей для администратора. Недостатки proxy:
- требует изменения сетевого стека на машине, где стоит firewall;
- нельзя напрямую запустить сетевые сервисы на машине, где стоит firewall, так как proxy перехватывает работу портов;
- неминуемо замедляет работу, потому все данные обрабатываются дважды: «родной» программой и собственно proxy;
- так как proxy должен уметь работать с данными какой-либо программы, то для каждой программы нужен свой proxy;
- нет proxy для UDPи RPC;
- иногда необходима специальная настройка клиента для работы с proxy;
- proxy не защищен от ошибок в самой системе, а его работа сильно зависит от наличия последних;
- корректность работы proxy напрямую связана с правильностью обработки сетевого стека;
- использование proxy может требовать дополнительных паролей, что неудобно для пользователей.

Динамическая фильтрация пакетов (dynamic packet filter firewalls)

В основном этот уровень повторяет предыдущий, за двумя важными исключениями:

- возможно изменение правил обработки пакетов «на лету»;
- включена поддержка UDP.

Уровень kernel proxy

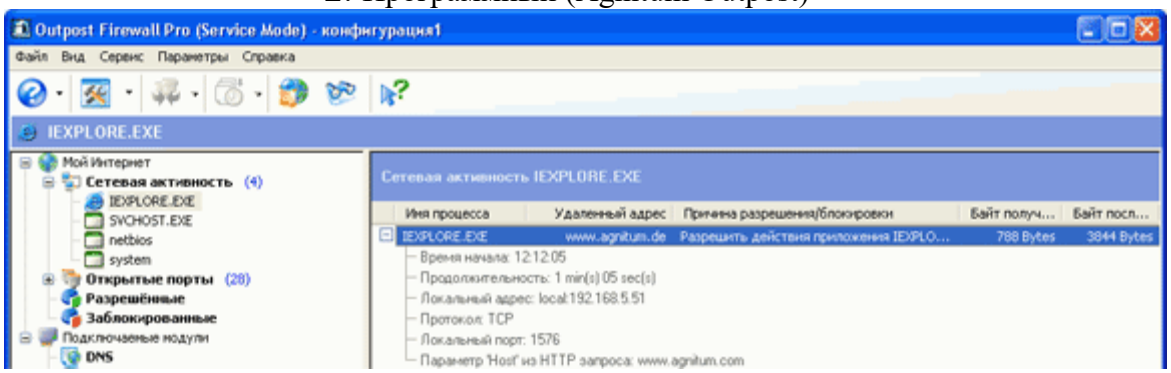
Уровень kernel proxy возник достаточно недавно. Основная его идея — попытка поместить описанный выше алгоритм firewall программного уровня в ядро операционной системы, что избавляет компьютер от лишних затрат времени на передачу данных между ядром и программой proxy. Это повышает производительность и позволяет производить более полную проверку проходящей информации.

Примеры межсетевых экранов

1. Аппаратный (D-Link)

DFL-1100
Межсетевой экран для сетей крупных предприятий

2. Программный (Agnitum Outpost)



Вспомогательные системы обеспечения безопасности компьютерных сетей - сканеры.

Архитектура сканера

Основной принцип функционирования сканера заключается в эмуляции действий потенциального злоумышленника по осуществлению сетевых атак. Поиск уязвимостей путем имитации возможных атак является одним из наиболее эффективных способов анализа защищенности АС, который дополняет результаты анализа конфигурации по шаблонам, выполняемый локально с использованием шаблонов (списков проверки). Современные сканеры способны обнаруживать сотни уязвимостей сетевых ресурсов, предоставляющих те или иные виды сетевых сервисов. Их предшественниками считаются сканеры телефонных номеров (war dialers), использовавшиеся с начала 80-х и непотерявшие актуальности по сей день. Первые сетевые сканеры представляли собой простейшие сценарии на языке Shell, сканировавшие различные TCP- порты. Сегодня они превратились в зрелые программные продукты, реализующие множество различных сценариев сканирования. Современный сетевой сканер выполняет четыре основные задачи:

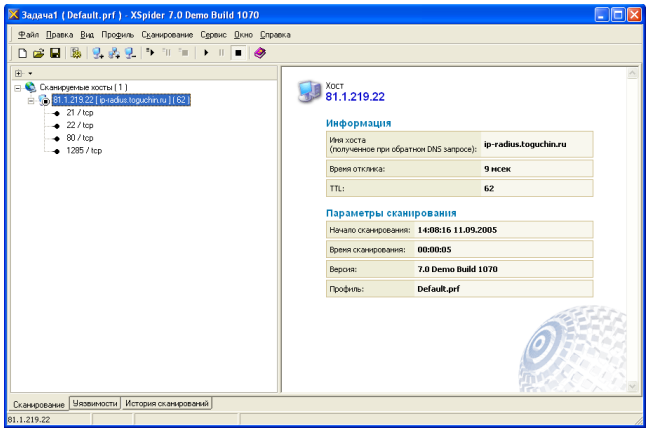
- Идентификацию доступных сетевых ресурсов;
- Идентификацию доступных сетевых сервисов;
- Идентификацию имеющихся уязвимостей сетевых сервисов;
- Выдачу рекомендаций по устранению уязвимостей.

В функциональность сетевого сканера не входит выдача рекомендаций по использованию найденных уязвимостей для реализации атак на сетевые ресурсы. Возможности сканера по анализу уязвимостей ограничены той информацией, которую могут предоставить ему

доступные сетевые сервисы. Принцип работы сканера заключается в моделировании действий злоумышленника, производящего анализ сети при помощи стандартных сетевых утилит, таких как host, showmount, traceout, rusers, finger, ping и т. п. При этом используются известные уязвимости сетевых сервисов, сетевых протоколов и ОС для осуществления удаленных атак на системные ресурсы и осуществляется документирование удачных попыток.

Число уязвимостей в базах данных современных сканеров медленно, но уверенно приближается к 10000.

Пример сканера XSpider



1. Порядок выполнения работы.

Условия выполнения практической работы. Данная работа должна выполняться в присутствии администратора компьютерного класса или уполномоченного им лица, которому предоставляются права на осуществление следующих действий в операционных системах Windows XP, работающих как в сетевом режиме, так и в одиночном режиме:

- права на установку программного обеспечения;
- права на работу как в составе рабочей группы или домена Windows, так и в составе локального администратора рабочей станции;
- права на предоставление учетной записи учащимся, позволяющей установку ПО.

Практическая работа проводится в двух вариантах:

1. Автономный.

В компьютерном классе должны находиться не менее 2-х машин, объединенных в сеть. На первой устанавливается *сетевой сканер* или *межсетевой экран*. В случае установки МСЭ вторая машина используется для тестирования защиты первой от ICMP пакетов с помощью стандартной утилиты *ping*. При «автономном» тестировании сканера вторая машина будет использоваться в качестве исследуемого объекта.

2. Совместный.

В компьютерном классе должны находиться также не менее 2-х машин, объединенных в сеть. На части из них устанавливается *сканер*, на остальных – МСЭ. При этом для проверки защиты рабочей станции от ICMP пакетов с помощью МСЭ (а также для тестирования сканера) будет использоваться сетевой сканер.

Администратор! Обрати внимание. После установки изучаемого ПО межсетевые экраны могут заблокировать доступ сетевого трафика к рабочим станциям, тем самым,

нарушив работоспособность сети. Для предотвращения данной ситуации необходимо сразу назначить всем МСЭ политику «разрешения».

Порядок работы

Работа будет проходить в два этапа. Первый этап предназначен для изучения работы XSpider, Outpost и WindowsXP в «автономном» режиме. Второй этап – для изучения работы в совместном режиме. На каждом этапе студенты делятся на две группы, одна из которых будет работать с МСЭ, вторая – со сканером или псевдосканером (утилитой ping).

Действия, общие для двух этапов:

1. Взять из папки \\m00\fit2005 файлы установки сканера XSpider и МСЭ Agnitum Outpost;
2. На каждом рабочем месте выполнить установку сканера и МСЭ;
3. При установке Outpost соглашаться со всеми вопросами. По окончании установки – перезагрузить машину;
4. Перед началом работы перевести установленный МСЭ в режим разрешения. Открыть Outpost -> меню «Параметры» -> «Политики» -> выбрать режим «Разрешать»;
5. Узнать имя и IP-адрес своего рабочего компьютера: «Пуск» -> «Выполнить» -> “cmd” -> “ipconfig /all”;

Этап 1. Автономный режим. Каждый студент из группы 1 должен работать в паре со студентом из группы 2.

Группа 1:

1. Запустить пинг компьютера-соседа из группы 2: «Пуск» -> «Выполнить» -> “cmd” -> “ping ip-addr -t”; (утилита ping располагается в C:\windows\system32)
2. Смотреть на ответные пинг-пакеты.
3. Фиксировать моменты, когда ответные пакеты пропадают и появляются.
4. Сравнить данные с моментами изменения конфигурации МСЭ напарником

Группа 2:

1. Открыть Outpost;
2. Зайти в меню «Параметры» -> «Системные» -> «ICMP параметры» -> отключить/включить эхо-запросы и ответы;
3. Проверить состояние ответов на ping-запросы у напарника;
4. Повторить п.1-2 несколько раз.

Поменяться с напарником ролями и повторить вышеуказанные пункты.

Этап 2. Совместный режим. Каждый студент из группы 1 должен работать в паре со студентом из группы 2.

Группа 1:

1. Запустить утилиту сканирования сети XSpider;
2. В меню «Правка» выбрать «Добавить хост»;
3. Введите IP-адрес хоста напарника;

4. Узнать у напарника текущий режим работы МСЭ;
5. В меню «Сканирование» выберите «Старт все»;

Начнется попытка XSpider сканировать указанный хост. В случае, если на целевом хосте отключены ICMP-ответы, то сканирование происходить не будет без установки в XSpider специальной опции: меню «Профиль» ->

«Редактировать текущий» -> «Поиск хостов» -> поставить галочку «Сканировать не отвечающие хосты».

6. Сбросить флаг «Сканировать не отвечающие хосты» для возврата XSpider в первоначальную конфигурацию.

Группа 2:

1. Открыть Outpost;
2. Зайти в меню «Параметры» -> «Системные» -> «ICMP параметры» -> отключить/включить эхо-запросы и ответы;
3. Проверить, как работает XSpider у напарника;
4. Повторить п.1-2 несколько раз для двух режимов XSpider – требующего ICMP-ответа и не требующего.

Поменяться с напарником ролями и повторить вышеуказанные пункты.

По завершению практической работы установленное в процессе занятия ПО необходимо удалить из системы.

Контрольные вопросы:

1. Опишите утилиту ping, методы и случаи ее применения.
2. Описать данные, полученные о компьютере напарника с помощью XSpider
3. Какого типа уязвимости были найдены?
4. Как можно предотвратить появление таких уязвимостей с помощью изученных средств?
5. Какие еще сканеры и МСЭ вы знаете? Какие между ними и изученными отличия?

Лабораторная работа № 3. Резервное копирование программ, системных параметров и файлов

Цель: изучить возможности резервного копирования в ОС Window

Формируемые компетенции или их части

№ п/п	Содержание компетенции	Шифр
1.	Способен проводить сопровождение ИТ инфраструктуры	ПК-2

Теоретическая часть

Задание 1. Изучите теоретический материал темы, выполните конспект в тетради.

С помощью элемента Панели управления Архивация и восстановление можно:

- ✓ Выполнять архивацию заданных папок по расписанию и восстанавливать их из резервной копии
- ✓ создать полный образ системы
- ✓ создать загрузочный диск для восстановления **Windows 10**

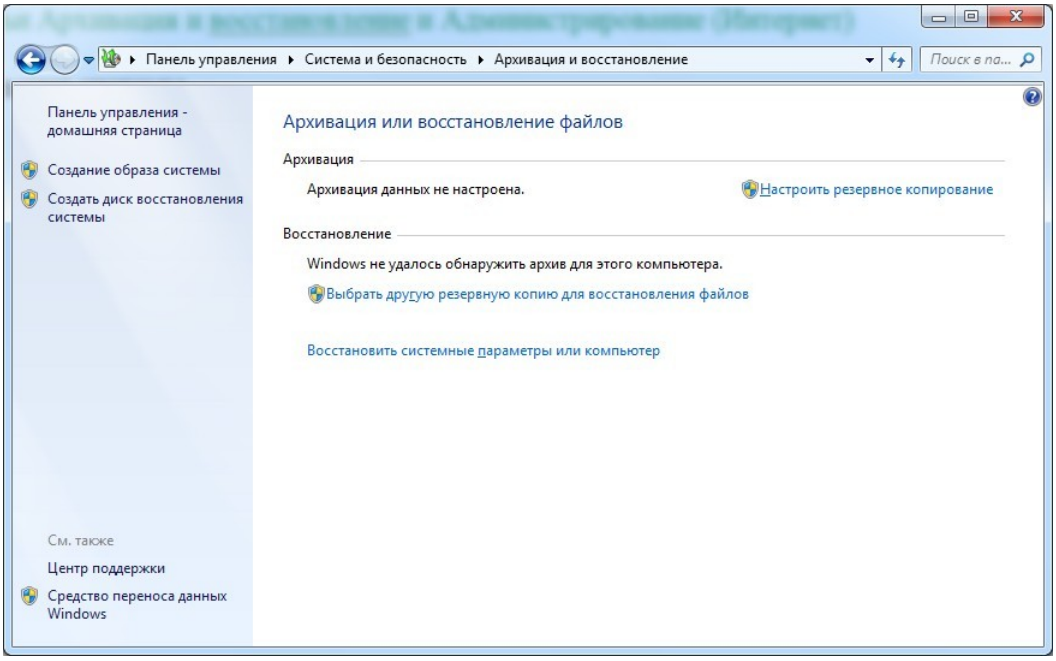


Рис. 1. Диалоговое окно Архивация и восстановление

Windows 10 позволяет пользователю создавать как резервные копии папок, так и полный образ разделов жесткого диска.

Тип архивации	**Технология и возможности**
Пользовательские файлы	Архивация производится на уровне файлов. Сохранение резервных копий возможно на разделы NTFS и FAT32. Добавления к первоначальному архиву происходят инкрементно (т. е. добавляются только изменившиеся файлы).

	Для сжатия используется формат ZIP. Имеется возможность восстановления отдельных папок и библиотек.
Образ раздела	Архивация производится на уровне блоков (в архив включаются только используемые блоки). Сохранение резервных копий возможно только на разделы NTFS. Полный образ сохраняется в формате VHD, при этом сжатия файлов не происходит. В дальнейшем образы создаются инкрементно, т. е. добавляются только изменившиеся блоки. Для этого используется функционал теневых копий. Последующее создание полных образов также возможно. Образы разделов дают возможность быстрого восстановления ОС и файлов в случае выхода из строя жесткого диска.

Эти функции в совокупности с возможностью загрузки в среду восстановления без установочного диска способны удовлетворить запросы большинства пользователей. Теперь вполне можно обходиться без сторонних программ резервного копирования.

Изменения в пользовательском интерфейсе

Изменения в возможностях архивации **Windows 10** затронули не только технологии, но и пользовательский интерфейс. В частности:

- ✓ переработан интерфейс главного окна элемента панели управления **Архивация и восстановление**
- ✓ создан новый пользовательский интерфейс для управления пространством, занятым под резервные копии
- ✓ упрощено восстановление файлов, выполняющееся с помощью мастера
- ✓ реализована интеграция с центром поддержки для своевременного уведомления пользователей о необходимости создания резервной копии

Настройка параметров регулярного резервного копирования

По умолчанию резервное копирование не настроено. Щелкните ссылку **Настроить резервное копирование** в главном окне элемента **Панели управления**, чтобы задать параметры архивации.

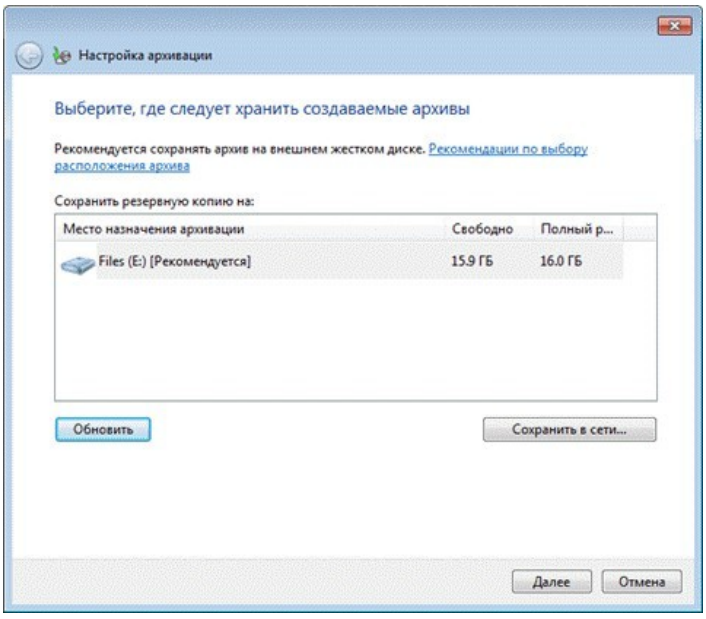


Рис. 2. Диалоговое окно Настройка архивации

Варианты размещения резервной копии файлов

Размещение	**Комментарии**
Внутренний жесткий диск	Вы можете разместить архивные файлы на: несистемном разделе того же физического диска, на котором установлена ОС любом разделе другого физического диска Рекомендуется второй вариант, ибо в случае выхода из строя системного диска вы потеряете как операционную систему, так и резервные копии.
Внешний жесткий диск	Если настроена архивация по расписанию, внешний жесткий диск должен быть подключен на момент создания резервной копии. **Примечание:** Windows 10 не поддерживает создание образов на USB дисках с флэш-памятью.
Локальная сеть	Поддерживается архивация только на компьютеры сети, работающие под управлением Windows 10. Пользователю потребуются учетные данные для доступа к компьютеру, на котором размещается резервная копия.

Вы можете размещать архивы файлов на разделах, отформатированных как в файловую систему NTFS, так и в FAT32. При архивации на жесткий диск файлы размещаются в корневом каталоге раздела. Для архива нельзя задать вложенную папку, но можно размещать на этом диске другие файлы и папки.

Определившись с размещением архива, необходимо задать параметры архивации. Можно предоставить это решение операционной системе, а можно выбрать папки самостоятельно.

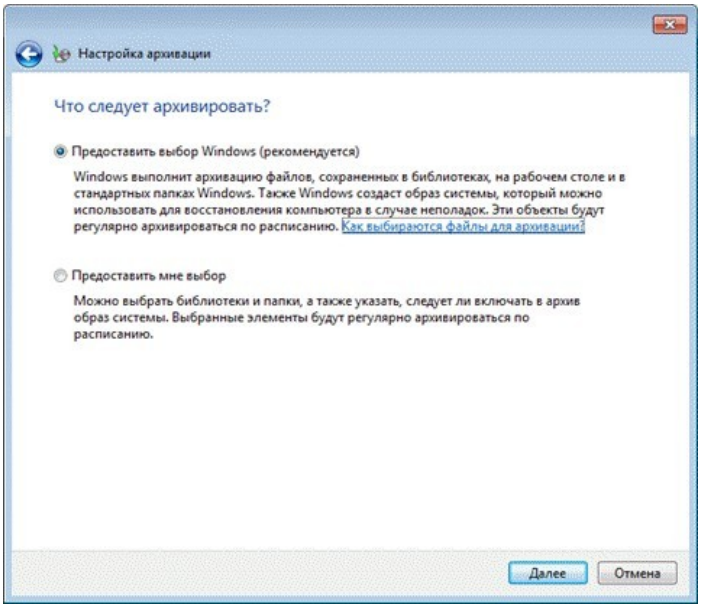


Рис. 3. Диалоговое окно Настройка архивации

При самостоятельном выборе можно создать резервные копии:

- ✓ пользовательских файлов, включая библиотеки
- ✓ папок локального диска
- ✓ полного образа системы

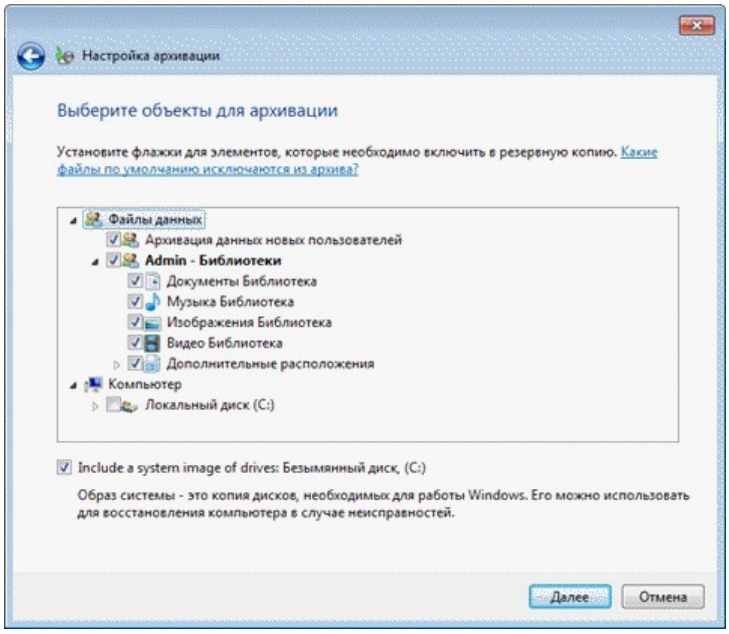


Рис. 4. Диалоговое окно Настройка архивации

В конце **Windows 10** выводит сводку параметров резервного копирования.

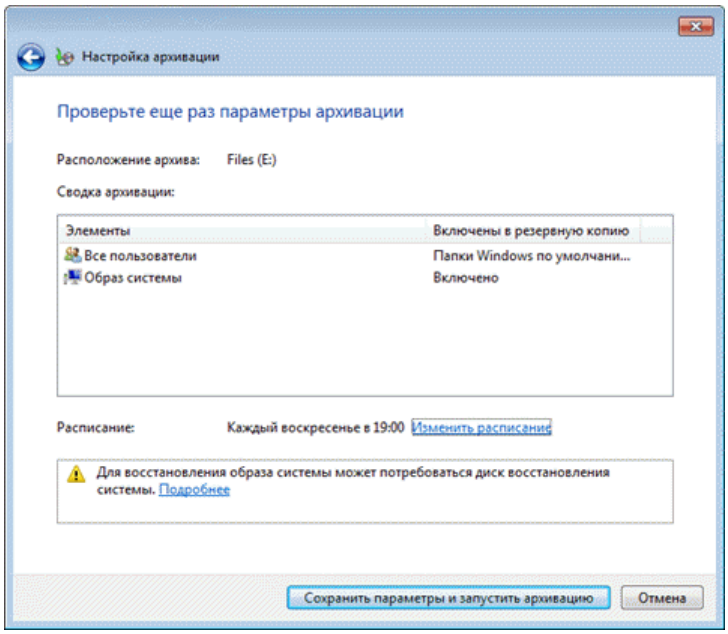


Рис. 5. Диалоговое окно Настройка архивации

Щелкните ссылку **Изменить расписание**, чтобы настроить резервное копирование по расписанию в удобное вам время.

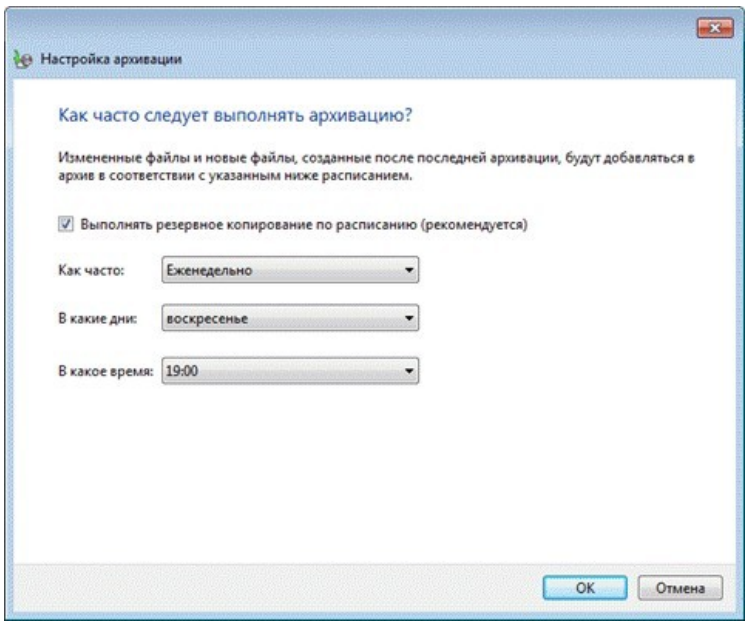


Рис. 6. Диалоговое окно Настройка архивации

Заданные параметры расписания сохраняются в **планировщике заданий**, который отвечает за своевременный запуск архивации.

По завершении настройки параметров архивации пользователь возвращается в главное окно элемента **Панели управления**.

Создание резервной копии файлов

Теперь в главном окне отображаются все параметры архивации. Нажмите кнопку **Архивировать**, чтобы начать процесс резервного копирования.

Ход архивации отображается с помощью полосы прогресса, но вы можете посмотреть подробности, нажав кнопку **Просмотр сведений**.

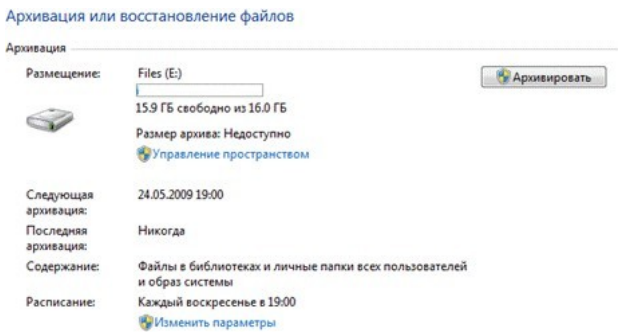


Рис. 7. Диалоговое окно Архивация или восстановление файлов

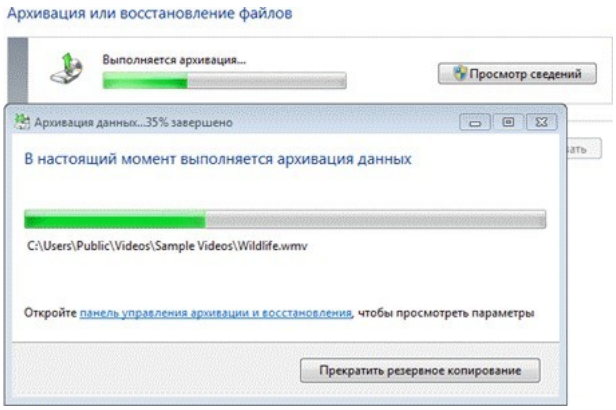


Рис. 8. Диалоговое окно выполнения архивации файлов

Завершив архивацию, можно посмотреть сведения об используемом дисковом пространстве и перейти к управлению архивами.

Создание образа системы

В отличие от файловых архивов, системный образ можно сохранить только на диске, отформатированном в файловую систему **NTFS**. Это обусловлено тем, что образы представляют собой файлы в формате **VHD**, размер которых может превышать 4 Гб (предельный размер файла для FAT32).

Первый системный образ представляет собой полный снимок раздела, а последующие являются инкрементными, т. е. включают в себя лишь изменения по сравнению с предыдущим образом. Эта возможность, позволяющая сэкономить дисковое пространство, реализована с помощью теневых копий. Такой принцип создания образов применяется при их сохранении на внутренних, внешних и оптических дисках. Для внутренних и внешних дисков этот принцип действует до тех пор, пока на диске имеется достаточно места. Когда место заканчивается, создается полный образ, а все предыдущие удаляются. Что же касается сетевых дисков, то на них всегда создается полный образ, а старый образ при этом перезаписывается новым.

Рассмотрим создание первого образа.

- ✓ В левой панели элемента **Архивация и восстановление** нажмите ссылку **Создание образа системы**. Откроется окно с вариантами размещения образа.
- ✓ На следующем шаге вы сможете выбрать разделы для архивации.

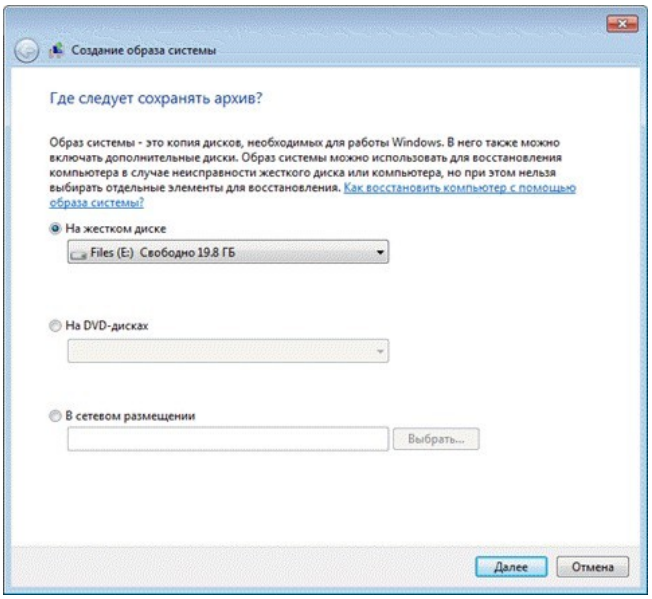


Рис. 9. Создание образа системы – шаг 1

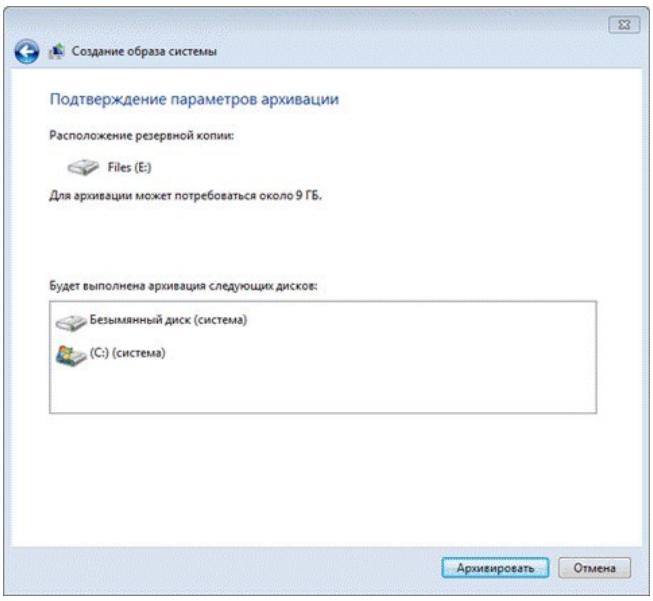


Рис. 10. Создание образа системы – шаг 2

✓ В образ автоматически включается **служебный раздел со средой восстановления (Windows RE)** и **системный раздел**. Исключить их из резервной копии нельзя. Если в системе имеются другие разделы, вы сможете выбрать их на этом шаге. Определившись с выбором разделов, нажмите кнопку **Архивировать**, чтобы начать процесс создания резервной копии.

Все следующие образы создаются точно так же. Они содержат только изменившиеся блоки. Для того чтобы снова создать полный образ системы, вам необходимо удалить существующие образы или перенести их на другой раздел. Вы также можете переместить их из корневого каталога диска во вложенные папки, однако примите к сведению, что в этом случае их не увидит программа восстановления системы из образа.

Управление пространством

✓ В главном окне элемента панели управления **Архивация и восстановление** щелкните ссылку **Управление пространством**. Откроется окно, в котором выводится информация о расположении архива, сводка об использовании дискового пространства, а также ссылки и кнопки для просмотра архивов и управления ими.

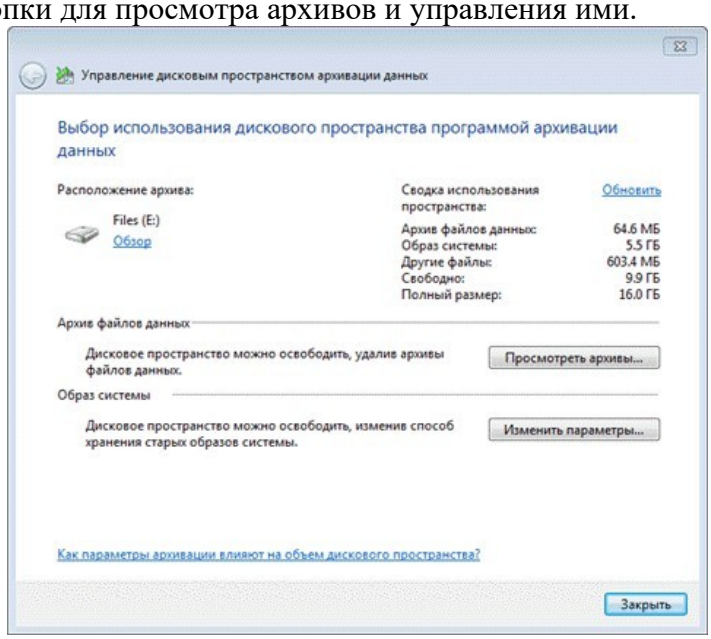


Рис. 11. Диалоговое окно Управление дисковым пространством архивации

Расположение резервных копий

Помимо просмотра подробных сведений об используемом пространстве, можно открыть место хранения резервной копии - нажмите ссылку **Обзор**, и файлы откроются в Проводнике. Windows 10 распознает папку с архивом и предоставляет доступ к параметрам восстановления.

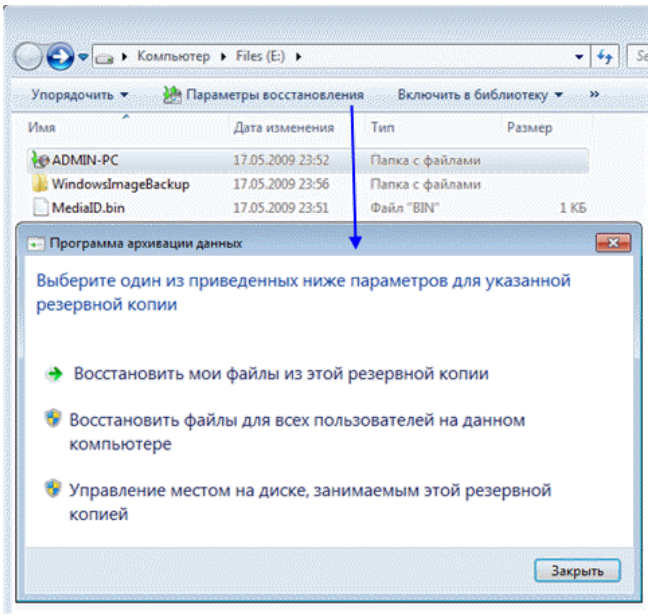


Рис. 12. Определение расположения резервных копий

Из списка папки:

- ✓ **%COMPUTERNAME%** (в данном случае **ADMIN-PC**) - архив файлов
- ✓ **WindowsImageBackup -** папка с образом раздела

Содержимое файлового архива

Открыть папку с архивом можно с помощью контекстного меню. Содержимое архива прозрачно для пользователя - внутри ZIP-архивы, и при желании файлы можно оттуда извлечь непосредственно из Проводника.

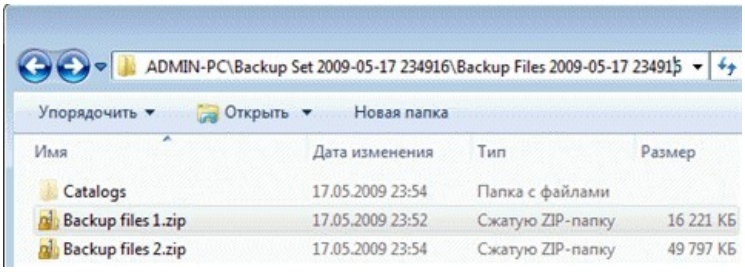


Рис. 13. Содержимое архива

Однако из **Панели управления** восстанавливать файлы удобнее, например, благодаря встроенному поиску.

Содержимое образа

Архивный образ системы создается в формате **VHD** и хранится в папке **WindowsImageBackup** наряду со вспомогательными файлами.

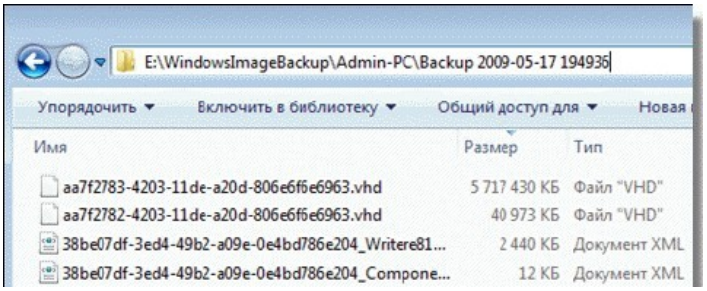


Рис. 14. Папка **WindowsImageBackup**

Увидеть его содержимое можно, воспользовавшись новой возможностью Windows 10 - подключением виртуальных жестких дисков в утилите управления дисками (**Пуск - Поиск - diskmgmt.msc - Действие - Присоединить виртуальный жесткий диск**).

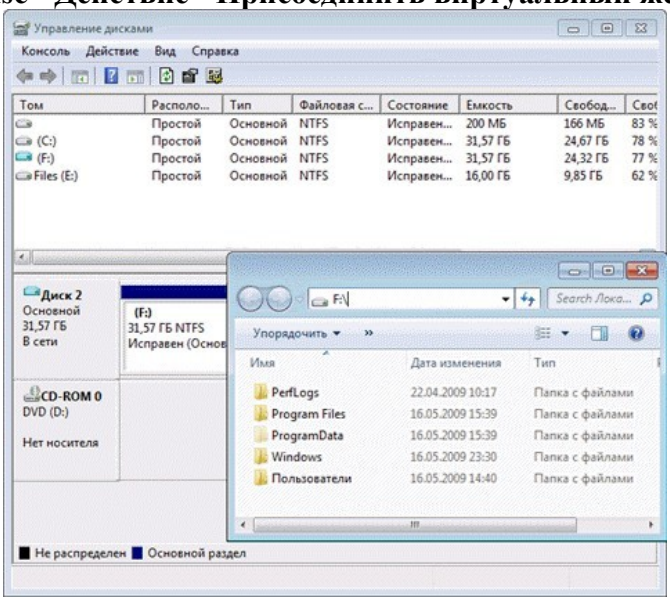


Рис. 15. Утилита Управление дисками

Возможно, вас заинтересует вопрос, можно ли добавить файлы на виртуальный жесткий диск. Технически это возможно, однако с точки зрения восстановления средствами Windows это ничего не даст. Лучше сделать новый образ - изменившиеся блоки добавляются инкрементно на основе теневых копий, что позволяет сэкономить дисковое пространство.

Просмотр и удаление резервных копий

Из окна управления пространством пользователь может удалять файловые архивы и резервные образы.

Нажмите кнопку **Просмотр архивов** в окне управления пространством, чтобы увидеть список архивов.

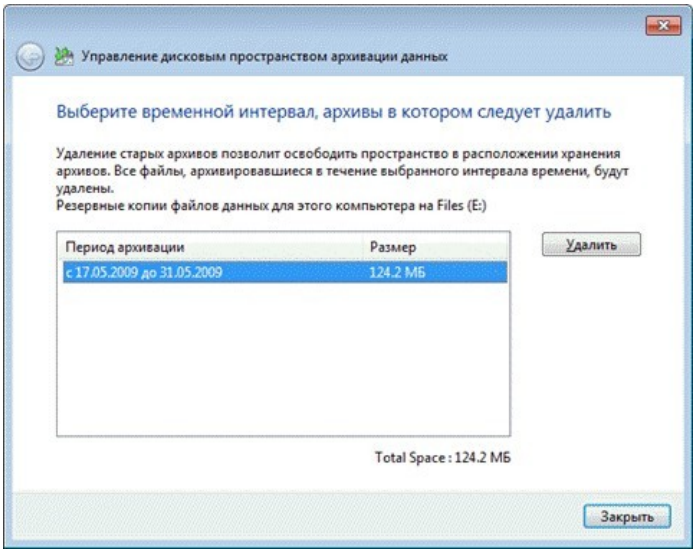


Рис. 16. Период архивации

Windows 10 находит все архивы и отображает период архивации и занимаемое дисковое пространство. В этом окне можно удалить ненужные архивы. Чтобы удалить резервные образы, нажмите кнопку **Изменить параметры** в окне управления пространством. Откроются параметры хранения образов.

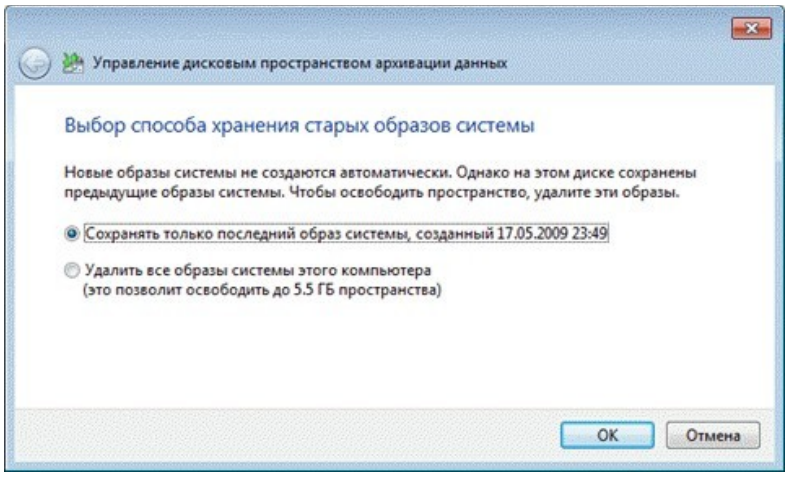


Рис. 17. Параметры удаления

Система предлагает пользователю удалить абсолютно все образы, либо все образы кроме последнего.

Рекомендации по резервному копированию

Все знают, что нужно регулярно выполнять резервное копирование, но при этом далеко не все его делают. Учитывая широкие возможности резервного копирования в Windows 10, о потере важных данных вы будете сожалеть только в том случае, если не настроите регулярную архивацию.

Для хранения резервных копий подойдет отдельный жесткий диск - внутренний или внешний, подключаемый по USB или FireWire. Если в вашем распоряжении есть сетевой диск, его также можно задействовать. Хранение резервных копий на другом

разделе того же диска, где установлена ОС, не является хорошей идеей. В случае выхода из строя диска вы потеряете как систему, так и резервные копии.

Общие рекомендации, которые нужно корректировать в зависимости от имеющегося свободного дискового пространства:

Образы системного раздела

- ✓ **Первый образ.** Установите Windows 10, затем все обновления и драйверы. Убедившись в нормальной работе ОС и устройств, создайте первый резервный образ.
- ✓ **Второй образ.** Установите все приложения и настройте систему по своему желанию. Поскольку более тонкая настройка ОС, как правило, производится по ходу ее использования, поработайте в Windows 10 пару недель. Убедившись в нормальной работе ОС, создайте второй резервный образ. Если перед этим вы удалите первый образ, у вас будет полный образ полностью обновленной и настроенной системы с любимым набором приложений.
- ✓ **Последующие образы.** В зависимости от имеющегося у вас свободного дискового пространства, создавайте последующие образы ежемесячно/ежеквартально. Если возникнет проблема, требующая восстановления из образа, вы сможете вернуться к относительно недавнему состоянию системы.

Архивы пользовательских файлов

- ✓ Частота архивации ваших файлов определяется тем, насколько они ценны для вас и как часто вы добавляете или создаете новые файлы. В общем случае рекомендуется выполнять архивацию еженедельно или два раза в месяц. В сочетании с ежемесячным созданием образов системы вручную у вас будет отличный резервный набор, позволяющий не только вернуть с систему к недавнему рабочему состоянию, но и восстановить все ваши данные и файлы. Вы всегда сможете освободить дисковое пространство, удалив старые архивы, если место на диске потребуется для других нужд.
- ✓ В графическом интерфейсе невозможно задать разные расписания для создания образов и архивации данных. Поэтому, если вы хотите в разное время автоматически создавать образ и выполнять архивацию файлов, воспользуйтесь утилитой командной строки **wbadmin** и **планировщиком заданий**.

Контрольные вопросы:

1. Перечислите типы архивации и их возможности, которые можно выполнить с помощью элемента Панели управления Архивация и восстановление
2. Перечислите варианты размещения резервной копии файлов
3. Опишите алгоритм создания резервной копии файлов
4. Опишите алгоритм создания резервной копии образа системы
5. Опишите возможности использования диалогового окна Управление пространством
6. Перечислите рекомендации по резервному копированию

Лабораторная работа № 4. Использование методов замены для шифрования данных

Цель: изучить классические шифры замены, научиться зашифровывать тексты с помощью шифров замены

Формируемые компетенции или их части

№ п/п	Содержание компетенции	Шифр
1.	Способен проводить сопровождение ИТ инфраструктуры	ПК-2

Теоретическая часть

Примеры классических шифров замены

Шифр Цезаря

Один из самых первых известных методов шифрования носит имя римского императора Юлия Цезаря, который если и не сам изобрел его, то активно им пользовался. Этот метод основан на замене каждой буквы шифруемого текста на другую путем смещения в алфавите от исходной буквы на фиксированное количество символов, причем алфавит читается по кругу, т.е. после буквы *я* рассматривается буква *а*. Регистр символов не учитывается. Так, например, слово **АЛФАВИТ** при смещении на три символа вправо кодируется словом **ГОЧГЕЛХ.** Пример выполнения задания на рис. 1

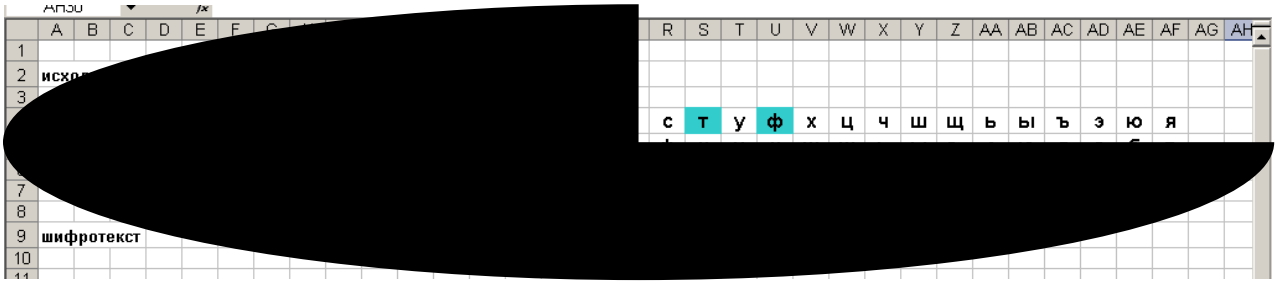


Рис. 1 Шифр Цезаря для слова АЛФАВИТ

С помощью шифра Цезаря можно выполнять расшифровку текста, при этом буквы шифротекста нужно выбирать на сдвинутом алфавите, соответствующие им буквы верхнего ряда будут составлять открытый текст. Пример дешифрования на рис. 2.

Рис. 2 Дешифрование текста

Задача 1. Расшифруйте слово **НУЛТХСЖУГЧЛВ,** закодированное с помощью шифра Цезаря. Известно, что каждая буква исходного текста заменяется третьей после нее буквой.

Задача 2. Зашифруйте слово **БЕЗОПАСНОСТЬ** с помощью шифра Цезаря, учитывая что каждая буква исходного текста заменяется пятой после нее буквой.

Шифр Тритемиуса

Некоторые трудности для криптоанализа представляет шифр, связываемый с именем ученого аббата Тритемиуса из Вюрцбурга. Этот шифр является развитием шифра Цезаря.

Зашифруем с помощью данного шифра фразу:

В связи с создавшимся положением отодвигаем сроки возвращения домой Рамзай

В качестве ключевого слова используем **ЗАПИСЬ Решение:**

Буквы алфавита нумеруются по порядку числами 0, 1, 30. При шифровании ключевое слово (или номера его букв) подписывается под сообщением с повторениями (рис. 3)

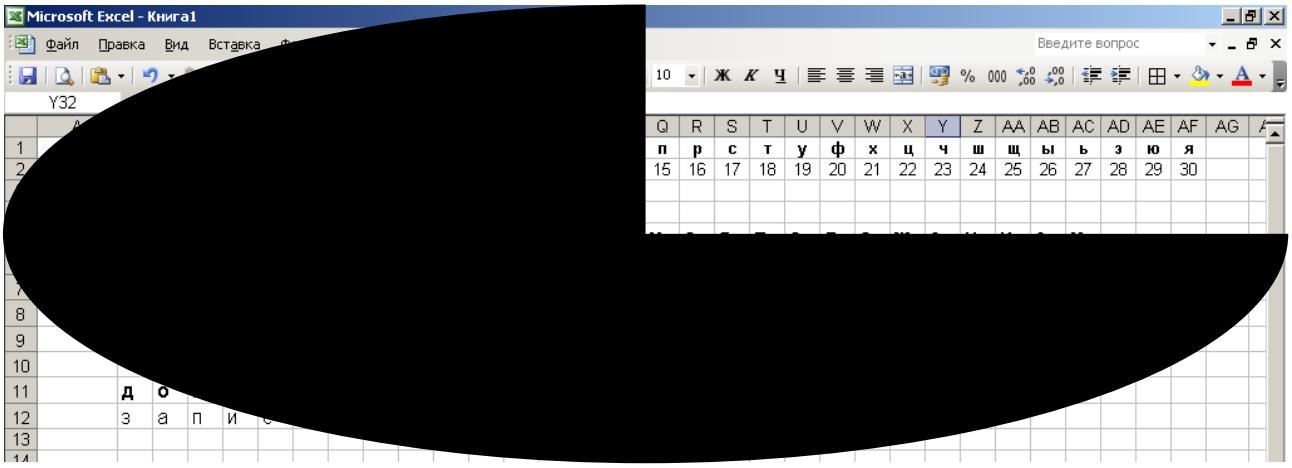


Рис. 3 Пример выполнения задания

Каждая буква сообщения и ключа заменяется на свой порядковый номер в алфавите (рис. 4), далее выполняются преобразования по определенному правилу.

Каждая буква сообщения «сдвигается» вдоль алфавита по следующему правилу: буква с номером *m,* под которой стоит буква ключевого слова с номером *k,* заменяется на букву с номером ***l=m+k*** **(если m+k<31)** или букву с но- мером ***l=m+k*—31 (если m+k≥31).** Например, первая буква «в» сдвигается на 7 букв и заменяется буквой «й», следующая буква «с» остается без изменения и т. д. Таким образом, номер l кодирующей буквы вычисляется по формуле:

l=m+k (mod 31).

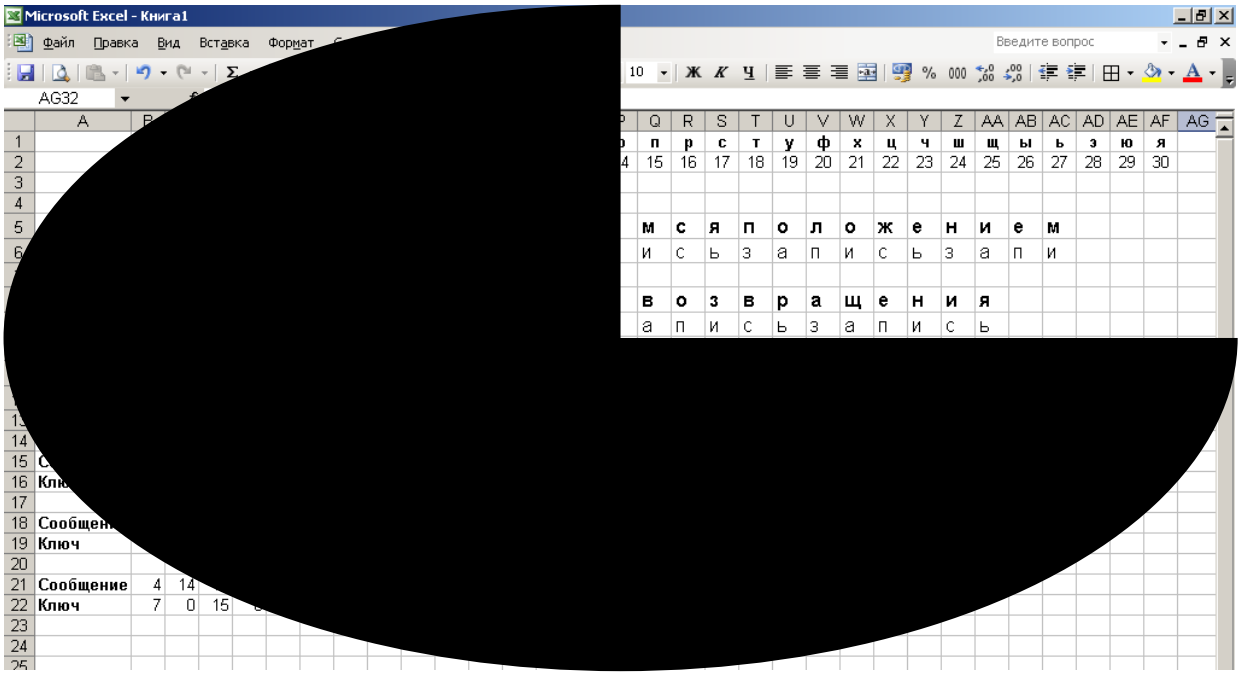


Рис. 4 Замена букв сообщения и ключа на их порядковые номера в алфавите После суммирования по модулю 31 получаем следующую последовательность чисел:

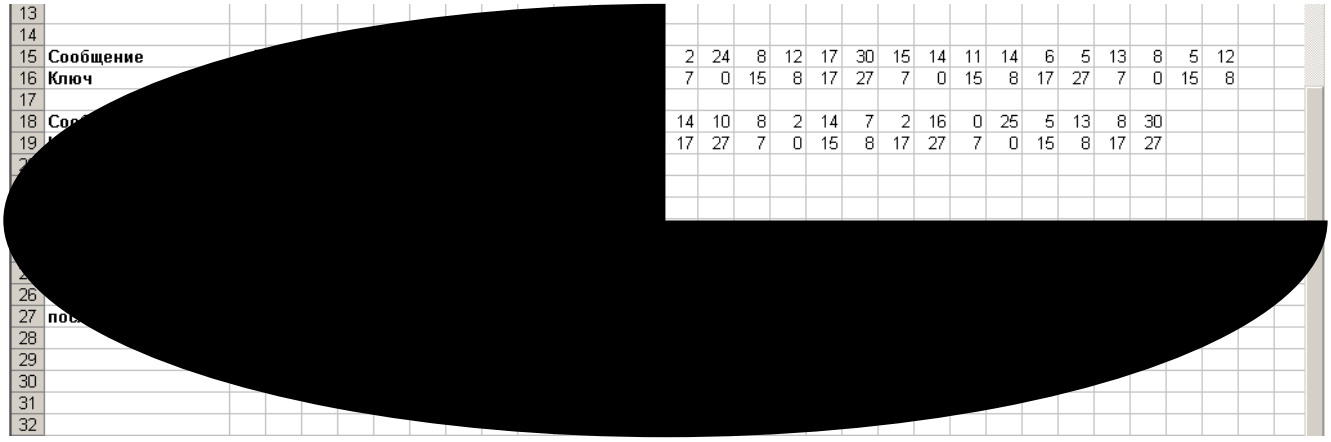


Рис. 5 Полученная числовая последовательность Далее, заменяя числа на буквы, получим шифротекст:

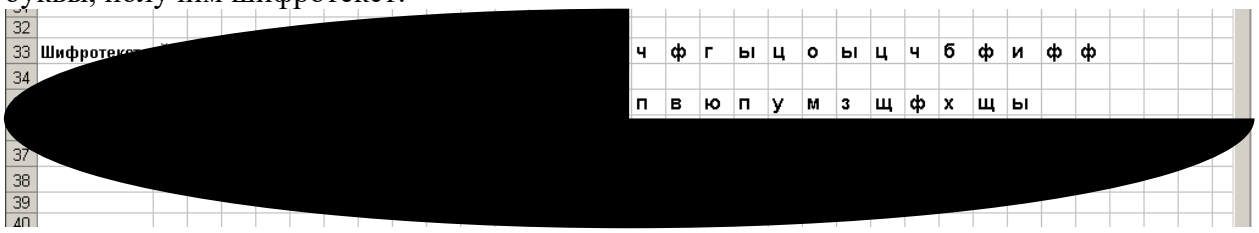


Рис. 6 Результат шифрования

Задача 3. С помощью шифра Тритемиуса зашифруйте текст:

А) СРОЧНО ПРИЕЗЖАЙ ИВАН Ключ БАЙТ

Б) ОТКРЫТЫМ ТЕКСТОМ НАЗЫВАЕТСЯ ИСХОДНОЕ СООБЩЕНИЕ Ключ МОЦАРТ

Шифр Вижинера

Таблица Вижинера представляет собой квадратную матрицу с n^2 элементами, где n — число символов используемого алфавита. На рис. 7 показана таблица Вижинера для кириллицы. Каждая строка получена циклическим сдвигом алфавита на символ.

Для шифрования выбирается буквенный ключ, в соответствии с которым формируется рабочая матрица шифрования (первое правило).

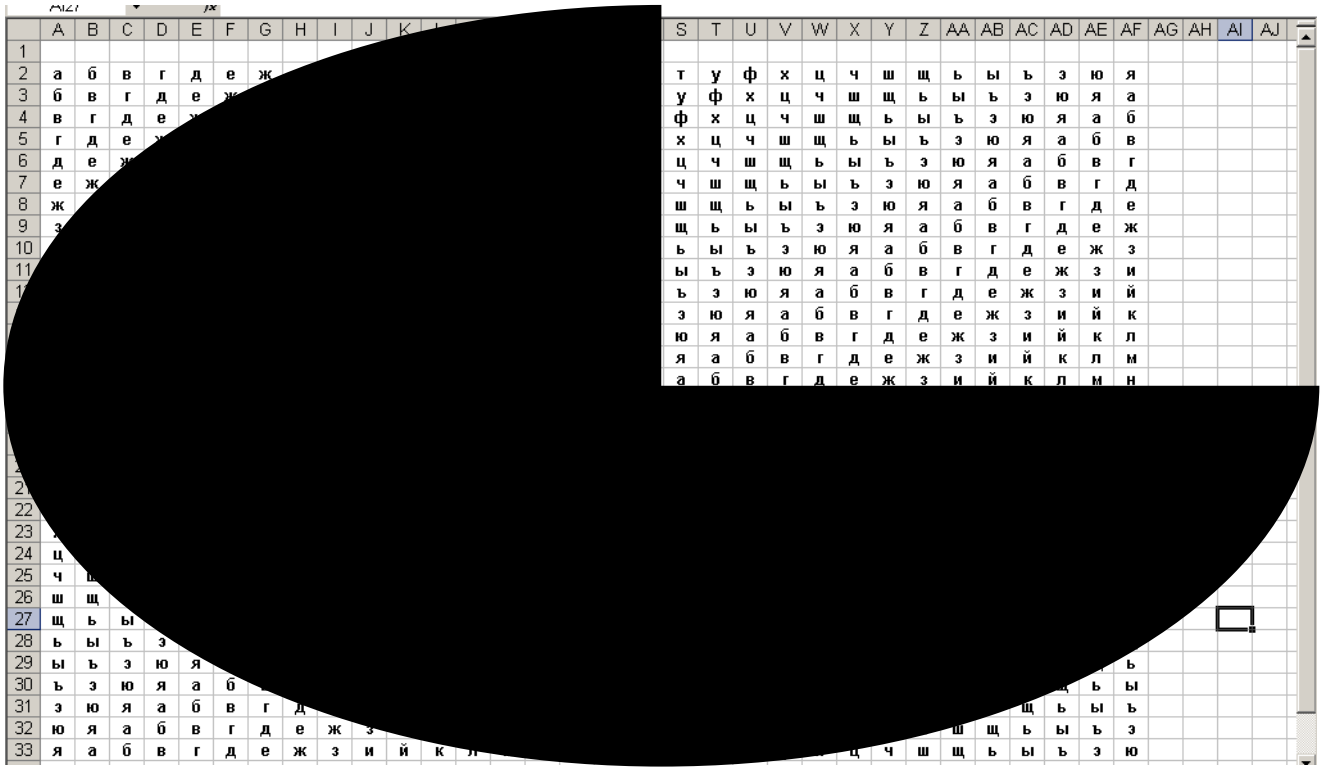


Рис. 7 Таблица Вижинера Осуществляется это следующим образом:

из полной таблицы выбирается первая строка и те строки, первые буквы которых соответствуют буквам ключа. Первой размещается первая строка, а под нею — строки, соответствующие буквам ключа в порядке следования этих букв в ключе. Пример такой рабочей матрицы для ключа **ВЕНТИЛЬ** приведен на рис. 8.

Процесс шифрования осуществляется следующим образом (второе правило):

1. под каждой буквой шифруемого текста записываются буквы ключа. Ключ при этом повторяется необходимое число раз;
2. каждая буква шифруемого текста заменяется по подматрице буквами, находящимися на пересечении линий, соединяющих буквы шифруемого текста в первой строке подматрицы и находящихся под ними букв ключа;
3. полученный текст может разбиваться на группы по нескольку знаков.

Пусть, например, требуется зашифровать фразу ГРУЗИТЕ АПЕЛЬСИНЫ БОЧКАМИ с помощью ключа ВЕНТИЛЬ

В соответствии с первым правилом записываем под буквами шифруемого текста буквы ключа и подготавливаем рабочую матрицу (рис. 6)

Рис. 8. Подготовка к шифрованию

Дальше осуществляется шифрование **в соответствии со вторым правилом:**

1. берем первую букву текста **(Г)** и соответствующую ей букву ключа **(В).**
2. по букве текста **(Г)** входим в матрицу шифрования и выбираем под ней букву, расположенную в строке, соответствующей букве ключа **(В),** - в нашем примере такой буквой является **Е**, выбранную таким образом букву помещаем в шифротекст. На рис. 9 показан алгоритм замены букв и шифр первого слова.

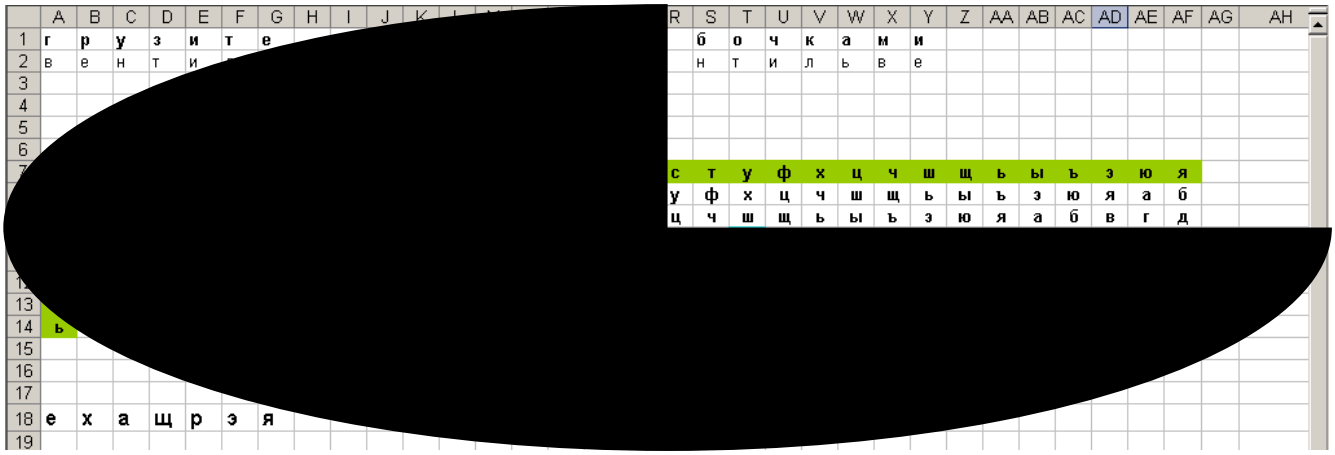


Рис. 9. Шифр первого слова

Задача 4. Самостоятельно закончите шифрование фразы

Задача 5. С помощью таблицы Вижинера зашифруйте фразу:

МАКСИМАЛЬНО ДОПУСТИМОЙ ЦЕНОЙ ЯВЛЯЕТСЯ ПЯТЬСОТ РУБЛЕЙ ЗА ШТУКУ

Ключ **САЛЬЕРИ**

Расшифровка текста производится в следующей последовательности:

1. над буквами зашифрованного текста последовательно записываются буквы ключа, причем ключ повторяется необходимое число раз,
2. в строке подматрицы Вижинера, соответствующей букве ключа, отыскивается буква, соответствующая знаку зашифрованного текста,
3. находящаяся над ней буква первой строки подматрицы и будет буквой исходного текста,
4. полученный текст группируется в слова по смыслу.

Задача 6. С помощью таблицы Вижинера расшифруйте:

А) слово ООЗЦБККГДХБ Ключ ВАГОН

Б) фразу УОЙНЮО ШТАЪАСМДШН Ключ МОРЕ

В) фразу ИИЫСЪЛНХТХ ДЗОЫДВ ЬЬРДПЧЦЧЬХШ ШСЦПЩГФЫПВСЖ РЮЙПРЪХЛБТАЛТХЧЛМП Й ЪКЫШШЭНВНЦ ЛТМШЪСЩГОХХ Ключ РАЗБОЙНИК

Дополнительное задание

Написать программу шифрования текста сообщения методами замены (подстановки) на любом языке программирования.

Отчет оформить в печатном и электронном видах. Продемонстрировать работу программы на произвольном сообщении

Контрольные вопросы:

1. Опишите алгоритм шифра Цезаря
2. Опишите алгоритм шифра Тритемиуса
3. Опишите правила шифрования по таблице Вижинера
4. Опишите правила расшифровки по таблице Вижинера
5. К какому классу шифров относятся перечисленные шифры?

Лабораторная работа № 5. Использование методов перестановки для шифрования данных

Цель: изучить классические шифры перестановки, научиться зашифровывать тексты с помощью шифров перестановки, познакомиться с основами криптоанализа

Формируемые компетенции или их части

№ п/п	Содержание компетенции	Шифр
1.	Способен проводить сопровождение ИТ инфраструктуры	ПК-2

Теоретическая часть

Классические шифры перестановки

При шифровании методом перестановки используются прямоугольные таблицы различной длины – высоты. Записывать в нее исходный текст можно разными способами: по строкам, по столбцам, по диагонали, по спирали и т.д. читать шифротекст можно также разными способами.

Самая простая перестановка — написать исходный текст задом наперед и одновременно разбить шифрограмму на пятерки букв. Например, из фразы

ПУСТЬ БУДЕТ ТАК, КАК МЫ ХОТЕЛИ

получится такой шифротекст:

ИЛЕТО ХЫМКА ККАТТ ЕДУБЬ ТСУП

В последней группе (пятерке) не хватает одной буквы. Значит, прежде чем шифровать исходное выражение, следует его дополнить незначащей буквой (например, О) до числа, кратного пяти:

ПУСТЬ-БУДЕТ-ТАККА-КМЫХО-ТЕЛИО

Тогда шифрограмма, несмотря на столь незначительное изменение, будет выглядеть по-другому:

ОИЛЕТ ОХЫМК АККАТ ТЕДУ Б ЬТСУП

Кажется, ничего сложного, но при расшифровке проявятся серьезные неудобства.

Во время Гражданской войны в США в ходу был такой шифр: исходную фразу писали в несколько строк. Например, по пятнадцать букв в каждой (с заполнением последней строки незначащими буквами).

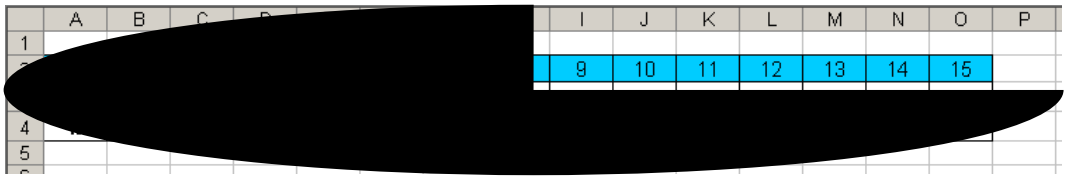


Рис. 1 Пример таблицы: текст записан по строкам

После этого вертикальные столбцы по порядку писали в строку с разбивкой на пятерки букв:

ПКУМС ЫТХЬО БТУЕД ЛЕИТК ТЛАМК НКОАП

Вариант этого шифра: сначала исходную фразу записать в столбики:

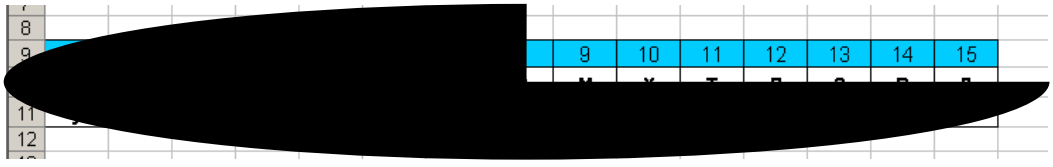


Рис. 2 Текст записан по столбцам

Потом разбить строки на пятерки букв:
ПСЬУЕ ТКАМХ ТЛАВД УТБДТ АККЫО ЕИБГЕ

Перестановки с ключом

При использовании ключа правила заполнения решетки и шифрования из нее упрощаются, становятся стандартными. Единственное, что надо помнить и знать, — это ключ, которым может быть любое слово, например **РАДИАТОР**. В соответствии с расположением букв в алфавите буква **А** получает номер **1**, вторая буква **А** — **2,** следующая по алфавиту буква **Д — 3,** потом **И — 4, О — 5,** первая буква **Р — 6,** вторая **Р — 7** и буква **Т — 8.** Заполняем решетку:

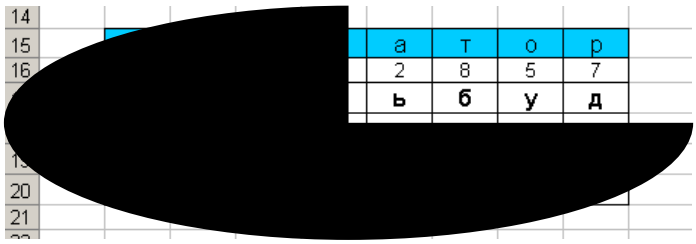


Рис. 3 Использование ключа

Записываем столбики в соответствии с номерами букв ключа:
УТЫ ЬКТ СТХ ТАО УАЛ ПЕМО ДКИ БКЕ
Затем последовательность опять разбивается на пятерки:
УТЫЬК ТСТХТ АОУАЛ ПЕМОД КИБКЕ

Таким шифром простой перестановки колонок пользовались немецкие секретные агенты во время Второй мировой войны. В качестве ключа они использовали первые буквы строк на определенной странице какой-нибудь обыкновенной книги.

Развитием этого шифра является **шифр перестановки колонок с пропусками,** которые располагаются в решетке тоже в соответствии с ключом (в нашем случае через 6-1-3-4-2-8-5-7 ... символов):

р	а	д	и	а	т	о	р
6	1	3	4	2	8	5	7
п	у	с	т	ь	б	*	у
*	д	е	т	*	т	а	к
к	*	а	к	*	м	ы	х
о	т	е	л	и	*	к	л

Рис. 4. Шифрование с пробелами

Шифрограмма будет такой:
УДТ ЬИ СЕАЕ ТТКЛ АЫК ПКО УКХЛ БТМ

Задача 1
С помощью табличной перестановки (без пробелов) зашифруйте фразу:
А) СРОЧНО ПРИЕЗЖАЙ ИВАН ключ **БАЙТ**

Б) В СВЯЗИ С СОЗДАВШИМСЯ ПОЛОЖЕНИЕМ ОТОДВИГАЕМ СРОКИ ВОЗВРАЩЕНИЯ ДОМОЙ. РАМЗАЙ Ключ **ЗАПИСЬ**

Задача 2

С помощью табличной перестановки (с пробелами) зашифруйте фразу:

В СВЯЗИ С СОЗДАВШИМСЯ ПОЛОЖЕНИЕМ ОТОДВИГАЕМ СРОКИ ВОЗВРАЩЕНИЯ ДОМОЙ. РАМЗАЙ Ключ **ЗАПИСЬ**

Шифрование методом перестановки по маршрутам

Преобразования из этого шифра состоят в том, что в фигуру исходный текст вписывается по ходу одного «маршрута», а затем по ходу другого выписывается с нее. **Такой шифр называют маршрутной перестановкой.**

Для примера возьмем решетку 6*6 (причем количество строк может увеличиваться или уменьшаться в зависимости от длины исходного сообщения) и заполним ее по строкам:

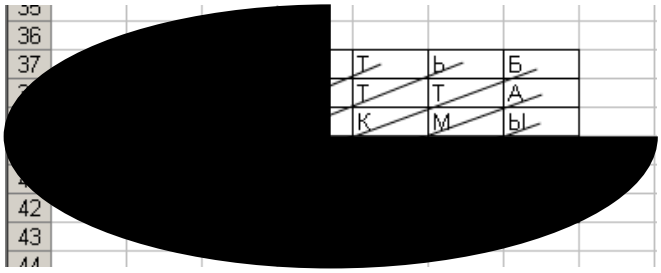


Рис. 5 Перестановка по диагонали

Если шифровать по стрелкам (диагоналям) сверху вниз с левого верхнего угла, то в итоге получится такая шифрограмма:

П УУ СДК ТЕКХ ЬТАОА БТКТБЖ АМЕВЗ ЫЛГИ ИДК ЕЛ М

Для окончательного оформления шифротекст может быть разбит на группы по 6 символов:

ПУУСДК ТЕКХЬТ АОАБТК ТБЖАМЕ ВЗЫЛГИ ИДКЕЛМ

Можно вписывать исходное сообщение в прямоугольную таблицу, выбрав такой маршрут: по горизонтали, начиная с левого верхнего угла поочередно слева направо и справа налево. Выписывать же сообщение будем по другому маршруту: по вертикали, начиная с верхнего правого угла и двигаясь поочередно сверху вниз и снизу вверх.
Зашифруем, например, указанным способом фразу:

ПРИМЕР МАРШРУТНОЙ ПЕРЕСТАНОВКИ

Для решения задачи заполним таблицу (рис. 5)

п	р	и	м	е	р	м
н	т	у	р	ш	р	а
о	й	п	е	р	е	с
и	к	в	о	н	а	т

Зашифрованная Фраза выглядит так:

МАСТ АЕРР ЕШРН ОЕРМ ИУПВ КЙТР ПНОИ

Рис. 5 Пример маршрутной перестановки

Задача 3. Расшифруйте цитаты, зашифрованные методами перестановки:

А) изречение немецкого философа Фридриха Ницше:
ОЬТСО НЙАЧУ ЛСВТЯ РЕВЕН ИЛЕТИ ДЕБОП

Б) изречение немецкого ученого – гуманиста Эразма Роттердамского:
ЙЫТЫР КСТНА ЛАТЕН ТЕАДЗ ОСИИЦ АТУПЕ РОООО

В) изречение чешского писателя Карела Чапека:
ЕЛЙГС АМОЛТ ЕМИЬР УНСЕО ЕАНОМ МЕООП МОЖОЕ ОЕКШО ШРАОЬ АЙОСЙ ДОДНР ОЕЕУО

Г) изречение польского писателя – фантаста Станислава Лема:
ТОУМА МЕЖЕЧ ЫАООО ОММГЗ ЕСНМЕ ДЕООО ЧЫАОД НЛОТМ УМООО ТДЕРО ЕОЧОМ МОООО

Дополнительное задание

Написать программу шифрования текста сообщения методами перестановки на любом языке программирования.

Отчет оформить в печатном и электронном видах. Продемонстрировать работу программы на произвольном сообщении

Контрольные вопросы:

1. Опишите простейшие примеры шифров перестановки
2. Опишите суть метода перестановки с ключом
3. Опишите суть метода шифрования перестановкой с пропусками (пробелами)
4. Опишите суть метода маршрутной перестановки
5. Возможен ли криптоанализ шифров перестановки, в чем его суть?

Лабораторная работа № 6. Методы криптоанализа классических шифров

Цель: познакомиться с основами криптоанализа шифров перестановки

Формируемые компетенции или их части

№ п/п	Содержание компетенции	Шифр
1.	Способен проводить сопровождение ИТ инфраструктуры	ПК-2

Теоретическая часть

Шифр столбцовой перестановки

При решении заданий на криптоанализ шифров перестановки необходимо восстановить начальный порядок следования букв текста. Для этого используется анализ совместимости символов, в чем может помочь таблица сочетаемости (таб. 1 – 2, см. Приложение).

При анализе сочетаемости букв друг с другом следует иметь в виду зависимость появления букв в открытом тексте от значительного числа предшествующих букв. Для анализа этих закономерностей используют понятие условной вероятности.

Систематически вопрос о зависимости букв алфавита в открытом тексте от предыдущих букв исследовался известным русским математиком А.А.Марковым (1856 - 1922). Он доказал, что появления букв в открытом тексте нельзя считать независимыми друг от друга. В связи с этим А. А. Марковым отмечена еще одна устойчивая закономерность открытых текстов, связанная с чередованием гласных и согласных букв. Им были подсчитаны частоты встречаемости биграмм вида гласная-гласная (*г,г*), гласная-согласная (*г,с*), согласная-гласная (*с,г*), согласная-согласная (*с,с*) в русском тексте длиной в 10^5 знаков. Результаты подсчета отражены в таб. 3 (см. Приложение)

Задание: расшифровать криптограмму, зная, что при шифровании использован метод столбцовой перестановки

СВПООЗЛУЙЬСТЬ_ЕДПСКОКАОЙЗ

Решение:

Текст содержит 25 символов, что позволяет записать его в квадратную матрицу 5х5. Известно, что шифрование производилось по столбцам, следовательно, расшифрование следует проводить, меняя порядок столбцов.

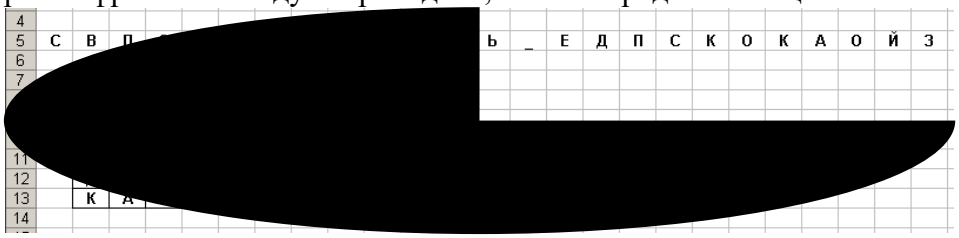


Рис. 1 Таблица перестановки

Необходимо произвести анализ совместимости символов (таблицы сочетаемости букв русского и английского алфавита, а также таблица частот биграмм представлены в Приложении). В первом и третьем столбце сочетание СП является крайне маловероятным для русского языка, следовательно, такая последовательность столбцов быть не может. Рассмотрим другие запрещенные и маловероятные сочетания букв: ВП (2,3 столбцы), ПС (3,1 столбцы), ПВ (3,2 столбцы). Перебрав их все, получаем наиболее вероятные сочетания биграмм по столбцам:

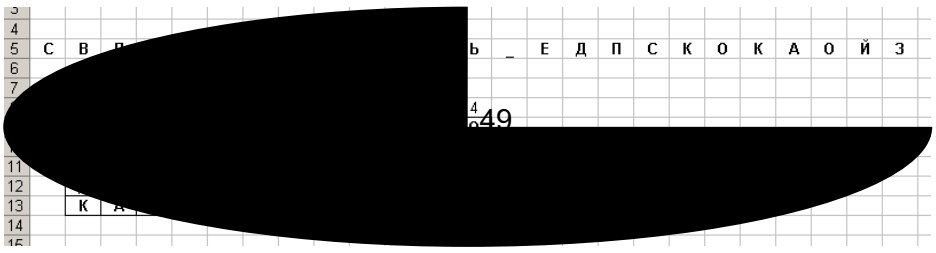


Рис. 2 Столбцы таблицы переставлены

Получаем осмысленный текст: **ВОСПОЛЬЗУЙТЕСЬ_ПОДСКАЗКОЙ**

Задание 1: Расшифровать фразу, зашифрованную столбцовой перестановкой

1. ОКЕСНВРП_ЫРЕАДЕЫН_В_РСИКО
2. ДСЛИЕЗТЕА_Д_ЛЬЮВМИ_ _АОЧХК
3. НМВИАИ_НЕВЕ_СМСТУОРДИАНКМ
4. ЕДСЗЬНДЕ_МУБД_УЭ_КРЗЕМНАЫ
5. СОНРЧОУО_ХДТ_ИЕИ_ВЗКАТРРИ
6. _ОНКА_БНЫЕЦВЛЕ_К_ТГОАНЕИР
7. НЗМАЕЕАА_Г_НОТВОССОТЬЯАЛС
8. РППОЕААДТВЛ_ЕБЬЛНЫЕ_ПА_ВР
9. ОПЗДЕП_ИХРДОТ_И_ВРИТЧ_САА
10. ВКЫОСИРЙУ_ОЬВНЕ_СОАПНИОТС
11. ПКТИРАОЛНАОИЧ_З_ЕСЬНЕЛНЖО
12. ИПКСОЕ_ТСМНАЧИ_ОЕН_ГДЕЛА_
13. АМВИННЬТЛЕАНЕ_ЙОВ_ОПХАРТО
14. АРЫКЗЫ_КЙТНЛ_ААЫ_ОЛБКЫТРТ
15. _ПАРИИВИАРЗ_БРА_ИСТЬЛТОЕК
16. П_ЛНАЭУВКАА_ЦИИВР_ОКИЕДРО
17. ЖВНОАН_АТЗОЬСН_ЫО_ФВИИКИЗ
18. ОТВГОСЕЬЬТАДВ_С_ЬЗАТТЕЫАЧ
19. ЯАМРИТ_ДЖЕХ_СВЕД_ТСУВЕТНО
20. УЬБДТ_ОЕГТВ_ОЫКЭА_ВКАИУЦИ
21. ЛТБЕЧЛЖЫЕ_ _ОАПТЖРДУ_ЛМНОА
22. ИТПРКРФАГО_АВЯИА_ЯНЖУАКАН
23. ПКЕЕРРПО_ЙУОТ_ИТПСУТЛЯЕИН
24. ИЬЖЗНСД_ТУН_ЕТАНУВЕ_РЫГОЗ
25. ЕОУРВА_НЬРИАДИЦЕПИ_РНШВЫЕ

Шифр двойной перестановки

Задание: расшифровать криптограмму, зная, что при шифровании использован метод двойной перестановки

ЫОЕЧТТОУ_СНСОРЧТРНАИДЬН_Е

Решение:

Текст содержит 25 символов, что позволяет записать его в квадратную матрицу 5х5. известно, что шифрование производилось сначала по столбцам, а затем по строкам, следовательно, расшифрование следует проводить тем же способом.

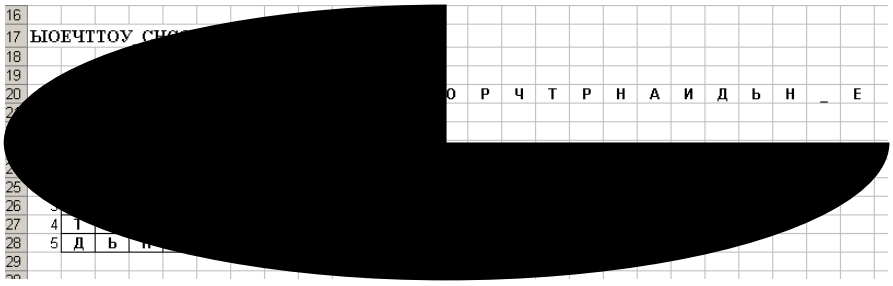


Рис. 3. Исходная таблица перестановки

Производим анализ совместимости символов. Если в примере столбцовой перестановки можно было легко подобрать нужную комбинацию путем перебора, то здесь лучше воспользоваться таблицей частот букв русского языка. Для оптимизации скорости выполнения задания можно проверить все комбинации букв только в первой строке. Получаем ОЕ-15, ОЧ-12, ЕТ-33, ТЕ-31, ЧО-х, ЕО-7, ЧЫ-х, ОЫ-х, ТЫ-11, ТЧ-1, ЧЕ-23 (где х-запрещенная комбинация).

Из полученных результатов можно предположить следующую комбинацию замены столбцов **2 4 3 5 1:**

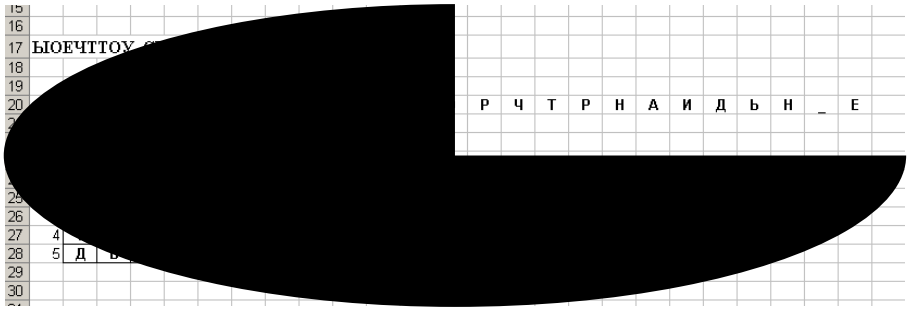


Рис. 4 Перестановка столбцов таблицы

Теперь необходимо переставить строки в нужном порядке. **3 2 4 5 1:**

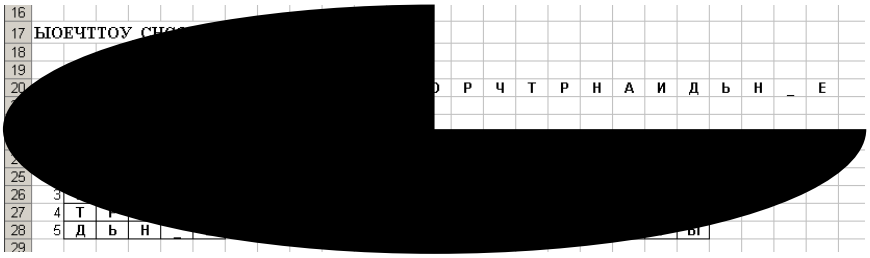


Рис. 5. Перестановка строк таблицы

Получаем осмысленный текст: **СРОЧНО_УСТРАНИТЬ_НЕДОЧЕТЫ**

Задание 2: Расшифровать фразу, зашифрованную

Двойной перестановкой (сначала были переставлены столбцы, затем строки)

12. СЯСЕ_ _ЛУНЫИАККННОГЯДУЧАТН
3. МСЕЫ_ЛЫВЕНТОСАНТУЕИ_РЛПОБ
4. АМНРИД_УЕБСЫ_ЕЙРСООКОТНВ_
5. ОПЧУЛС_БООНЕВ_ОЖАЕОНЕЩЕИН
6. ЕШИАНИРЛПГЕЧАВРВ_СЕЫНА_ЛО
7. АРАВНРСВЕЕОАВ_ЗАНЯА_КМРЕИ
8. А_ЛТАВЙООЛСО_ТВ_ШЕЕНЕСТ_Ь
9. ФИ_ЗИММУЫНУУКБ_Е_ДЬШЫИВЧУ
14. С_ОЯНВ_СЬСЛААВРЧЕАРТОГДЕС
15. ЗШАФИПРАЛОЕНЖ_ОЬН_ДАРВОНА
16. КЭЕ_ТДУМБ_ЬСЗЕДНЕЗМАОР_ТУ
17. _ЕАЛЯРАНВЯАЧДА_ЕРПЕСАНВ_Ч
18. _И_ЕНТРЗИ_ОКЕВНОДЛЕША_ИМП
19. РОБДОЕВПС_МСХЬА_ _ИВПСНИОТ
20. ЕСДНОГТЕАНН_НЕОВМР_ЕУНПТЕ
21. _ЙЕСТОВО_НИИНЛАЕТИЖДСОПВ_

10. ВР_ЕСДЕИ_ТПХРОИ_ЗБУАДНУА_

11. ЩТААЙПЕЕ_ТБГУРРСВЬЕ_ОРЗВВ

11. АВАРНСЧАА_НЕДВЕДЕРПЕОЙ_ИС

12. ДОПК_СОПАЛЕИНЛ_ГИНЙОИЖЕ_Т

13. ЛУАЗИЯНСА_ДТДЕАИ_ШРФЕОНП_

22. НДИАЕОЫЛПНЕ_ _НВЕАНГТ_ИЗЛА

23. П_БИРДЛЬНЕВ_ОП_ОПДЗЕВЫТЕА

24. МДООИТЕЬ_СМТ_НАДТЕСУБЕХНО

25. АИНАЛЖНОЛЕШФ_ЗИ_ЧАРОЬСНЕ_

Контрольные вопросы:

1. Что такое криптоанализ?
2. Опишите метод криптоанализа шифра столбцовой перестановки
3. Опишите метод криптоанализа шифра двойной перестановки
4. Какие дополнительные сведения желательно использовать при криптоанализе?

Лабораторная работа № 7. Криптосистемы с открытым ключом. Методы ЭЦП

Цель: изучить математические методы, положенные в основу СОК, на примере криптосистемы RSA; познакомиться с алгоритмом цифровой подписи

Формируемые компетенции или их части

№ п/п	Содержание компетенции	Шифр
1.	Способен проводить сопровождение ИТ инфраструктуры	ПК-2

Теоретическая часть

Шифрование с открытым ключом (СОК)

В современных информационных системах стало популярным **шифрование с открытым ключом,** которое осуществляется на основе математических знаний, например, таких разделов, как разложения чисел на простые множители, вычисление логарифмов чисел, решение алгебраических уравнений.

На основании **теоремы Рабина** доказано, что разложение на простые множители двух больших чисел эквивалентно раскрытию ключа для **шифра RSA** и практически невозможно в реальном времени с учетом возможностей современных ЭВМ.

Криптосистема RSA разработана **в 1977 году** и получила название в честь ее создателей: Рона Ривеста, Ади Шамира и Леонарда Эйдельмана.

Шифры с открытым ключом достаточно просты в обращении, практичны и обладают высокой криптостойкостью. И хотя сравнительно просто найти пару больших взаимно простых чисел, к настоящему времени не разработаны эффективные алгоритмы разложения чисел на простые множители. Так, разложение на множители числа в 200 и более цифр займет сотни лет работы компьютера. А так как при употреблении шифра с открытым ключом используются очень большие простые числа, содержащие сотни цифр в десятичной системе счисления, то вскрыть такие шифры весьма сложно.

Поэтому поиск простых чисел и их общей формулы в настоящее время представляет не только теоретический, но и практический интерес.

Получив сообщение, получатель сначала расшифровывает его закрытым ключом, а затем проверяет его подлинность. Для этого он сравнивает дешифрованный текст с тем, который был получен с помощью открытого ключа.

Алгоритмы кодирования и декодирования на самом деле весьма сложны. Основные идеи специальных кодов изложены в соответствующей литературе и защищены от злоумышленников на различных уровнях, включая юридическую защиту.

Рассмотрим один из таких алгоритмов – алгоритм RSA для некоторого пользователя A_i.

1. Пользователь выбирает пару различных простых чисел p_i и g_i.
2. Находит произведение $r_i = p_i * g_i$ и функцию Эйлера $\varphi(r_i)$ — число взаимно-простых с r_i натуральных чисел, меньших r_i, включая 0 и 1: $\varphi(r_i) = (p-1)(g-1)$
3. Находит **открытый ключ c_i** — взаимно-простое с $\varphi(r_i)$ и меньшее его.
4. Находит **закрытый ключ d_i** — произвольное решение сравнения $d_i * c_i \equiv 1 (mod(\varphi(r_i)))$ и меньшее $\varphi(r_i)$.
5. **Публикует открытый ключ — пару $\{c_i, r_i\}$,** которые доступны для любого пользователя.
6. Для отправления сообщения w абоненту A_i его нужно **зашифровать открытым ключом $\{c_i, r_i\}$: $w' = w^c \ (mod\ r_i) < r_i$.**

7. Получив сообщение, A_i дешифрует его своим секретным ключом $\{d_i, r_i\}$:
$w'' = (w')^d \pmod{r_i}$.

Очевидно, что для полностью правильной дешифровки $(w = w'')$ нужно, чтобы и исходное сообщение было меньше r_i. Для этого нужно *предварительно* зашифровать сообщение в форму, мощность алфавита которой меньше r_i или разбить сообщение на несколько.

С точки зрения практической реализации такой шифр обладает высокой криптостойкостью, так как в его основе лежит выбор простых чисел. В настоящее время, как известно, не найдена математическая формула или алгоритм установления простого числа. Генерация простых чисел достаточно трудоемкая задача. Еще большую трудность вызывает определение ключей, также являющихся простыми числами.

Алгоритм RSA используется в банковских компьютерных сетях, особенно для работы с удаленными клиентами (обслуживание кредитных карточек).

В настоящее время алгоритм **RSA** используется во многих стандартах, среди которых SSL, S-HHTP, S-MIME, S/WAN, STT и PCT.

Задача. С помощью алгоритма RSA выполнить шифрование и дешифрование сообщения «ВАЗА».

Решение:

Выберем для простоты небольшие простые числа (в отличие от тех больших, которые выбирают при реальном кодировании).

Пусть $p_i = 2$, $g_i = 11$.
Тогда $r_i = 2 * 11 = 22$, $\varphi(r_i) = (2-1)(11-1) = 10$.

Выберем в качестве c_i число, взаимно-простое с 10 (т.е. **НОД** $(c_i, 10) = 1$), например $c_i = 3$.

Выберем d_i из сравнения $(3 * d_i) \equiv 1 \pmod{10}$. Таким (минимальным) числом является $d_i = 7$, т . к . $(3 * 7) \equiv 1 \pmod{10}$, $21 \equiv 1 \pmod{10}$.
Получили **открытый ключ** $\{c_i, r_i\} = \{3, 22\}$, **закрытый ключ** $\{d_i, r_i\} = \{7, 22\}$,
При решении задачи используем алфавит:

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

Заменим буквы алфавита цифрами, соответствующими их порядковому номеру в алфавите, исключив буквы Ё и Ъ:

А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21

Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я
22	23	24	25	26	27	28	29	30	31

Получим сообщение:

В	А	З	А
3	1	8	1

Зашифруем сообщение с помощью открытого ключа {3, 22} для того, чтобы послать его абоненту А.

Используем преобразование: $w' = w^c \pmod{r_i}$, $w'_1 = (3^3) \pmod{22} = 27 \pmod{22} = 5$,

$w'_2 = (l^3) \pmod{22} = 1$,

$w'_3 = (8^3) \pmod{22} = 512 \pmod{22} = 6$.

$w'_4 = (l^3) \pmod{22} = 1$.

Получили сообщение $w' = (5, 1, 6, 1)$.

Абонент *А* расшифрует это сообщение (5, 1, 6, 1) с помощью закрытого ключа {7, 22}:

Используем преобразование: $w'' = (w')^d \pmod{r_i}$. $w''_1 = (5^7) \pmod{22} = 78125 \pmod{22} = 3$,

$w''_2 = (1^7) \pmod{22} = 1$,

$w''_3 = (6^7) \pmod{22} = 279936 \pmod{22} = 8$,

$w''_4 = (1^7) \pmod{22} = 1$,

Проверим результат из условия: $w = w''$

(3, 1, 8, 1) → ВАЗА

Выполнить практические задания:

Задача 1. Используя открытый ключ {3,22} и закрытый ключ {7,22} зашифровать и расшифровать слово МОСКВА

Задача 2 (выполнить по вариантам). Зашифровать и расшифровать сообщения:

№ варианта	Исходные данные (простые числа p и g)	Сообщение	
1	p = 3, g = 11	А) ПАРОЛЬ Б) ТАЙНИК	В) Сообщение зашифровывается открытым ключом
2	p = 3, g = 17	А) БИАНКИ Б) МАСТЕР	В) Сообщение расшифровывается закрытым ключом
3	p = 5, g = 17	А) ТЕОРИЯ Б) СЫЩИК	В) Криптография изучает методы шифрования
4	p = 3, g = 23	А) ПИРАТ Б) ЛОЦМАН	В) Пароли должны периодически меняться
5	p = 2, g = 19	А) ВОПРОС Б) КАРЛИК	В) Криптоанализ шифра очень сложен

Задача 3

Примечание: для выполнения задания студентам необходимо разбиться на пары. У каждого в паре должны быть собственные ключи.

Каждому в паре самостоятельно:

1. Выбрать простые числа **p** и **g,**
2. Вычислить ключи,

3. Обменяться открытыми ключами с соседом,
4. С помощью открытого ключа соседа зашифровать слово (сообщение), передать соседу,
5. Расшифровать полученное сообщение с помощью своего закрытого ключа.
6. Проверить результат.

Цифровая (электронная) подпись

Для организации многосторонней секретной связи используется шифр с открытым ключом. Кодирование сообщения A заключается в преобразовании $F: A \rightarrow A^d (mod p)$, где пара (d, p) называется **ключом.** Получатель сигнала декодирует его таким же преобразованием с помощью ключа (l, p). Очевидно, что получатель принципиально сможет получить исходное A только если $A < p$, поэтому если надо закодировать много информации (большое слово), его надо разбить на кортежи длиной, меньшей p.

Очевидно, операции кодирования и декодирования информации, по сути, тождественны и отличаются друг от друга лишь показателями степени, поэтому для них выполняется **переместительный закон**:

$$A \rightarrow (A^l)^d (mod\ p) = A^{ld} (mod\ p) = A^{dl} (mod\ p) = (A^d)^l (mod\ p) \leftarrow A.$$

В практике кодирования используются различные приемы, объединенные названием ***цифровая* или *электронная подпись.***

Отправитель кодирует сообщение A закрытым ключом $C = A^d (mod\ p)$ и посылает получателю информацию, т. е. пару (d, p) в виде подписанного сообщения. Получатель, получив это сообщение, **декодирует подпись сообщения открытым ключом (l, p), т.е. находит $A' = C' (mod\ p)$.**

Если $A = A'$, то письмо дошло правильно и без помех или оно было отправлено в нешифрованном виде. Если $A \neq A'$, то сообщение при передаче было искажено, т. е. произошла потеря информации.

В теории вычетов доказывается, что при отсутствии помех и выполнения некоторых условий (взаимной простоты чисел d, l, p) результат $A = A'$ достигается всегда.

Задача 4.

Примечание: для выполнения задания студентам необходимо разбиться на пары. У каждого в паре должны быть собственные ключи.

Каждому в паре самостоятельно:

1. Выбрать простые числа **p** и **g,**
2. Вычислить ключи,
3. Обменяться открытыми ключами с соседом,
4. С помощью своего закрытого ключа зашифровать слово (сообщение), передать соседу,
5. Расшифровать полученное сообщение с помощью открытого ключа соседа.
6. Проверить результат.

Дополнительное задание

Написать программу шифрования текста сообщения рассмотренными методами на любом языке программирования.

Отчет оформить в печатном и электронном видах. Продемонстрировать работу программы на произвольном сообщении

Контрольные вопросы:

1. Укажите, на какие виды делятся существующие криптосистемы?
2. Охарактеризуйте криптосистемы с открытым ключом
3. Поясните, на каких математических принципах основана криптосистема RSA
4. Расскажите, когда и кем была разработана система RSA, где она используется?
5. Приведите алгоритм вычисления ключей в системе RSA
6. Приведите алгоритм шифрования сообщения в системе RSA
7. Приведите алгоритм дешифрования сообщения в системе RSA
8. Охарактеризуйте принципы ЭЦП
9. Поясните, чем различаются алгоритмы RSA и ЭЦП

Лабораторная работа № 8. Методы сжатия. Алгоритм Шеннона - Фано

Цель: ознакомиться с общими принципами сжатия информации с использованием метода Шеннона - Фано

Формируемые компетенции или их части

№ п/п	Содержание компетенции	Шифр
1.	Способен проводить сопровождение ИТ инфраструктуры	ПК-2

Теоретическая часть

Эффективное кодирование информации. Общие положения

Напомним, что кодирование – это представление сообщений в форме, удобной для передачи по данному каналу, а декодирование – восстановление информации по принятому сигналу. Одним из важнейших вопросов кодирования является повышение его эффективности, т.е. путем устранения избыточности снижение среднего числа символов, требующихся на букву сообщения. Такое кодирование получило название **эффективное кодирование.** Из сказанного выше следует, что **эффективное кодирование решает задачу максимального сжатия информации.**

Эффективное кодирование базируется на **основной теореме Шеннона для канала без помех**, суть которой сводится к следующему:

сообщения, составленные из букв некоторого алфавита, можно закодировать так, что среднее число двоичных символов на букву сколь угодно близко к энтропии источника этих сообщений, но не меньше этой величины.

Наличие в сообщениях избыточности позволяет рассматривать вопрос о сжатии данных, т.е. о передаче того же количества информации с помощью последовательностей символов меньшей длины – методы сжатия без потерь (обратимые). Для этого используют специальные алгоритмы сжатия, уменьшающие избыточность.

Эффект сжатия оценивают коэффициентом сжатия:

$$K=n/q$$

Где **n** – число минимально необходимых символов для передачи сообщения;
q – число символов в сообщении.

Так, при эффективном двоичном кодировании **n** равно энтропии источника информации.

Наряду с методами сжатия не уменьшающими количество информации в сообщении применяют методы сжатия основанные на потере малосущественной информации, - методы сжатия с потерями (необратимые). Следует отметить, что применение методов сжатия с потерями не приемлемо для некоторых видов информации, например, текстовой или числовой.

Обратимое сжатие всегда приводит к снижению объема выходного потока информативности. Из выходного потока при помощи восстанавливающего алгоритма можно получить исходный поток.

Основные методы обратимого сжатия:	**Основные методы необратимого сжатия:**
Шеннона – Фано; Хаффмена; LZW (Lanper – Ziv – Welch); арифметическое сжатие.	MPEG (Moving Pictues Experts Group); JPEG (Joint Photographic Expert Group); фрактальное сжатие.

Наибольшее распространение среди методов сжатия информации без потерь нашли **статистические алгоритмы сжатия,** учитывающие вероятность появления отдельных

символов в информационном потоке. В первую очередь это алгоритмы Шеннона – Фано и Хаффмена.

Алгоритм Шеннона – Фано. Эффективное кодирование базируется на основной теореме Шеннона для канала без помех.

- ✓ Буквы алфавита сообщений вписываются в таблицу в порядке убывания вероятностей;
- ✓ Буквы алфавита разделяются на две группы так, чтобы суммы вероятностей в каждой группе были по возможности одинаковы (максимально близки); в группе может быть любое число символов, в том числе – один;
- ✓ Всем буквам верхней половины в качестве первого символа приписывается единица (1), а всем нижним – нули;
- ✓ Каждая из полученных групп в свою очередь разбивается на две подгруппы с одинаковыми суммарными вероятностями и т.д. процесс повторяется до тех пор, пока в каждой подгруппе останется по одной букве.

Выполнить практическое задание:

Задача 1. Построить код по алгоритму Шеннона – Фано для списка сообщений с заданным распределением вероятностей. Определить среднее число двоичных символов, приходящихся на одну букву

	S	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
1	0,08	0,1	0,15	0,15	0,3	0,05	0,12	0,05
2	0,15	0,1	0,15	0,15	0,1	0,1	0,15	0,1
3	0,15	0,02	0,25	0,15	0,08	0,15	0,2	-
4	0,02	0,25	0,04	0,01	0,4	0,1	0,03	0,15
5	0,15	0,2	0,08	0,12	0,15	0,1	0,1	-
6	0,07	0,04	0,3	0,1	0,07	0,12	0,3	-

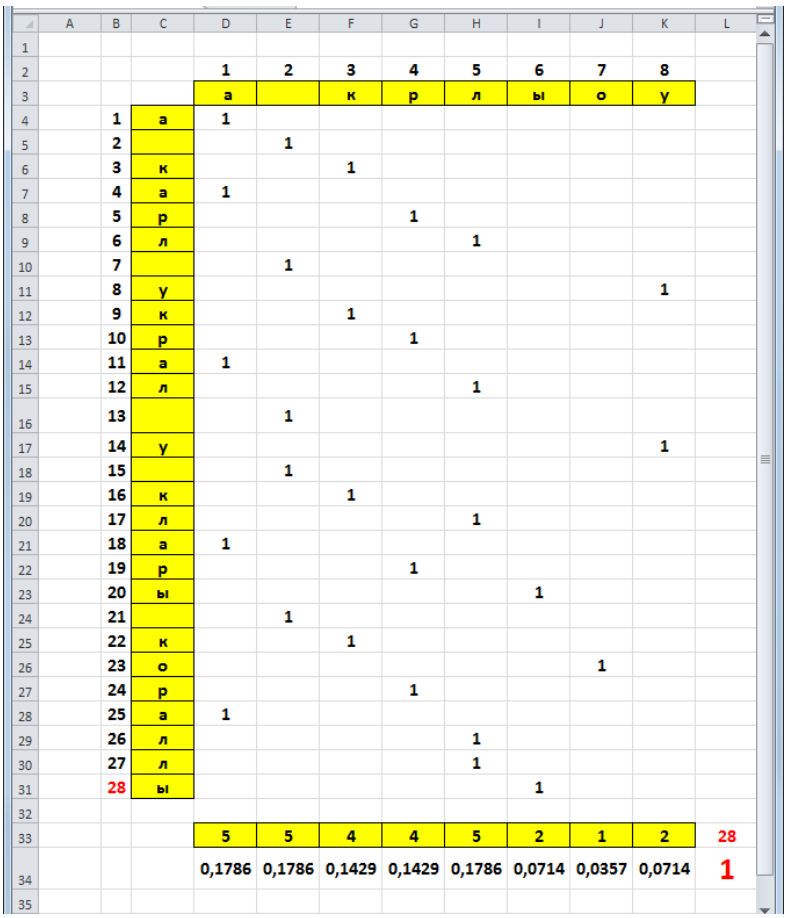
Рассмотрим пример использования алгоритма Шеннона – Фано для кодирования произвольного текстового сообщения (рис. 1, 2)

Построить код по алгоритму Шеннона – Фано для сообщения А КАРЛ УКРАЛ У КЛАРЫ КОРАЛЛЫ

Определить среднее число двоичных символов, приходящихся на одну букву.

Решение:

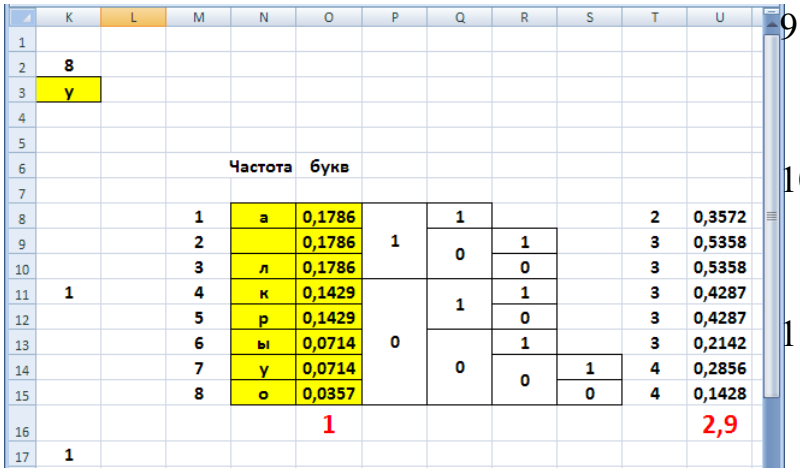
1. Вычислить общее количество символов в сообщении (диапазон B4:C31)
2. Выбрать символы без повторений (диапазон D2:K3)
3. Вычислить, сколько раз каждая буква и пробел используется в сообщении (диапазон D4:K31)



			1	2	3	4	5	6	7	8	
			а		к	р	л	ы	о	у	
1	а		1								
2				1							
3	к				1						
4	а		1								
5	р					1					
6	л						1				
7				1							
8	у									1	
9	к				1						
10	р					1					
11	а		1								
12	л						1				
13				1							
14	у									1	
15				1							
16	к				1						
17	л						1				
18	а		1								
19	р					1					
20	ы							1			
21				1							
22	к				1						
23	о								1		
24	р					1					
25	а		1								
26	л						1				
27	л						1				
28	ы							1			
			5	5	4	4	5	2	1	2	28
			0,1786	0,1786	0,1429	0,1429	0,1786	0,0714	0,0357	0,0714	1

Рис. 1. Вычисление количества букв и вероятностей

4. **Вычисления в диапазоне D33:K33** – в ячейке D33 использовать формулу =СУММ(D4:D32), скопировать формулу на диапазон;
5. **Вычисления в диапазоне D34:K34** – в ячейке D34 использовать формулу =D33/28, скопировать формулу на диапазон;
6. **Вычисления в диапазоне D34:K34** – в ячейке D34 использовать формулу =D33/28, скопировать формулу на диапазон;
7. **Вычисления в ячейке L33** - использовать формулу =СУММ(D33:K33);
8. **Вычисления в ячейке L34** - использовать формулу =СУММ(D34:K34);



	8										
	у										
				Частота	букв						
		1	а	0,1786		1			2	0,3572	
		2		0,1786	1		1		3	0,5358	
		3	л	0,1786		0	0		3	0,5358	
1		4	к	0,1429			1		3	0,4287	
		5	р	0,1429		1	0		3	0,4287	
		6	ы	0,0714	0		1		3	0,2142	
		7	у	0,0714		0		1	4	0,2856	
		8	о	0,0357			0	0	4	0,1428	
				1						2,9	
	1										

Рис. 2. Алгоритм Шеннона – Фано

9. **Вычисления в ячейке O16** - использовать формулу =СУММ(O8:O15);
10. **Вычисления в ячейке U16** - использовать формулу =СУММ(U8:U15).
11. **Самостоятельно записать итоговые коды.**

Выполнить практическое задание:

Задача 2. Построить код по алгоритму Шеннона – Фано для сообщения
ВОТ ВИДИТЕ, ЧТО НИЧЕГО НЕ ВИДИТЕ, А ПОЧЕМУ - СКОРО УВИДИТЕ

Определить среднее число двоичных символов, приходящихся на одну букву.

Задача 3. Построить код по алгоритму Шеннона – Фано для произвольного сообщения (не менее 25-30 символов). Определить среднее число двоичных символов, приходящихся на одну букву.

Контрольные вопросы:

1. Охарактеризуйте понятие «эффективное кодирование»
2. Поясните суть основной теоремы Шеннона для канала без помех
3. Поясните, каким образом вычисляется коэффициент сжатия
4. Перечислите основные методы обратимого сжатия
5. Перечислите основные методы необратимого сжатия
6. Опишите порядок кодирования сообщений с помощью алгоритма Шеннона – Фано
7. Перечислите основные информационные характеристики источника сообщения
8. Поясните понятие энтропия источника
9. Поясните, каким образом вычисляется среднее число символов на букву в коде по алгоритму Шеннона - Фано
10. Поясните алгоритм построения кода для произвольного сообщения по алгоритму Шеннона - Фано
11. Поясните, как вычислить вероятность появления каждой буквы в произвольном сообщении