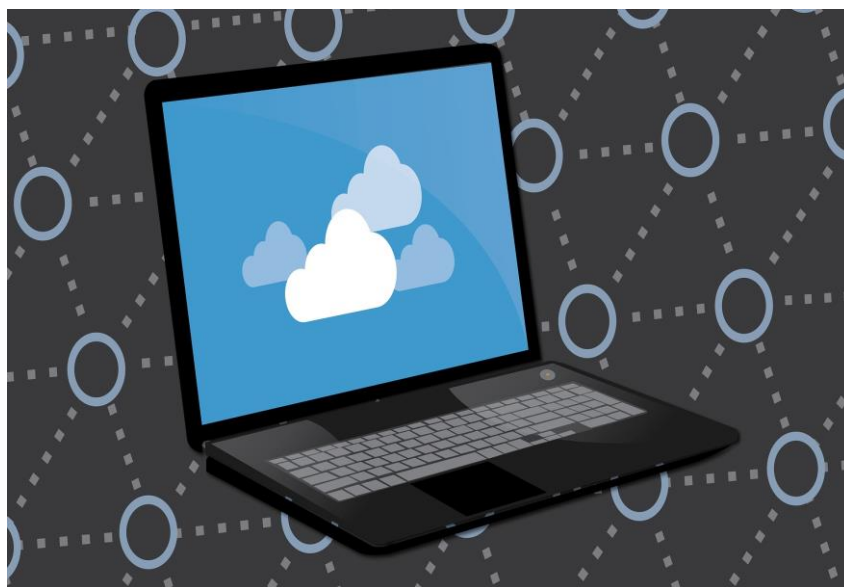


И.В. Ананченко, Т.В. Зудилова, С.Э. Хоружников

**СРЕДСТВА РЕЗЕРВНОГО КОПИРОВАНИЯ,  
ВОССТАНОВЛЕНИЯ, ЗАЩИТЫ ДАННЫХ  
В ОПЕРАЦИОННЫХ СИСТЕМАХ WINDOWS**



Санкт-Петербург  
2019

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ  
РОССИЙСКОЙ ФЕДЕРАЦИИ  
УНИВЕРСИТЕТ ИТМО

И.В. Ананченко, Т.В. Зудилова, С.Э. Хоружников

# **СРЕДСТВА РЕЗЕРВНОГО КОПИРОВАНИЯ, ВОССТАНОВЛЕНИЯ, ЗАЩИТЫ ДАННЫХ В ОПЕРАЦИОННЫХ СИСТЕМАХ WINDOWS**

Учебное пособие

РЕКОМЕНДОВАНО К ИСПОЛЬЗОВАНИЮ В УНИВЕРСИТЕТЕ ИТМО

по направлению подготовки 11.03.02 Инфокоммуникационные  
технологии и системы связи

в качестве учебно-методического пособия для реализации образовательных  
программ высшего образования бакалавриата

 УНИВЕРСИТЕТ ИТМО

Санкт-Петербург  
2019

Ананченко И.В., Зудилова Т.В., Хоружников С.Э. Средства резервного копирования, восстановления, защиты данных в операционных системах Windows – СПб: Университет ИТМО, 2019. – 50 с.

Рецензенты:

Певнева Анна Геннадьевна, кандидат технических наук, доцент, научный сотрудник факультета безопасности информационных технологий, Университета ИТМО.

В пособии рассматриваются теоретические и практические аспекты работы со средствами резервного копирования, восстановления, защиты данных в операционных системах Windows.



**Университет ИТМО** – ведущий вуз России в области информационных и фотонных технологий, один из немногих российских вузов, получивших в 2009 году статус национального исследовательского университета. С 2013 года Университет ИТМО – участник программы повышения конкурентоспособности российских университетов среди ведущих мировых научно-образовательных центров, известной как проект «5 в 100». Цель Университета ИТМО – становление исследовательского университета мирового уровня, предпринимательского по типу, ориентированного на интернационализацию всех направлений деятельности.

© Университет ИТМО, 2019

© Ананченко И.В., Зудилова Т.В., Хоружников С.Э., 2019

## Содержание

Введение.....	4
<b>1 СОВРЕМЕННЫЙ ПОДХОД К РЕЗЕРВНОМУ КОПИРОВАНИЮ, ВОССТАНОВЛЕНИЮ И ЗАЩИТЕ ДАННЫХ В КОМПЬЮТЕРНЫХ СИСТЕМАХ.....</b>	<b>6</b>
1.1 Проблема защиты и восстановление данных .....	6
1.2 Контрольные вопросы по изучаемой теме.....	9
<b>2 СОЗДАНИЕ РЕЗЕРВНЫХ КОПИЙ В ОПЕРАЦИОННОЙ СИСТЕМЕ WINDOWS 10.....</b>	<b>10</b>
2.1 Выполнение практической работы по теме "Создание резервной копии средствами ОС Windows 10" .....	13
2.2 Ход выполнения работы .....	13
2.3 Контрольные вопросы по изучаемой теме.....	22
<b>3 РЕЗЕРВНОЕ КОПИРОВАНИЕ ФАЙЛОВ И ПАПЕК WINDOWS SERVER В ОБЛАЧНОЕ ХРАНИЛИЩЕ MICROSOFT AZURE.....</b>	<b>23</b>
3.1 Выполнение практической работы по теме "Резервное копирование файлов и папок с помощью службы архивации Azure с использованием модели развертывания Resource Manager" .....	25
3.2 Ход выполнения работы .....	25
3.3 Контрольные вопросы по изучаемой теме.....	32
<b>4 УТИЛИТА ROBOCOPY. АВТОМАТИЗАЦИЯ РЕЗЕРВНОГО КОПИРОВАНИЯ ФАЙЛОВ ПО СЕТИ И С ДИСКА НА ДИСК.....</b>	<b>33</b>
4.1 Выполнение практической работы по теме "Создание резервной копии средствами утилиты копирования Robocopy" .....	33
4.2 Ход выполнения работы .....	34
4.3 Контрольные вопросы по изучаемой теме.....	41
<b>5 МИГРАЦИЯ ФИЗИЧЕСКОГО КОМПЬЮТЕРА В ВИРТУАЛЬНУЮ СРЕДУ С ПОМОЩЬЮ DISK2VHD.....</b>	<b>42</b>
5.1 Виртуализация компьютера с помощью Disk2VHD.....	42
5.2 Выполнение практической работы по теме "Создание виртуализированной копии физического компьютера в виртуальной среде с помощью Disk2VHD" .....	43
5.3 Ход выполнения работы .....	44
5.4 Контрольные вопросы по изучаемой теме.....	45
<b>Заключение .....</b>	<b>45</b>
<b>Литература .....</b>	<b>48</b>

## ВВЕДЕНИЕ

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

Пособие состоит из пяти разделов:

**Современный подход к резервному копированию, восстановлению и защите данных в компьютерных системах** – рассматриваются общие подходы к созданию резервных копий, отмечены наиболее часто встречающиеся причины, приводящие к тому, что созданию резервных копий уделяется недостаточное внимание.

**Создание резервных копий в операционной системе Windows 10** – рассматривается создание архивов файлов, создание образа операционной системы и диска восстановления системы. Даются практические рекомендации, как можно выполнить резервное копирование и восстановление данных средствами ОС Windows 10.

**Резервное копирование файлов и папок Windows Server в облачное хранилище Microsoft Azure** – обсуждаются основные преимущества использования средств облачного резервного копирования (Azure Backup), даны практические рекомендации по реализации резервного копирования файлов и папок с помощью службы архивации Azure с использованием модели развертывания Resource Manager.

**Утилита Robocopy. Автоматизация резервного копирования файлов по сети и с диска на диск** – подробно рассматривается работа с утилитой Robocopy, используемой для автоматизации копирования и восстановления данных.

**Миграция физического компьютера в виртуальную среду с помощью DISK2VHD** – рассматривается использование программного средства DISK2VHD для виртуализации физических компьютеров. Создание полноценной работоспособной виртуальной копии физического компьютера позволяет, например, размещать виртуальные машины в облаке, решая вопросы, связанные с повышением отказоустойчивости, а также находить оптимальные решения, связанные с выводом из эксплуатации устаревающей компьютерной техники.

Обучающиеся выполняют работы в компьютерном классе под руководством преподавателя. Если данное пособие используется, как

дополнительное, то обучающийся может выполнять задания работ в рамках самоподготовки самостоятельно, используя свой компьютер.

Перед тем, как обучающиеся приступят к выполнению работы, преподаватель проводит небольшой инструктаж о том, как выполнять работу и на какие моменты следует обратить особое внимание. Преподаватель может сообщить обучающимся о тех изменениях в ходе выполнения работы, которые должны быть выполнены обучающимися с учетом аппаратной конфигурации оборудования в учебном классе, установленной операционной системы и прикладных пользовательских программ, которые могут повлиять на результаты выполнения работы. Преподаватель может перед началом работы опросить студентов о том, что, как и в какой последовательности необходимо выполнить. Если группа обучающихся большая, то допускается совместное выполнение одной работы, но не более чем двумя обучающимися на одном компьютере.

По итогам выполнения работы обучающиеся подготавливают и защищают отчет. Обычно отчет выполняется в виде электронного документа и предоставляется преподавателю на проверку в виде файла формата rtf, doc, docx или pdf. С разрешения преподавателя отчет о проделанной работе может быть оформлен на бумажных листах формата А4, которые должны быть скреплены перед сдачей отчета преподавателю. Первый лист отчета титульный – содержит информацию об учебном заведении, факультете, названии дисциплины, теме выполненной работы. Приводится информация об обучающемся, выполнившим работу. Приводится информация о преподавателе, проверяющем работу. В нижней части листа информация о месте (городе), где находится учебное заведение и год выполнения работы. В содержательной части отчета о проделанной работе необходимо указать номер и тему работы. Затем следует описать ход выполнения работы. Желательно проиллюстрировать ход выполнения работы скриншотами (копиями экрана), полученными в процессе выполнения работы.

Если преподавателем были заданы вопросы по выполнению работы, на которые предложено ответить письменно, то приводятся вопросы и ответы на них. Завершается отчет выводами по проделанной работе. Отмечаются достоинства и недостатки изученной технологии, область использования разработки и т.д.

Желательно привести в отчете список использованной литературы и интернет ресурсов (сайтов сети Интернет).

Учебное пособие предназначено для студентов, изучающих дисциплину “Администрирование сетей Windows”, которые могут использовать материалы пособия в процессе выполнения лабораторных и практических работ.

# **1 СОВРЕМЕННЫЙ ПОДХОД К РЕЗЕРВНОМУ КОПИРОВАНИЮ, ВОССТАНОВЛЕНИЮ И ЗАЩИТЕ ДАННЫХ В КОМПЬЮТЕРНЫХ СИСТЕМАХ**

## **1.1 Проблема защиты и восстановления данных**

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

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

Актуальны вопросы защиты данных и для пользователей домашних компьютеров, которые в настоящее время практически все используют ресурсы сети Интернет (в виде постоянного или периодического подключения). В большинстве своем пользователи достаточно хорошо представляют себе угрозы, связанные с тем, что кто-то чужой получит доступ к компьютеру (человек-злоумышленник, атакующий выбранный им сетевой хост, или вирус, не нацеленный именно на этот конкретный компьютер, но заражающий исполняемые файлы, выполняемые под управлением той или иной операционной системы).

Как правило, на каждом компьютере установлена антивирусная программа, например, это может быть бесплатное решение Microsoft Security Essentials (для Windows 7) или Защитник Windows (Windows 8, Windows RT, Windows 8.1, Windows RT 8.1, Windows 10). Пользователь может использовать более сложную

систему защиты, включающую в себя не только антивирусный функционал, но и средства, обеспечивающие безопасное подключение к компьютерным сетям, анализ входящего и исходящего трафика и т.д. В качестве примера отметим Kaspersky Internet Security для всех устройств [1] – надежное и удобное решение для защиты, совместимое с операционными системами (ОС) Windows, Mac и Android. Используемая проактивная облачная защита в составе данного решения надежно защищает от вирусов, троянских и других вредоносных программ, от взаимодействия с опасными веб-сайтами, а также блокирует навязчивую баннерную рекламу и спам. Для малого бизнеса может использоваться программа Kaspersky Small Office Security. Программы Kaspersky Security и Dr.Web Enterprise Security Suite [2] хорошо подходят для решений среднего и крупного бизнеса.

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

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

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

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

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



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

2. Отсутствие свободного места на носителях данных для создания резервных копий. Данный фактор объясняет, почему пользователи игнорируют действия по созданию резервных копий, которые необходимо регулярно создавать. Очевидно, что для сохранения архивов необходимо свободное место, и если его нет, то или надо покупать накопители или арендовать ресурсы для хранения данных (многие облачные провайдеры за относительно невысокую плату предоставляют услуги архивирования информации в облако с поддержкой средств программной автоматизации).
3. Необходимость выделять время и ресурсы на создание резервных копий. Для проведения операции резервного копирования необходимо время – может потребоваться несколько часов. Во время создания резервных копий на обеспечение процедуры затрачивается процессорное время, производительность системы, на которой запущен процесс архивирования, снижается. Несмотря на возможности теневого копирования, пользователи предпочитают не создавать архивные копии в то время, когда работают с данными. Отметим, что нежелательно создавать новые папки, удалять существующие или перемещать их на новое место, если данные операции затрагивают носители, для которых создаются резервные копии.
4. Соблюдение графика создания архивных копий. Если начало операции резервного копирования должно инициироваться вручную или если требуется трудоемкая настройка работы программного обеспечения для создания архивных копий по расписанию, то все это не способствует своевременному созданию архивов.

Отсутствие архивов с актуальной информацией не позволяет относительно быстро и без потерь восстановить данные в случае их утраты по основному месту размещения. Утрата данных возможна не только в том случае, когда вообще не создаются резервные копии, но и тогда, когда процесс

архивирования организован неправильно. Например, копируется не вся необходимая информация, архивные копии хранятся на ненадежных носителях, что не позволяет выполнить восстановление информации в полном объеме, архивные копии хранятся в том же самом месте, где и основные носители, что приводит к полной утрате информации в случае чрезвычайных ситуациях (пожары, наводнения и пр.).

## **1.2 Контрольные вопросы по изучаемой теме**

1. Какие две большие группы вопросов рассматриваются для обеспечения безопасности данных?
2. Почему обеспечение безопасности данных не сводится только к вопросам предотвращения несанкционированного доступа к данным со стороны злоумышленников?
3. Перечислите основные причины, почему пользователи не любят создавать архивные копии.
4. В каких случаях архивные копии создавать не требуется? Приведите примеры.
5. Приведите примеры антивирусных программ, которые могут использоваться для защиты персонального компьютера от вредоносного программного обеспечения.

## 2 СОЗДАНИЕ РЕЗЕРВНЫХ КОПИЙ В ОПЕРАЦИОННОЙ СИСТЕМЕ WINDOWS 10

Рассмотрим типовые примеры создания резервных копий данных, хранящихся и обрабатываемых под управлением ОС Windows 10.

Самый простой способ создать копию документа с важной информацией – просто скопировать файл на другой носитель. Например, на внешний жесткий диск. Заметим, что для уменьшения размера копируемой информации файлы можно предварительно сжать, создав архив с помощью какого-либо популярного архиватора, или воспользоваться встроенной возможностью самой операционной системы. Для этого выбираем файл, группу файлов или папку (см. Рисунок 1), “кликаем” правой клавишей мыши, в открывшемся меню выбираем пункт “Отправить” и в нем подпункт “Сжатая ZIP-папка”.

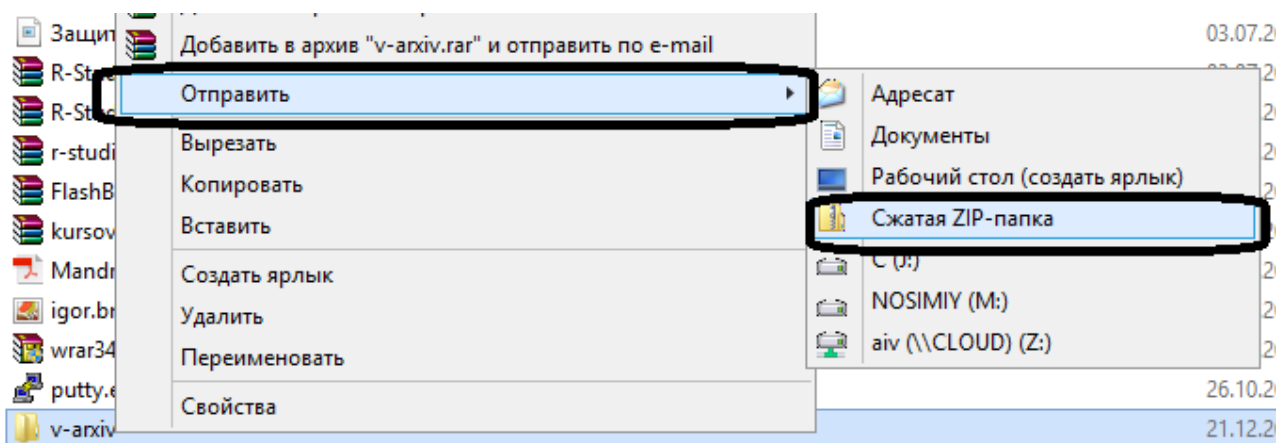


Рисунок 1 – Интерфейс формирования сжатой ZIP-папки

Альтернативное решение использованию архиватора, создающего архивы сжатых файлов – использование функционала самой ОС Windows, позволяющего сэкономить дисковое пространство после определения носителя или отдельного каталога на таком носителе, как сжатого. Если выбираем для сжатия папку, размещенную на носителе с файловой системой NTFS, то в свойствах папки нажимаем кнопку “Другие” (см. Рисунок 2), в окне “Дополнительные атрибуты” устанавливаем флажок в чекбоксе “Сжимать содержимое для экономии места на диске”.

Рассмотренным способом можно создавать резервные копии файлов, содержащих документы, фотографии, презентации, и другие данные, созданные прикладными программами пользователя. Решение не подойдет в случае, когда необходимо создавать архивные копии исполняемых и системных файлов, позволяющие восстанавливать ОС в случае сбоя.

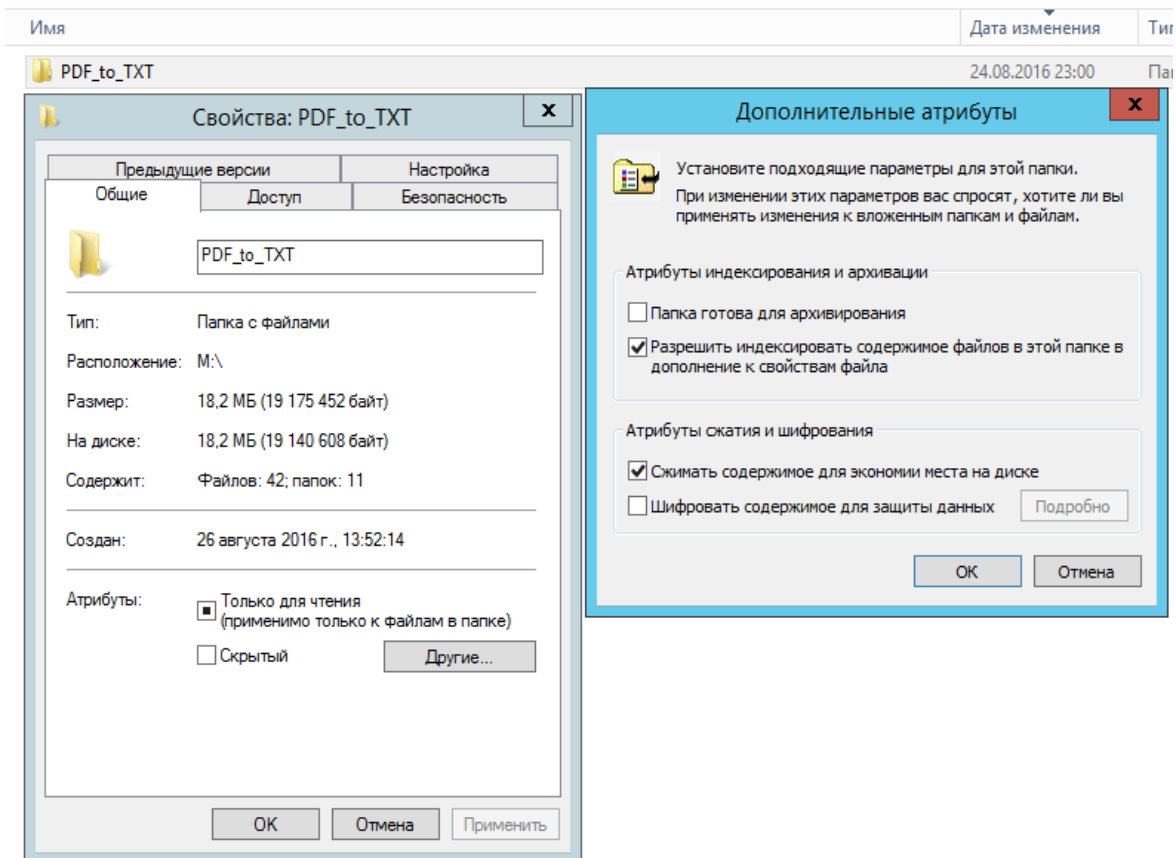


Рисунок 2 – Интерфейс настройки “Сжимать содержимое для экономии места на диске”

Для создания архивных копий, позволяющих восстанавливать ОС, следует воспользоваться специальными средствами. Работая с ОС Windows, вызовем “Панель управления”. В разделе "Система и безопасность" (см. Рисунок 3) доступны средства “Резервное копирование и восстановление (Архивация и восстановление Windows 7). Восстановление файлов из резервной копии)” и “История файлов (Сохранение резервных копий с помощью истории файлов. Восстановление файлов с помощью истории файлов)”.

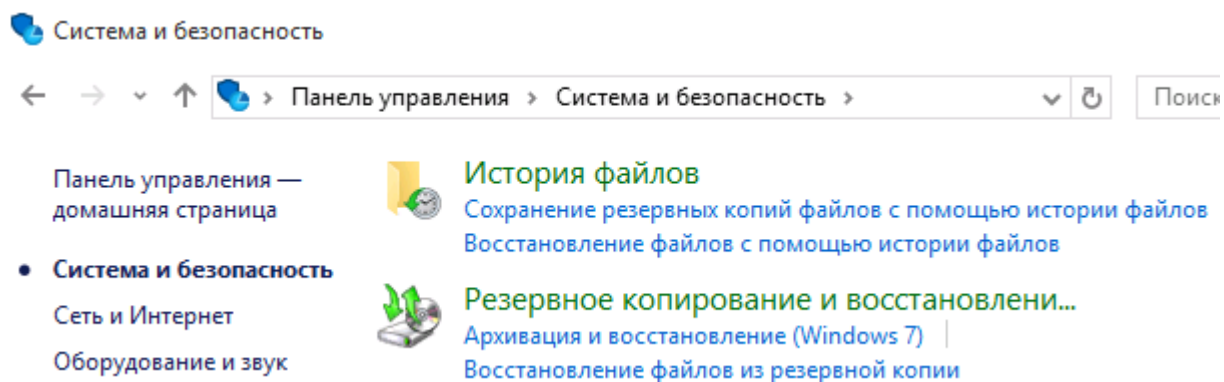


Рисунок 3 – Инструментарий создания архивных копий встроенными средствами ОС Windows 10

Рассмотрим подробнее предлагаемый инструментарий. Существует несколько способов создать резервную копию операционной системы компьютера [3]:

1. Нажимаем кнопку “Пуск”, затем выбираем “Панель управления”, в ней – “Система и безопасность”, а далее “Архивация и восстановление”.

2. Выполняем одно из указанных ниже действий. Если ни разу не использовали программу архивации данных или недавно обновлялась версия Windows, выбираем “Настроить резервное копирование”, а затем выполняем действия, предлагаемые Мастером. Если создавали ранее резервную копию, то можно дождаться запланированного резервного копирования или вручную создать резервную копию, выбрав “Создать резервную копию”. Если ранее создавали резервную копию, но хотим создать полную резервную копию, а не обновлять старую, выбираем “Создать”, “Полная резервная копия”, а затем выполняем действия, предлагаемые Мастером.

Перед выполнением лабораторных работ рекомендуется ознакомиться со списком литературы [3-12]. В пособии “Active Directory – архитектура, планирование развертывания и внедрение” [3] рассмотрены некоторые вопросы, связанные с обеспечением безопасности компьютеров, введенных в домен (в настоящем пособии эти вопросы не рассматриваются), в работах [4-12] можно найти ответы на вопросы, связанные с архивированием, резервным копированием и восстановлением данных.

## **2.1 Выполнение практической работы по теме (Лабораторная работа 1). Создание резервной копии средствами ОС Windows 10**

**Задание:** сконфигурировать виртуальную машину для выполнения лабораторной работы, создать резервную копию файлов, подлежащих архивированию, согласно индивидуальному заданию лабораторной работы.

Используемые файлы для выполнения лабораторной работы: VHD (или VHDX) диск с установленной ОС Windows 10 Enterprise, пустой VHD (VHDX) диск, аналогичный по параметрам первому, для сохранения архивных копий. Для доступа к гостевой операционной системе используется учетная запись Student с административными правами, пароль Pa\$\$w0rd. Для выполнения лабораторной работы может использоваться альтернативная конфигурация виртуальной машины, когда резервная копия сохраняется не на пустой (второй) виртуальный жесткий диск, а копируется в сетевую папку. В этом случае необходимо выполнить настройку доступа к сетевому окружению, используя информацию по настройке, полученную от преподавателя.

## **2.2 Ход выполнения лабораторной работы**

**Подготовительный этап.** Следует проверить конфигурацию виртуальной машины, используемой в лабораторной работе (см. Рисунок 4). Обратите внимание на наличие используемых виртуальных дисков и на объем оперативной памяти, выделяемой для работы виртуальной машины. Рекомендуется выставить флажок в позиции “Включить динамическую память”. Запускаем виртуальную машину с ОС Windows 10 Enterprise. Выполняем вход в гостевую ОС, используя учетную запись Student и пароль Pa\$\$w0rd. После этого делаем снимок (снапшот) состояния, что позволяет вернуться к исходному состоянию, если в ходе выполнения работы возникли какие-либо проблемы, по которым всю лабораторную работу (или один из ее этапов) потребуется выполнить с самого начала. Рекомендуемое имя start для снимка виртуальной машины (см. Рисунок 4 – кнопка 1). Для возврата к исходному состоянию используется соседняя кнопка (см. Рисунок 4 – кнопка 2). Во время выполнения работы можно создавать снапшоты (не более 50) с разными именами, в этом случае при необходимости можно будет вернуться к тому состоянию виртуальной машины, для которого был создан снапшот.

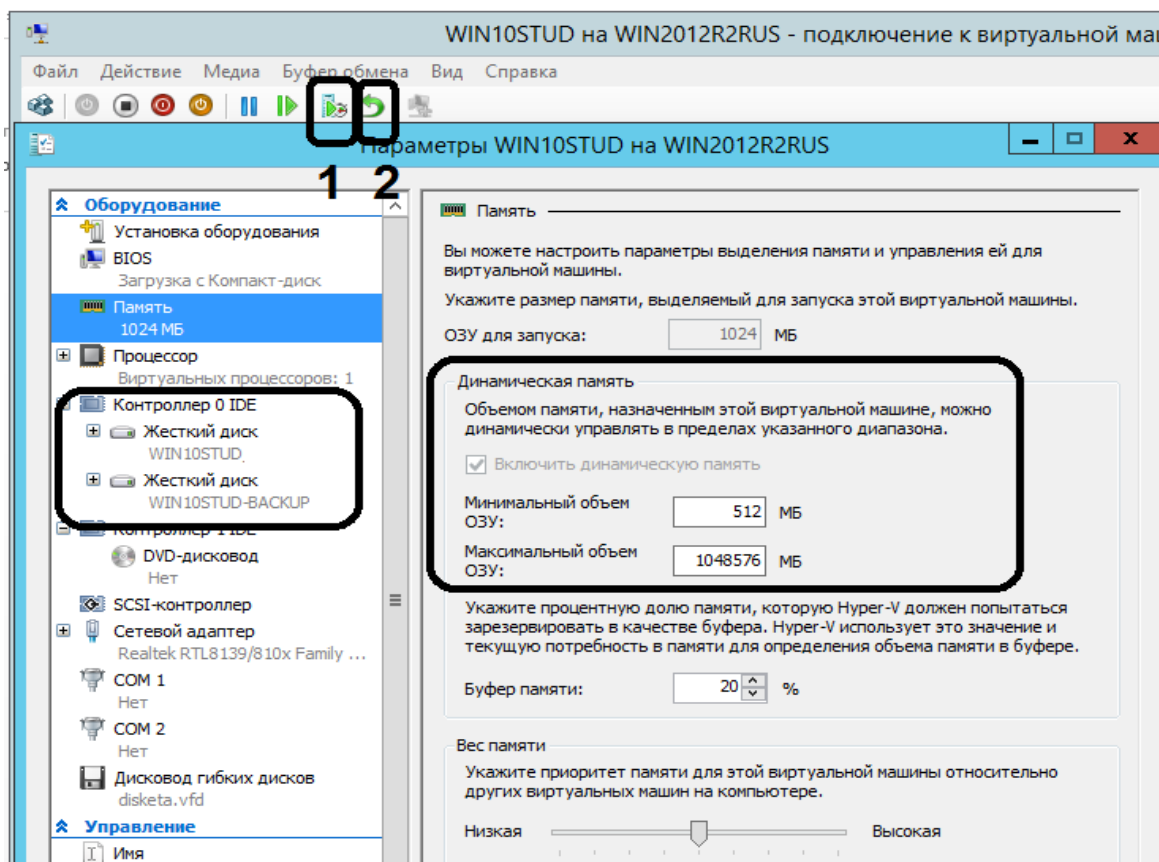


Рисунок 4 – Конфигурация виртуальной машины

Основная часть лабораторной работы – создание архива файлов, создание образа системы, создание диска восстановления системы. Перед тем, как приступить к выполнению операции создания архива, создаем на диске *C* папку *TEST1*, а в этой папке – текстовый файл (например, с именем *Нужный файл.txt*). В созданном файле записываем несколько строк. Этот файл затем будем восстанавливать. Моделируется ситуация, когда пользователь случайно изменил информацию в файле и ему требуется ранее сохраненная версия этого файла.

Создав и сохранив файл, выбираем “Резервное копирование и восстановление” (см. Рисунок 5).

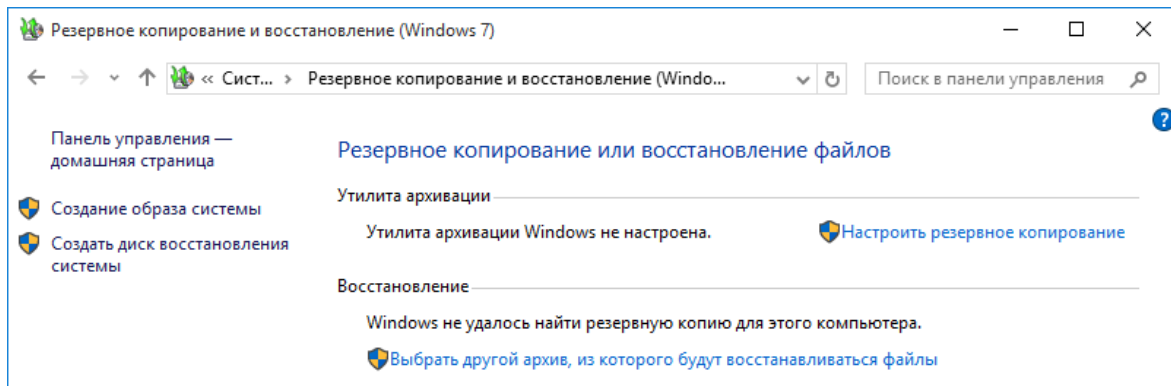


Рисунок 5 – Панель копирования и восстановления

Определяем диск, на который будем сохранять резервную копию (см. Рисунок 6).

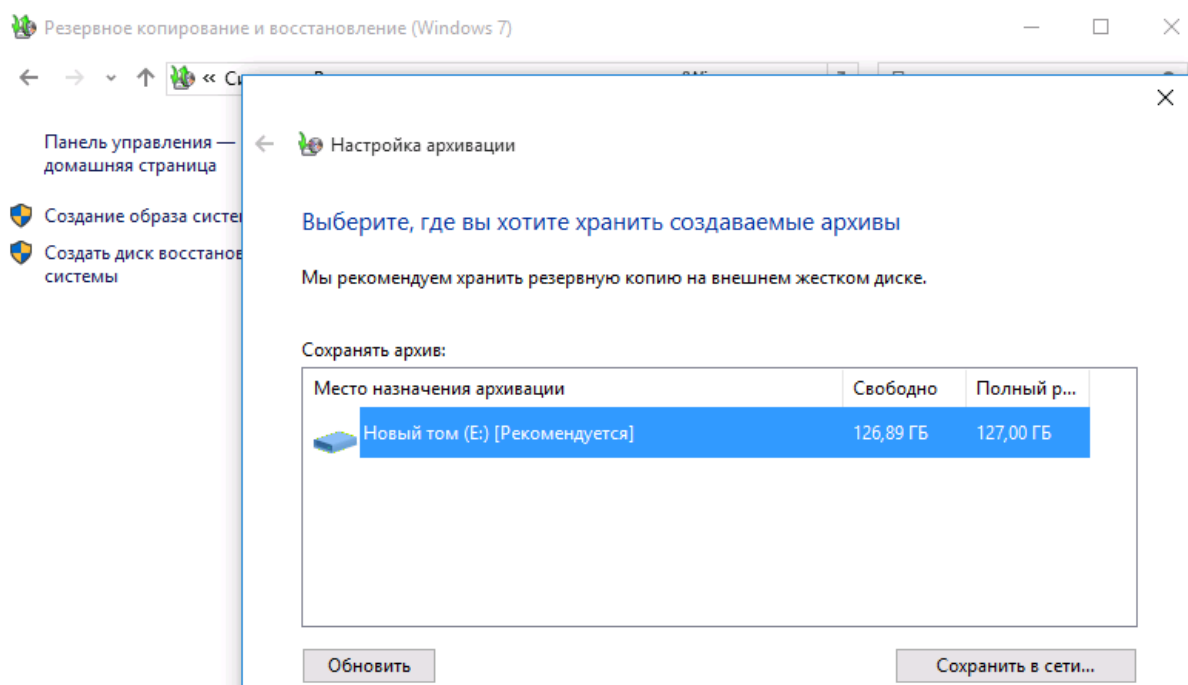


Рисунок 6 – Выбран диск для размещения резервной копии

Выбираем Радиокнопку (см. рисунок 7) “Предоставить мне выбор” на вопрос “Что вы хотите архивировать?”.



### Что вы хотите архивировать?

Предоставить выбор Windows (рекомендуется)

Windows выполнит архивацию файлов, сохраненных в библиотеках, на рабочем столе и в стандартных папках Windows. Также Windows создаст образ системы, который можно использовать для восстановления компьютера в случае неполадок. Эти объекты будут регулярно архивироваться по расписанию.

Предоставить мне выбор

Вы можете выбрать библиотеки и папки, а также указать, следует ли включать в резервную копию образ системы. Выбранные элементы будут регулярно архивироваться по расписанию.

Рисунок 7 – Панель выбор архивируемых элементов

Продолжаем операцию конфигурирования, указав (см. Рисунок 8), что архивации подлежат файлы данных “Библиотеки пользователя Student”, данные папки C:\TEST1 и что необходимо включить в создаваемый архив образ системы “Зарезервировано системой, (C:)”.

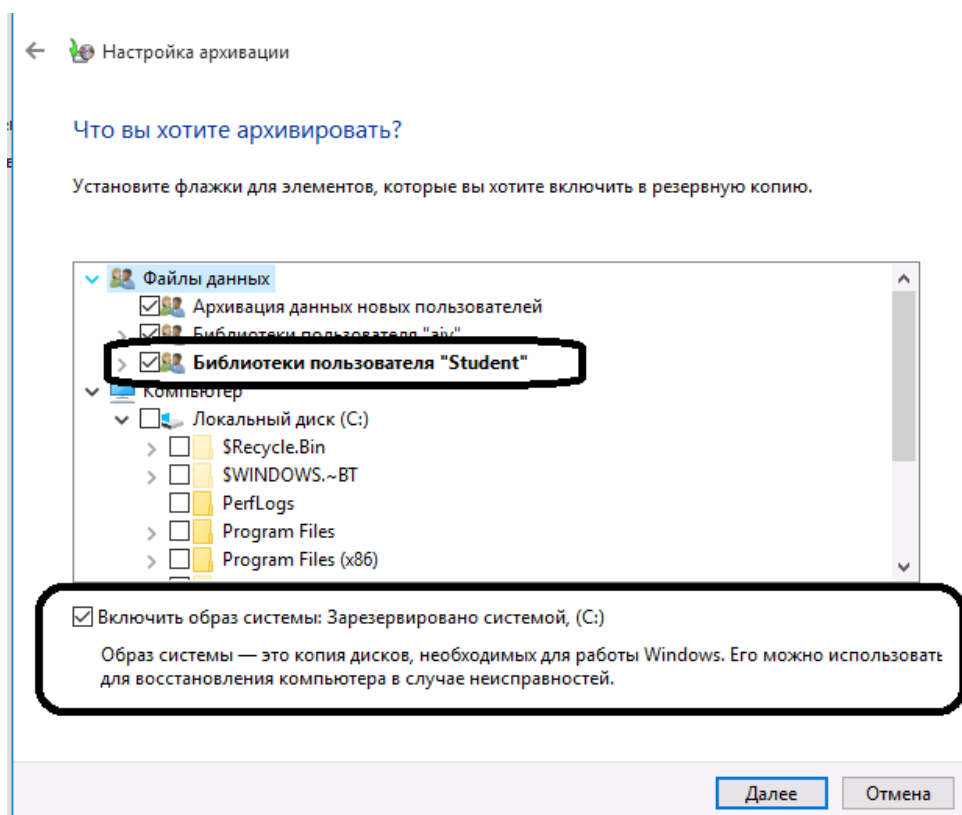


Рисунок 8 – Панель выбора файлов и включения образа системы

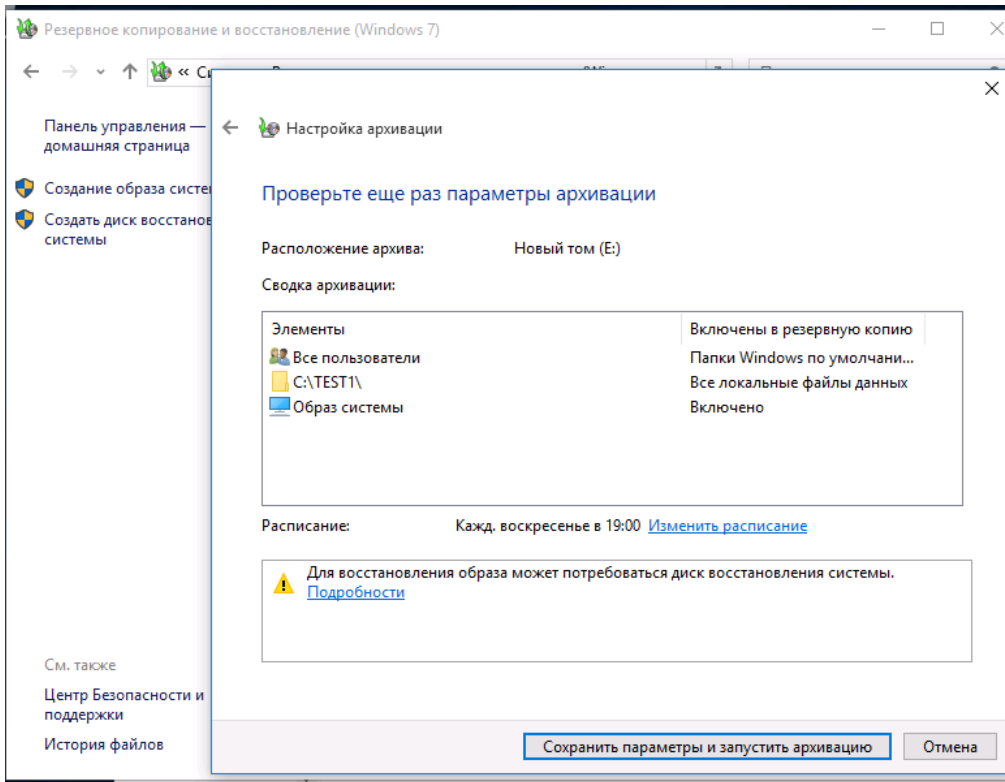


Рисунок 9 – Панель, позволяющая сохранить параметры и запустить архивацию

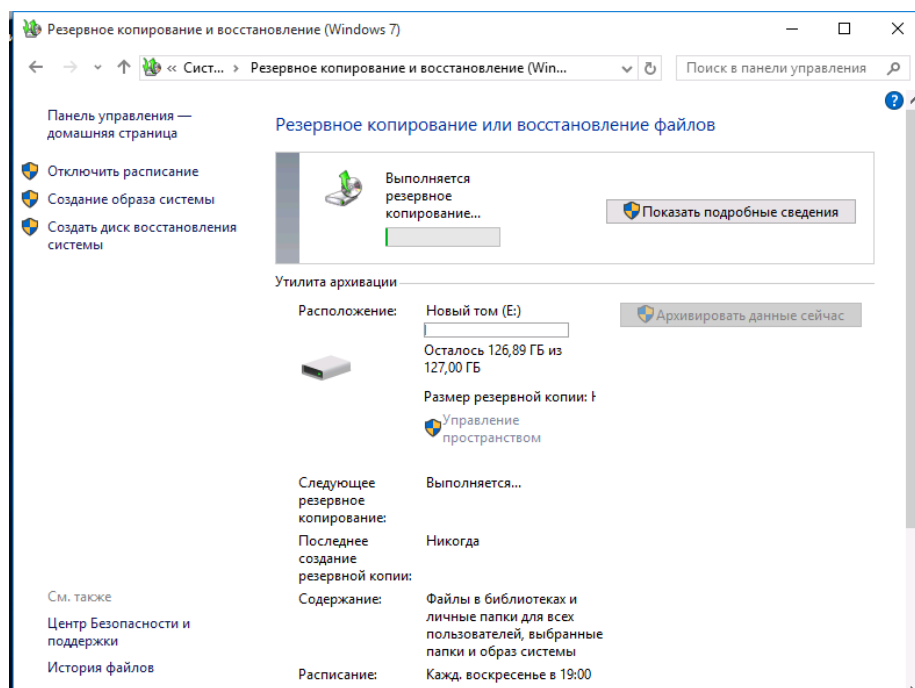


Рисунок 10 – Окно с информацией о выполняемом резервном копировании

Образ системы представляет собой копию дисков, необходимых для работы ОС Windows. Образ системы можно использовать для ее восстановления в случае неисправностей. Завершив выбор компонентов, переходим к следующему окну, позволяющему еще раз проверить параметры архивации перед запуском (см. Рисунок 9). Обратите внимание на позицию “Расписание – *Изменить расписание*”. Нажимаем кнопку “Сохранить параметры и запустить архивацию”. Контролируйте ход выполнения архивации (см. Рисунок 10).

В отчете к лабораторной работе отметьте, сколько времени потребовалось на выполнение операции архивации. Время, затрачиваемое на архивацию, зависит от размера архивируемых файлов, а также от быстродействия компьютера, на котором выполняется операция архивации.

**Создание диска восстановления.** Пункт выполняется опционально по заданию преподавателя. Для выполнения этого пункта работы необходимо иметь возможность работать с записывающим DVD-устройством на хостовом компьютере (для записи используются перезаписываемые DVD диски – DVD RW) или использовать эмулятор DVD-устройства, устанавливаемый в виртуальную машину.

Установка эмулятора DVD-устройства не описывается, т.к. существует достаточно большое число программ такого назначения, различающихся стоимостью, поддержкой базового функционала и дополнительными возможностями управления записью. Например, DAEMON Tools Pro – популярный инструмент для эмуляции оптических дисков и виртуализации приводов с дополнительными возможностями монтирования образов; DAEMON Tools Ultra – многофункциональное приложение, сочетающее в себе все основные функции популярного эмулятора оптических приводов DAEMON Tools; Alcohol 52% Free Edition – бесплатная версия популярного эмулятора CD/DVD-приводов – позволяет создавать до 6 виртуальных приводов с образами, поддерживает все версии современных форматов CD/DVD дисков.

Для выполнения этого задания по первому варианту (работа с физическим устройством – пишущим DVD приводом) потребуется доступ виртуальной машины к физическому устройству для записи компакт-дисков на родительской машине, под управлением которой работает виртуальная машина. Для этого в настройках виртуальной машины указываем (см. Рисунок 11) выбор опции монтирования физического дисководов компакт- и DVD-дисков для использования виртуальной машиной. В виртуальной машине в системе

“Резервное копирование и восстановление файлов” выбираем позицию “Создать диск восстановления системы” (см. Рисунок 12). Выбрав устройство DVD RW, вставляем записываемый диск в физическое устройство для записи компакт-дисков, нажимаем кнопку “Создать диск”. Контролируем процесс создания диска восстановления.

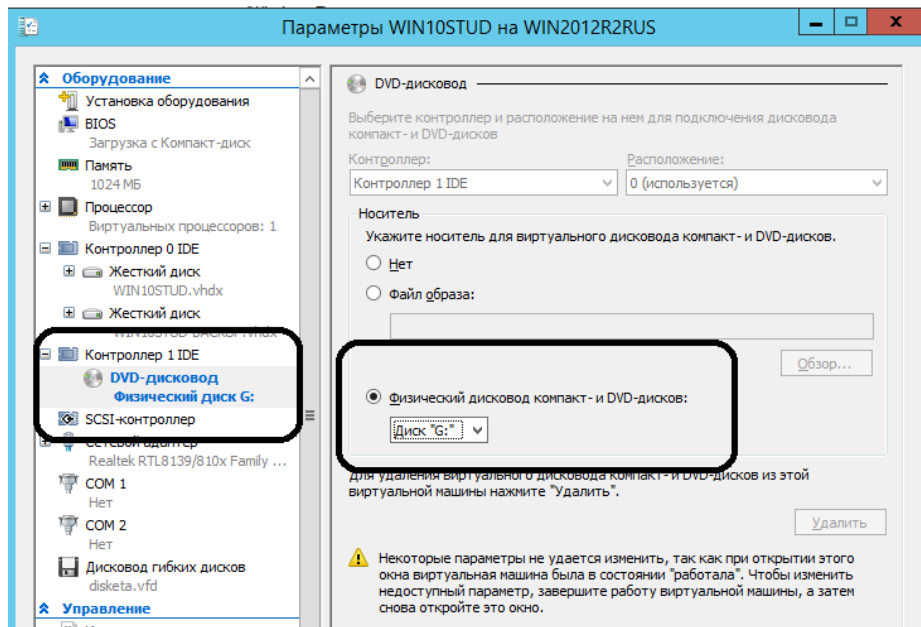


Рисунок 11 – Монтирование физического дисквода компакт и DVD-дисков для использования виртуальной машиной

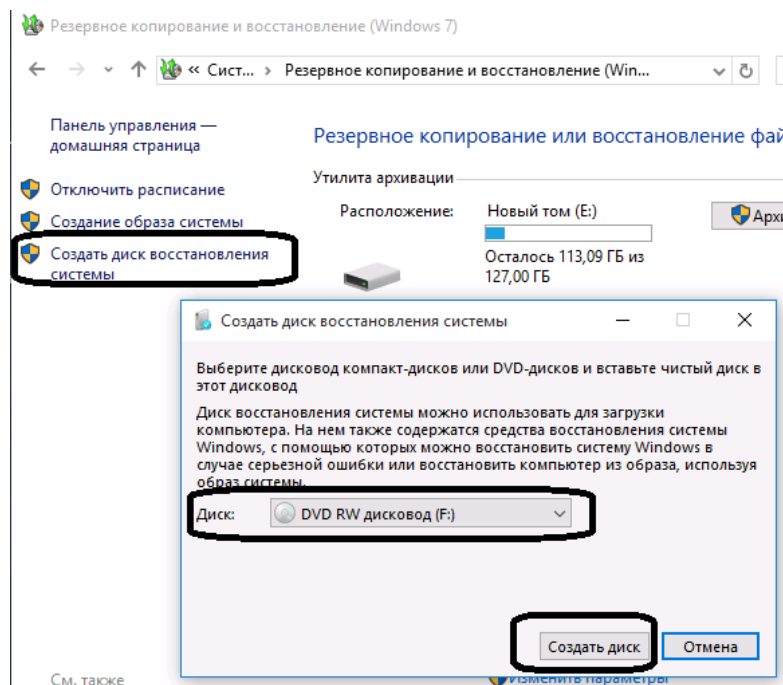


Рисунок 12 – Интерфейс создания диска восстановления системы

После создания диска для восстановления системы (если этот этап лабораторной работы выполнялся) переходим к этапу создания образа системы – пункт “Создание образа системы” (см. Рисунок 13).

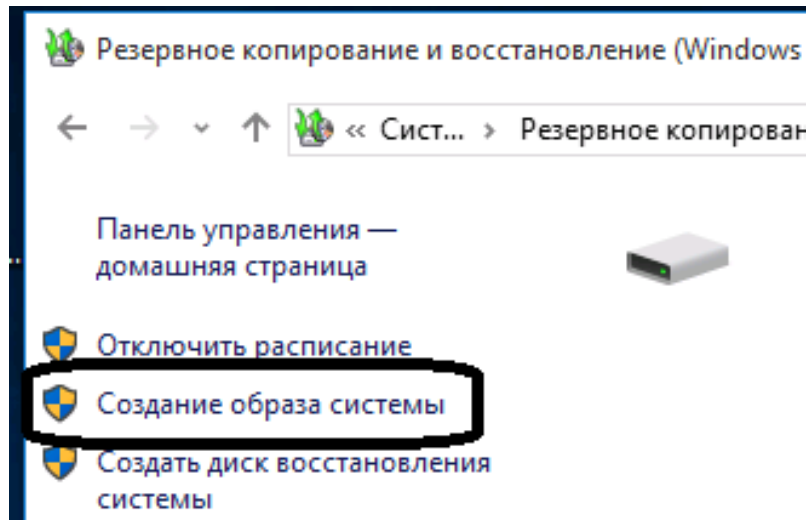


Рисунок 13 – Создание образа системы

Выбрав пункт “Создание образа системы”, определяем (см. Рисунок 14) место хранения архива – поддерживаются возможности размещения архивов 1) на жестком диске, 2) на DVD-дисках, 3) в качестве места для размещения может использоваться сетевая папка.

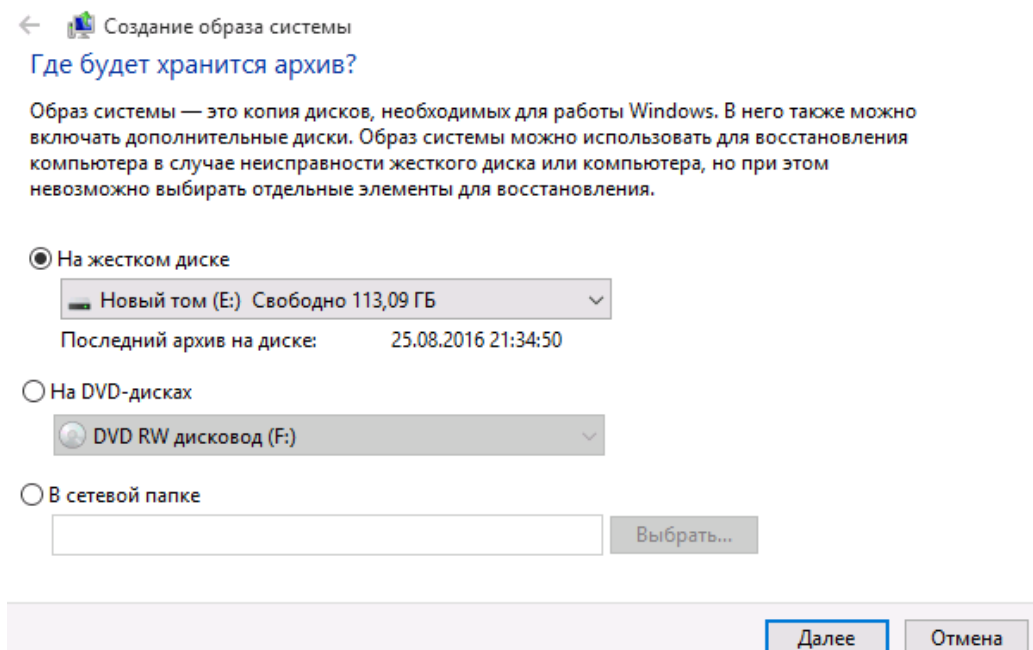


Рисунок 14 – Вид интерфейса, определяющего место хранения архива

После выбора места архивирования нажимаем кнопку “Архивировать” (см. Рисунок 15) и отслеживаем выполнение процесса архивирования. В отчете необходимо отметить общее время, затраченное на архивирование, размер полученного архива в мегабайтах.

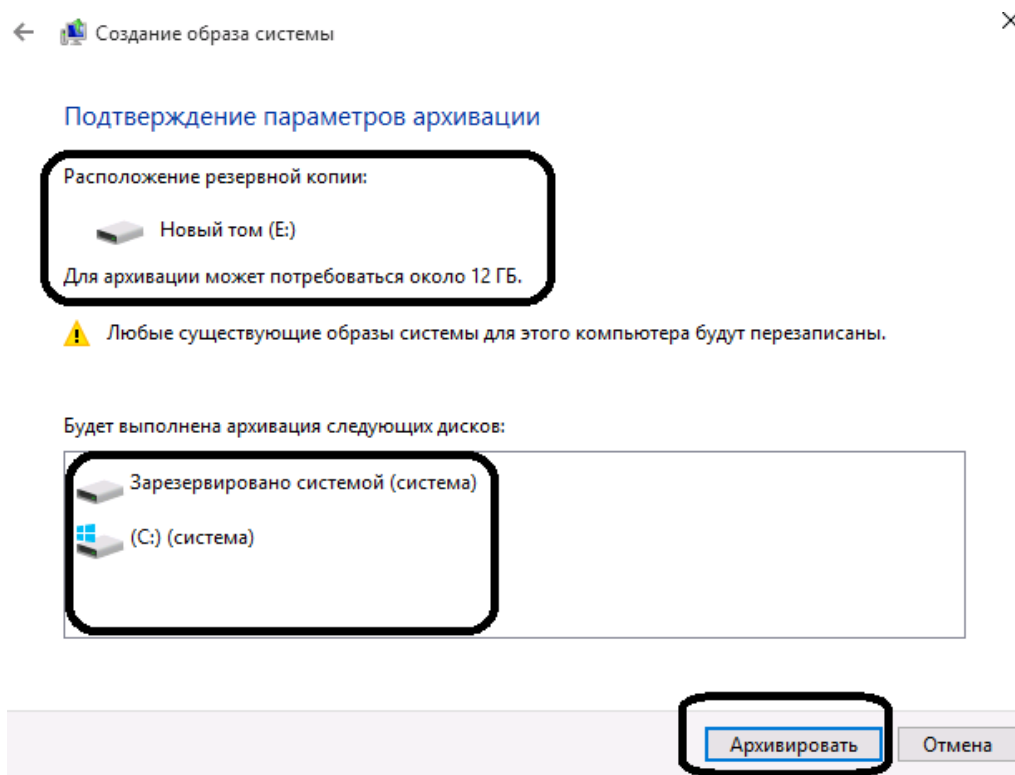


Рисунок 15 – Кнопка “Архивировать”, нажатие запускает процесс архивации

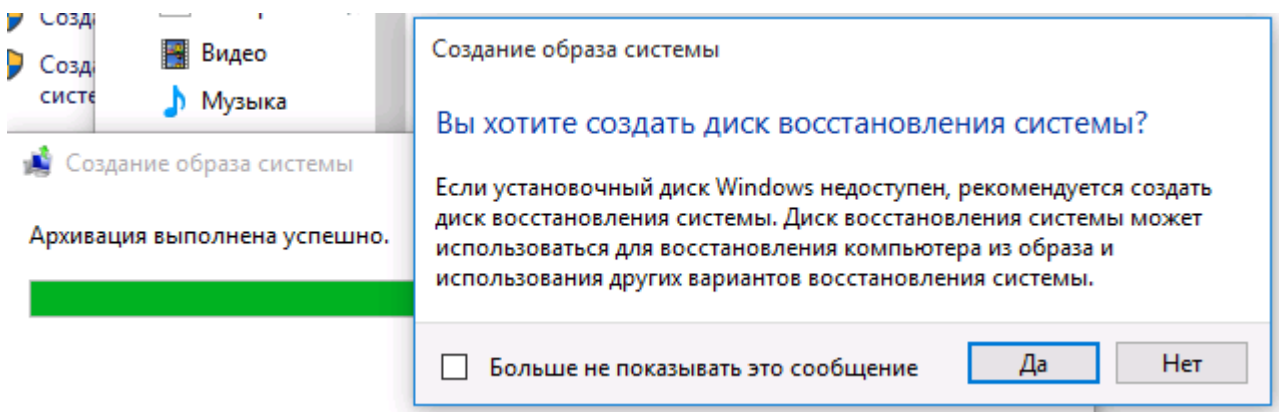


Рисунок 16 – Окно интерфейса создания диска восстановления системы

Отметим, что если диск восстановления системы не был создан ранее, то его можно создать после запуска процесса архивирования (см. рисунок 16). В ходе выполнения данного пункта лабораторной работы создавать диск восстановления не требуется – на вопрос отвечаем “Нет”.

В качестве дополнительного элемента в ходе выполнения лабораторной работы преподавателем может быть предложено выполнить восстановление ОС с использованием созданного образа системы.

### 2.3 Контрольные вопросы

1. Перечислите этапы выполнения работы.
2. Какое средство виртуализации используете в ходе выполнения работы?
3. Какую информацию необходимо отразить в отчете о проделанной работе?
4. Назовите основные возможности системы “Резервное копирование и восстановление Windows”.
5. Где можно размещать архивы, создаваемые системой “Резервное копирование и восстановление Windows”?
6. Поддерживается ли возможность размещения архивов, создаваемых системой “Резервное копирование и восстановление Windows”, в облачных хранилищах (Microsoft Azure)?
7. Опишите процесс создания диска восстановления. Какое оборудование для этого потребуется?

### **3 РЕЗЕРВНОЕ КОПИРОВАНИЕ ФАЙЛОВ И ПАПЕК WINDOWS SERVER В ОБЛАЧНОЕ ХРАНИЛИЩЕ MICROSOFT AZURE**

В настоящее время большинство компьютеров работает в локальных сетях с возможностью доступа к ресурсам глобальной сети Интернет. Размещение резервных копий в облачных хранилищах имеет ряд преимуществ по сравнению с традиционным хранением локальных архивных копий. Облачные хранилища, как правило, являются геораспределенными – при создании архивной копии можно указать создание нескольких экземпляров, которые будут храниться в разных центрах обработки данных (пользователь может выбрать расположение центров хранения данных, в том числе хранилища, находящиеся на разных континентах), что значительно повышает надежность хранения данных и их доступность. Если будет потерян доступ к одному из центров хранения данных (например, он полностью разрушен в результате стихийного бедствия), то это не приведет к потере данных, в отличие от ситуации, когда несколько копий хранятся только в одном центре обработки данных. Отметим, что хранение данных в облаке становится год от года все более популярным у пользователей. Этому способствует повышение пропускной способности каналов связи, а также снижение стоимости хранения архивов в облачных хранилищах. Одним из сдерживающих факторов выступает недоверие некоторых пользователей к тому, что данные хранятся где-то в сети, а не на физических серверах пользователей. Заметим, что такие опасения оправданы в том случае, если пользователи используют слабые (легко подбираемые) пароли, пренебрегают использованием систем шифрования хранимых данных, не следят за сохранностью конфиденциальной информации (паролями для работы с облачными службами, ключами шифрования и т.д.)

Рассмотрим работу со службой архивации Azure [12], являющейся достаточно простым и экономичным решением архивации, дополняющей проверенные и надежные локальные средства архивации, поддерживаемые ОС Windows и мощными многофункциональными инструментами создания архивных копий, размещаемых в облаке. Служба архивации Azure достаточно универсальна и может удовлетворить запросы разных пользователей компьютерных систем, от пользователей домашних компьютеров до корпоративных пользователей крупных организаций, Служба архивации Azure (интегрированная с Azure Site Recovery), позволяет выполнять автономное резервное копирование и восстановление данных компьютерных систем, поддерживает унифицированную доступность приложений и защиту данных [12].



Отметим основные преимущества использования средств облачного резервного копирования (Azure Backup):

1. высокая, практически постоянная доступность сервисов создания и восстановления архивных копий (пользователям Azure гарантируется, что сервисы будут доступны не менее 99,9% времени в течении года);
2. высочайшая надежность – для обеспечения сохранности данных создается три копии архива в одном дата-центре с возможностью настройки дополнительной георепликации архивных копий в другие дата-центры;
3. неограниченный объем хранилища для размещения архивных копий (ограниченный только платежеспособностью самого пользователя, оплачивающего услуги облачного хранения данных) с возможностью гибкого масштабирования хранилища под любые задачи;
4. удобство работы – поддерживается удобный, хорошо знакомый, а потому интуитивно понятный для Windows-администраторов интерфейс управления;
5. конфиденциальность – поддерживаются современные криптостойкие алгоритмы шифрования данных при передаче и хранении;
6. эффективное хранение данных за счет возможности создания инкрементальных копий архивируемых данных (добавляются только те данные, которые не были изменены по сравнению с ранее созданной копией – такое решение позволяет не только значительно уменьшить объем архивируемой информации и время, необходимое для выполнения архивации, но и снижает стоимость хранения вновь создаваемой архивной копии);
7. облачная архивация может выступать альтернативным решением долгосрочного хранения данных на магнитных лентах, так как облачный провайдер берет на себя ответственность за хранение данных – архивированные данные хранятся в нескольких экземплярах на отказоустойчивых файловых хранилищах, состояние информационных носителей в таких хранилищах постоянно контролируется, носители, вырабатывающие свой эксплуатационный ресурс, оперативно заменяются новыми;
8. поддерживаются в полном объеме все современные решения для автоматизации оперативной архивации данных [12].

### **3.1 Выполнение практической работы по теме (Лабораторная работа 2). Резервное копирование файлов и папок с помощью службы архивации Azure с использованием модели развертывания Resource Manager**

**Задание:** в ходе выполнения лабораторной работы моделируется типовая, часто встречающаяся ситуация, когда системному администратору необходимо настроить систему резервного копирования данных в облачное хранилище – Windows Azure. При выполнении лабораторной работы необходимо:

1. Выполнить настройку виртуальной машины, конфигурация аналогична использованной при выполнении первой лабораторной работы. Проверить наличие доступа к сети Интернет из виртуальной машины. Получить у преподавателя учетную информацию для работы с облачными службами.
2. Сконфигурировать службы в облаке для обеспечения возможности размещения архивных копий файлов в облачное хранилище. Установить и настроить агент для копирования архивных данных в облако, выполнить копирование папки, содержащей архивируемые файлы, в облачное хранилище.
3. *Дополнительный пункт (выполняется по заданию преподавателя при наличии времени и технической возможности) – выполнить восстановление информации из архивов, размещенных в облачных хранилищах.*

### **3.2 Ход выполнения лабораторной работы**

Процесс создания резервной копии файлов и папок в облаке может быть кратко представлен последовательностью из пяти основных пунктов:

1. Оформление пользователем подписки Azure (для выполнения лабораторной работы используются данные, предоставленные преподавателем).
2. Создание хранилища служб восстановления.
3. Скачивание необходимых файлов для развертывания агента служб восстановления.
4. Установка и регистрация агента служб восстановления.
5. Архивация файлов и папок в соответствии с заданием лабораторной работы.

Рассмотрим подробнее вышеперечисленные пункты (за основу была взята методика, предложенная Microsoft [13]).

## 1. Оформление подписки Azure.

Несмотря на то, что для выполнения лабораторной работы учетные данные предоставляются преподавателем, при желании можно получить бесплатную пробную подписку [14]. Возможность получения бесплатного доступа была успешно опробована авторами пособия. Для оформления доступа необходимо наличие банковской карты (дебетовая, кредитная), позволяющей оплачивать покупки в сети Интернет. Во время оформления вводятся данные карты и ее владельца, необходимые для выполнения платежа. В момент регистрации на карточном счете может быть заблокирована сумма, меньшая или равная 1 доллару США, как результат проверки того, что указанная карта действительно существует и выпустивший ее банк поддерживает выполнение операций с выпущенной картой. Через некоторое время (в случае авторов – в срок чуть меньше недели) заблокированные на карте средства снова стали возможными для использования. Такой подход, используемый Microsoft, позволяет бороться с повторными регистрациями пользователей, желающих многократно использовать возможности тестового доступа, которым каждый человек может воспользоваться только один раз.

## 2. Создание хранилища служб восстановления.

После входа в систему необходимо создать хранилище служб восстановления в том регионе, в котором планируется хранить данные, и определить способ репликации хранилища. Для создания хранилища служб восстановления в главном меню выбираем “Обзор”, затем в списке ресурсов вводим “Службы восстановления” и щелкаем “Хранилища служб восстановления” (см. рисунок 17). В меню “Хранилища служб восстановления” щелкаем “Добавить”.

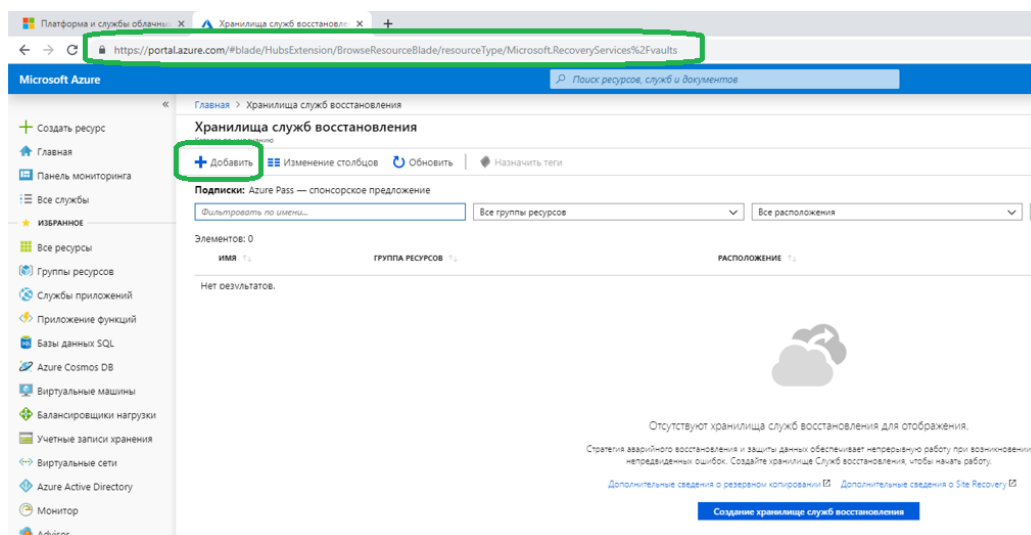


Рисунок 17 – Окно интерфейса “Хранилище служб восстановления”

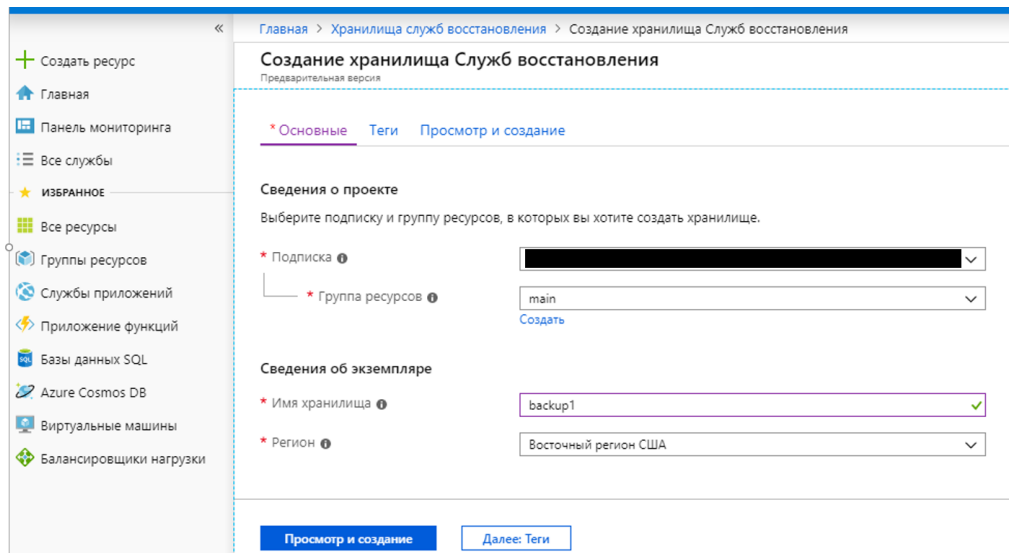


Рисунок 18 – Фрагменты интерфейса “Цель резервного копирования”

Открывается колонка хранилища служб восстановления, в которой указываем имя, подписку, группу ресурсов и место расположения. В поле “Имя” вводим имя хранилища. В поле “Расположение” выбираем географический регион, в котором будет находиться хранилище, и щелкаем “Создать”.

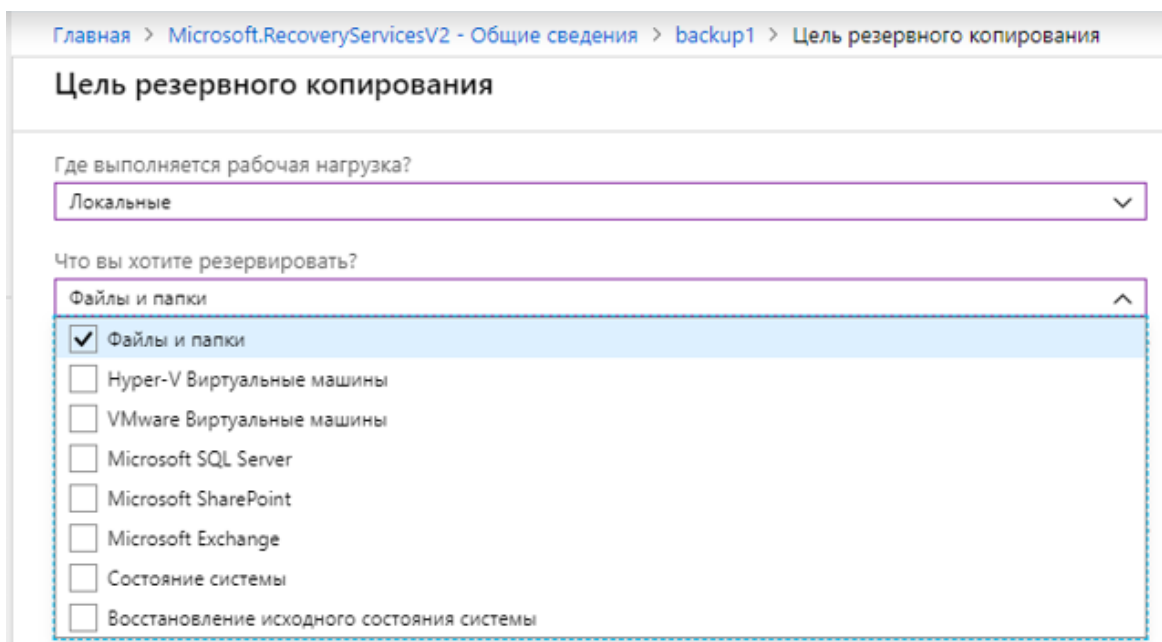


Рисунок 19 – Интерфейс “Цель резервного копирования”. Позиция “Файлы и папки”

Если созданное хранилище не отображается в окне просмотра, то следует использовать пункт *“Обновить”*. При первом создании хранилища служб восстановления определяется способ его репликации (см. Рисунок 18). Щелкаем *“Новое хранилище”*, чтобы открыть панель мониторинга. В колонке *“Параметры”* щелкаем *“Инфраструктура резервного копирования”*. В колонке *“Инфраструктура резервного копирования”* щелкаем *“Конфигурация архивации”* для просмотра типа репликации хранилища. Выбираем нужный тип репликации для хранилища (см. Рисунок 19). В соответствии с указаниями преподавателя в отчете отмечаем возможные типы репликации, доступные для выбора. Создав хранилище, подготавливаем инфраструктуру к архивации файлов и папок. Для этого скачиваем учетные данные хранилища и агент служб восстановления Microsoft Azure. Для скачивания файлов на панели мониторинга хранилища служб восстановления щелкаем *“Параметры”*. Открывается колонка *“Цели резервного копирования”*. В колонке *“Параметры”* щелкаем *“Присутная к работе > Архивация”*. В колонке *“Резервное копирование”* щелкаем *“Backup goal”* (Цель архивации). В меню *“Где выполняется рабочая нагрузка?”* выбираем *“Локально”*. В меню *“Что вы хотите резервировать?”* выбираем *“Файлы и папки”* и нажимаем кнопку *“ОК”*.

3. Для скачивания агента служб восстановления в колонке *Подготовка инфраструктуры* щелкаем *“Скачать агент для Windows Server или Windows Client (Download Agent for Windows Server or Windows Client)”*. Во всплывающем окне скачивания щелкаем *“Сохранить”*. По умолчанию файл *MARSagentinstaller.exe* сохраняется в папке для скачивания.

#### 4. Установка и регистрация агента.

Находим и дважды щелкаем файл *MARSagentinstaller.exe* в папке для скачивания (или в другом расположении). Выполняем шаги Мастера настройки агента служб восстановления Microsoft Azure (см. Рисунок 20).

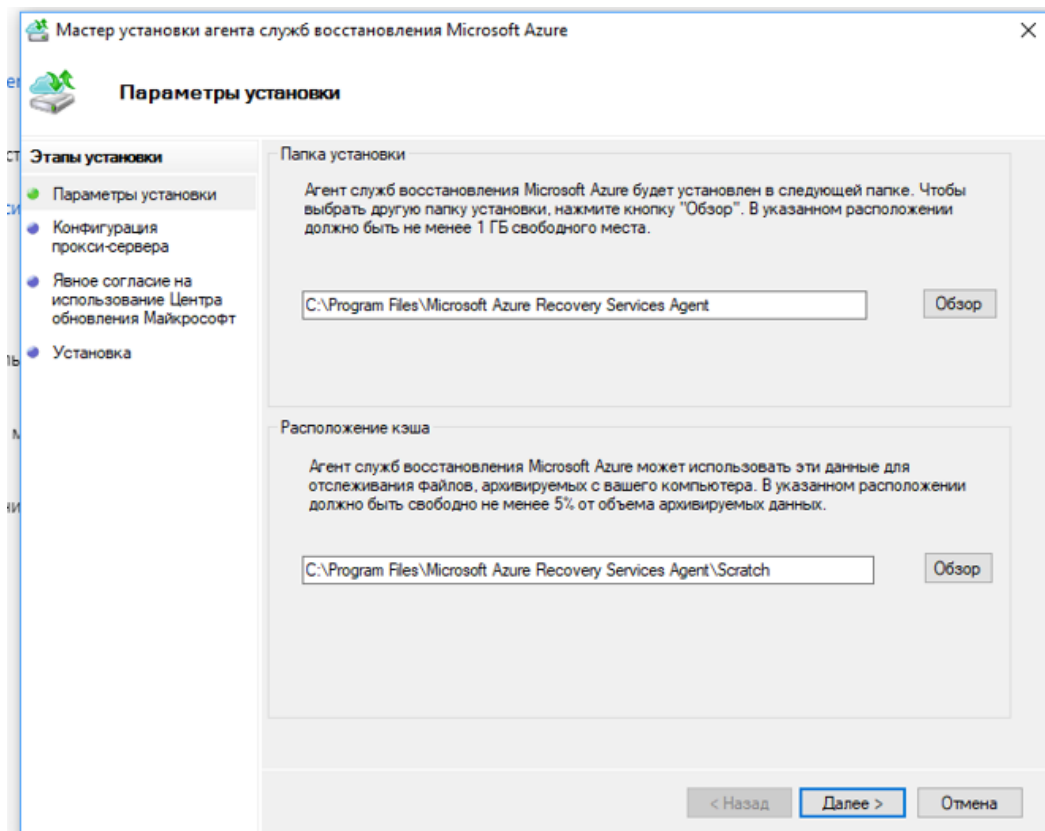


Рисунок 20 – Интерфейс Мастера установки агента восстановления Microsoft Azure

Для завершения работы с Мастером нужно: выбрать папку установки и папку кэша; если для подключения к Интернету используется прокси-сервер, указать данные прокси-сервера (см. Рисунок 21); если используется прокси-сервер, прошедший проверку подлинности, ввести имя пользователя и пароль; указать скачанные учетные данные хранилища; сохранить парольную фразу (пароль) шифрования (см. Рисунок 22) в безопасном месте. **Важно!** Пользователь сам отвечает за сохранность пароля, если он его забыл или потерял, то восстановить данные будет нельзя! После того, как агент установлен и компьютер зарегистрирован в хранилище, можно настроить параметры резервного копирования, в том числе по расписанию.

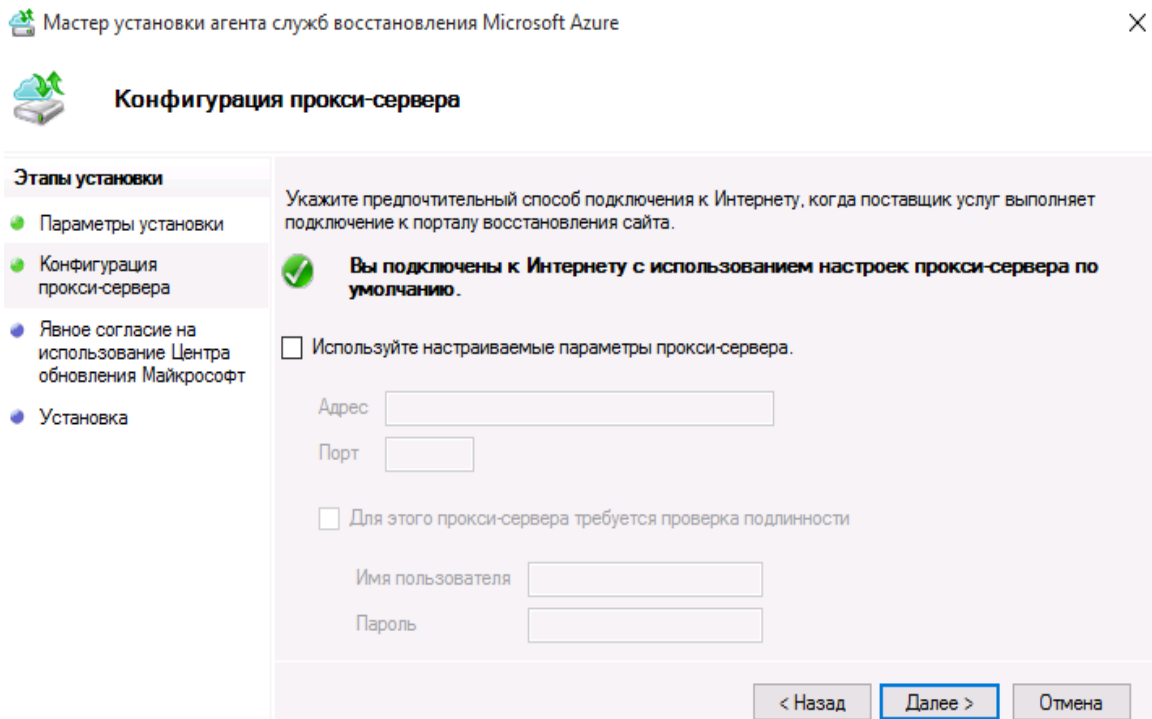


Рисунок 21 – Интерфейс конфигурации прокси-сервера

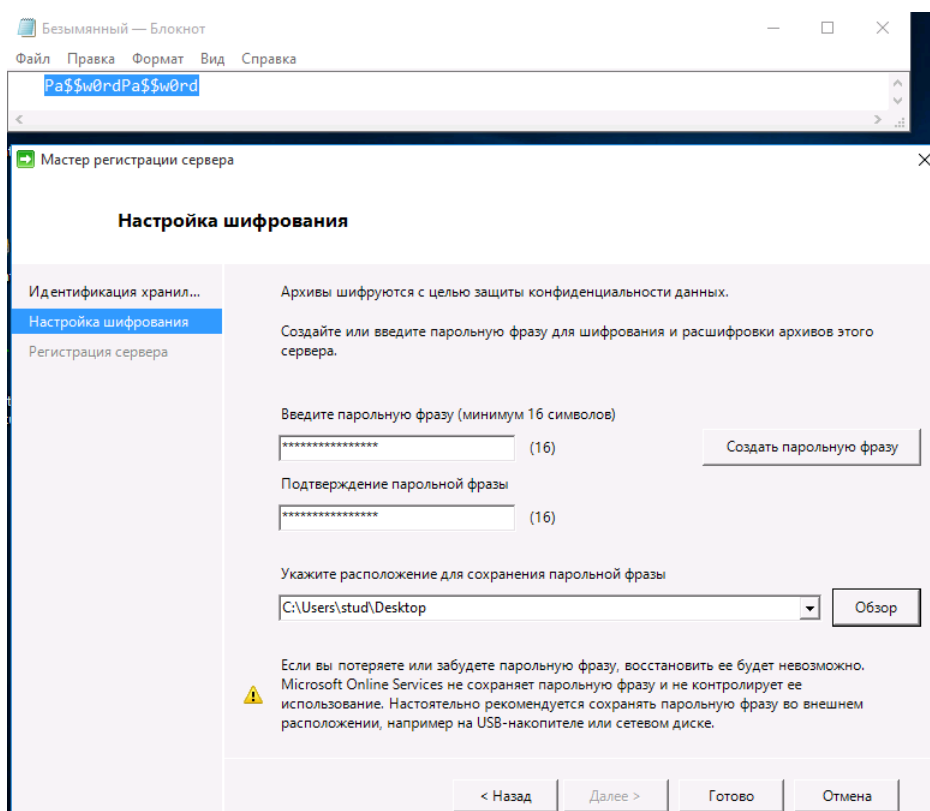
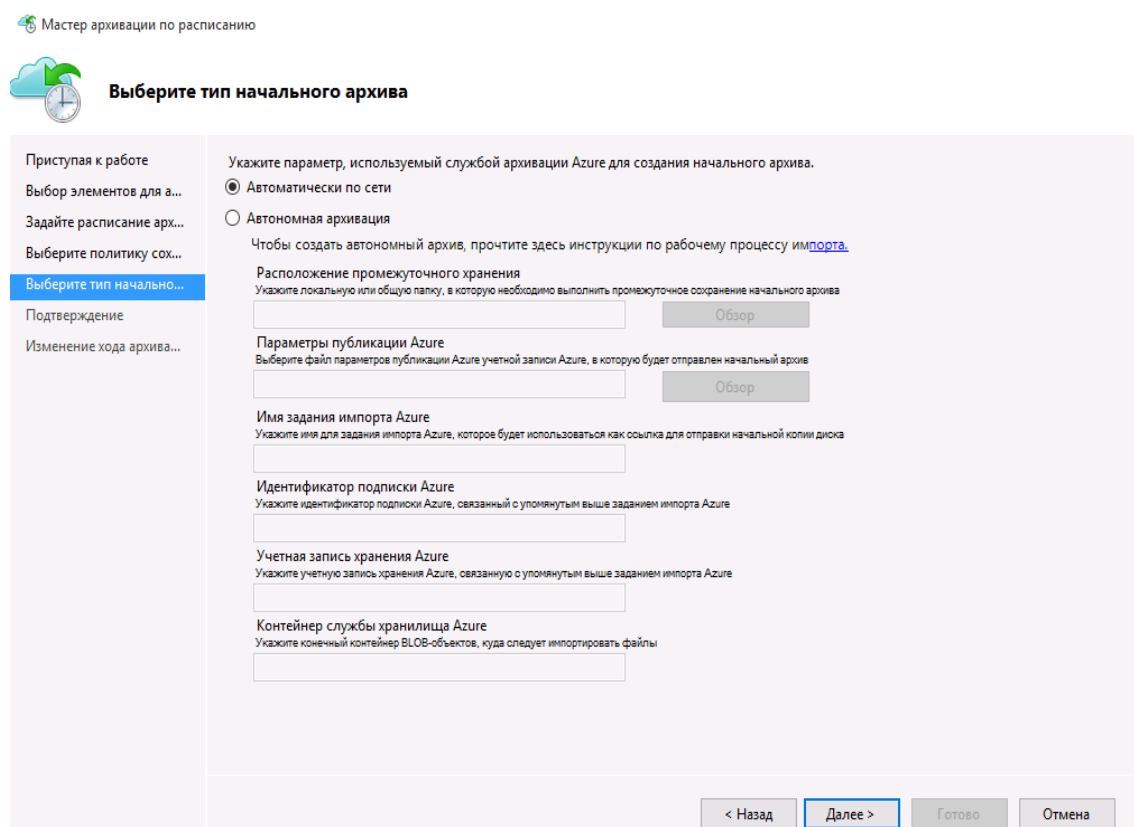


Рисунок 22 – Интерфейс настройки шифрования

## 5. Резервное копирование файлов и папок.

Чтобы выполнить первоначальную архивацию, используем агент служб восстановления Microsoft Azure. Открываем “Агент служб восстановления Microsoft Azure”. В агенте служб восстановления щелкаем “Создать расписание архивации”. На странице “Приступая к работе” в мастере планирования архивации нажимаем кнопку “Далее”. На странице “Выбор элементов для архивации” щелкаем “Добавить элементы” (см. Рисунок 23). Выбираем файлы и папки, которые нужно архивировать, и нажимаем кнопку “ОК”. Нажмите кнопку “Далее”. На странице “Задайте расписание архивации” указываем расписание резервного копирования и нажимаем кнопку “Далее”.



The screenshot shows the 'Master of scheduled backup' wizard. The current step is 'Select initial archive type'. The left sidebar contains a list of steps: 'Getting started', 'Select elements for arch...', 'Set backup schedule', 'Select backup policy', 'Select initial archive type' (highlighted), 'Confirmation', and 'Change backup progress...'. The main area has the title 'Select initial archive type' and a sub-header 'Specify the parameter used by the Azure Backup agent to create the initial archive.' There are two radio button options: 'Automatically over the network' (selected) and 'Autonomous backup'. Below the options are several input fields with labels and 'Обзор' (Preview) buttons: 'Intermediate storage location', 'Azure publication parameters', 'Azure import task name', 'Azure subscription identifier', 'Azure storage account', and 'Azure storage container'. At the bottom, there are navigation buttons: '< Назад', 'Далее >' (highlighted), 'Готово', and 'Отмена'.

Рисунок 23 – Интерфейс выбора типа начального архива

Технически можно запланировать ежедневную (не более трех раз в день) или еженедельную архивацию. Политика хранения определяет время, в течение которого должен храниться архив. Вместо настройки одной политики для всех точек архивации можно настроить разные политики хранения на основе времени



создания архива. Поддерживается выбор ежедневной, еженедельной, ежемесячной или ежегодной политики хранения.

На странице *“Выберите тип начального архива”* выберите тип начального архива, не снимая флажок *“Автоматически по сети”*, нажмите кнопку *“Далее”*. На странице *“Подтверждение”* проверяем параметры, которые мастер будет использовать для архивации данных на компьютере, затем нажимаем кнопку *“Архивировать”*. Можно нажать кнопку *“Закреть”*, чтобы закрыть Мастер. Если сделать это до завершения процесса архивации, мастер продолжит работу в фоновом режиме. После завершения начальной архивации в консоли службы архивации отобразится состояние *“Задание выполнено”*.

### **3.3 Контрольные вопросы**

1. Какие факторы способствуют использованию облачных хранилищ для архивирования данных?
2. С чем связаны основные возражения пользователей, опасющихся использовать облачные хранилища для архивирования данных?
3. Для чего используется файл MARSagentinstaller.exe?
4. Перечислите основные этапы процесса резервного копирования файлов и папок с помощью службы архивации Azure с использованием модели развертывания Resource Manager.
5. Что необходимо агенту служб восстановления Microsoft Azure для архивирования файлов в облако?
6. Перечислите этапы выполнения работы.
7. Какое средство виртуализации используете в ходе выполнения работы?
8. Какую информацию необходимо отразить в отчете о проделанной работе?

## **4 УТИЛИТА ROBOCOPY. АВТОМАТИЗАЦИЯ РЕЗЕРВНОГО КОПИРОВАНИЯ ФАЙЛОВ ПО СЕТИ И С ДИСКА НА ДИСК**

Утилита Robocopy (Robust File Copy for Windows) является программой командной строки, предназначена для автоматизированного копирования файлов и входит в состав ОС Windows Server 2012 R2, Windows Server 2012, Windows Server 2008 R2, Windows Server 2008 и Windows Server 2016. Для других версий ОС Windows утилита может быть загружена в виде отдельного файла. Программа предоставляет расширенные возможности, включающие копирование безопасности, резервное копирования API поддержки, возможность повторных попыток и ведения журнала. Более поздние версии поддерживают многопоточность и без буферизации ввода-вывода. Robocopy, например, может успешно использоваться системным администратором для копирования носителя восстановления на сервер. Для копирования файлов загрузки среды предустановки Windows в рабочие папки системный администратор может выдать команду вида:

```
robocopy "%ProgramFiles(x86)%\Windows Kits\8.1\Assessment and  
Deployment Kit\Windows Preinstallation Environment\amd64\Media"  
"C:\CustomizedImage" /E
```

Вышеприведенный пример рассмотрен в материале, опубликованном на официальном сайте Microsoft (рассматривается процесс настройки архивации клиента – Windows Server Essentials) [15].

Утилита Robocopy обычно используется в виде вызываемой утилиты командной строки в пакетных файлах, создаваемых системным администратором для решения повторяющихся задач системного обслуживания и администрирования. Следует особо отметить, что Robocopy – не просто утилита командной строки для копирования каталогов и/или папок, но и весьма эффективная утилита командной строки для репликации. Утилита стала доступна пользователям как часть Windows Resource Kit и была представлена как стандартный компонент в Windows Vista и Windows 7 [16].

### **4.1 Выполнение практической работы по теме (Лабораторная работа 3). Создание резервной копии средствами утилиты копирования Robocopy**

Для подготовки к выполнению лабораторной работы запустите две виртуальные машины, проверьте, что с первой машины (на ней проводятся

основные действия выполняемой лабораторной работы) доступен для чтения и записи сетевой ресурс (вторая виртуальная машина) `\\server2\backup`.

**Задание 1.** На первой виртуальной машине создать папку LOG1. По сценарию лабораторной работы в папку некое программное обеспечение в начале каждого часа записывает обновленные файлы протоколов работы с именами *log1.txt*, *log2.txt*, *log3.txt*. Разработать с задействованием утилиты Robocopy командный bat файл, позволяющий копировать файлы *log1.txt*, *log2.txt*, *log3.txt*. Файлы должны сохраняться в каталог LOG1 на сетевом ресурсе `\\server2\backup\LOG1`. Рассмотреть возможность запуска bat файла по расписанию с использованием планировщика задач. Файлы *log1.txt*, *log2.txt*, *log3.txt*, сохраняемые в каталог LOG1, должны перезаписывать файлы с одноименными названиями (файлы *log1.txt*, *log2.txt*, *log3.txt*), если файлы с такими именами уже есть на удаленном ресурсе.

**Задание 2.** На первой виртуальной машине создать папку LOG2. По сценарию лабораторной работы в папку LOG2 некое программное обеспечение в начале каждого часа записывает важные файлы, сгенерированные в процессе своей работы. Число файлов может быть различно, не известны и имена создаваемых файлов. Более того, в папке LOG2 программа может создавать вложенные папки с размещаемыми в них файлами.

Разработать с задействованием утилиты Robocopy командный bat файл, позволяющий копировать содержимое каталога LOG2 на сетевой ресурс `\\server2\backup\LOG2`. Одноименные файлы и папки, если такие уже есть на удаленном ресурсе в каталоге `\\server2\backup\LOG2`, должны быть перезаписаны.

**Задание 3.** Рассмотреть и описать в отчете возможности графической оболочки, используемой для настройки Robocopy.

## 4.2 Ход выполнения лабораторной работы

Рассмотрите приведенный ниже пример использования Robocopy в скрипте копирования, используя его в качестве образца и приведенную далее справочную информацию по утилите Robocopy, выполните Задания 1 и 2 лабораторной работы.

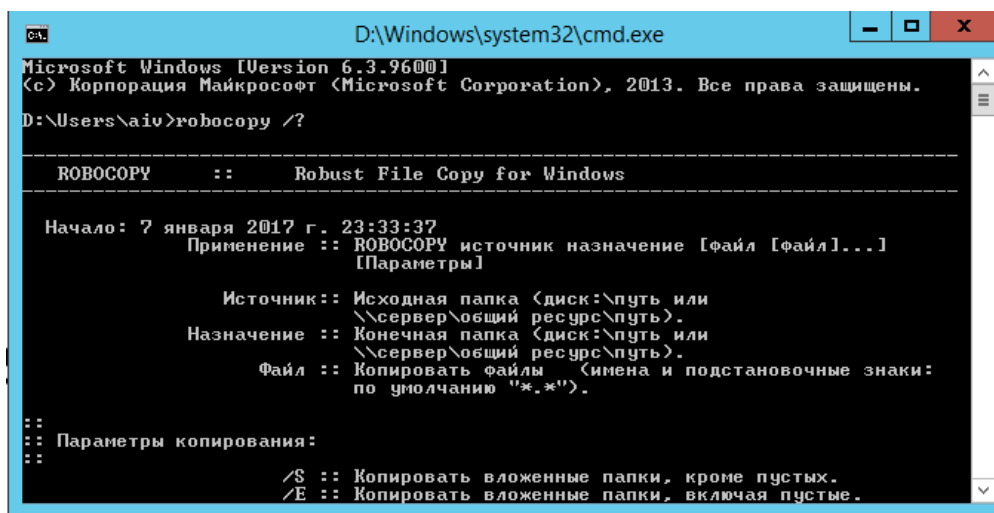
Пример использования ROBOCOPY в скрипте копирования [17]:

```
echo Start backup time: %DATE% %TIME% >> g:\BC\backup_time.txt
```

```
robocopy.exe S:\ g:\BC\MK\ /MIR /R:1 /W:1 /NP /TEE /LOG:g:\BC\00_sync.log
```

```
echo End backup time: %DATE% %TIME% >> g:\BC\backup_time.txt
```

Параметры утилиты ROBOCOPY (Robust File Copy for Windows) представлены ниже. Информацию о назначении ключей и параметров утилиты ROBOCOPY можно получить, запустив ее с ключом ROBOCOPY /? (см. Рисунок 24).



```
D:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.3.9600]
(c) Корпорация Майкрософт (Microsoft Corporation), 2013. Все права защищены.
D:\Users\aiu>robocopy /?

ROBOCOPY      ::      Robust File Copy for Windows

-----
Начало: 7 января 2017 г. 23:33:37
Применение  :: ROBOCOPY источник назначение [файл [файл]...]
               [Параметры]
Источник  :: Исходная папка <диск:\путь или
               \\\сервер\общий ресурс\путь>.
Назначение :: Конечная папка <диск:\путь или
               \\\сервер\общий ресурс\путь>.
Файл      :: Копировать файлы (имена и подстановочные знаки:
               по умолчанию "*.*").
::
:: Параметры копирования:
::
/S :: Копировать вложенные папки, кроме пустых.
/E :: Копировать вложенные папки, включая пустые.
```

Рисунок 24 – Вид вывода справки утилиты Robocopy с ключом /?

## Справочная информация

Применение Robocopy *источник назначение* [файл [файл]...] [Параметры]  
Источник – исходная папка (диск:\путь или \\\сервер\общий ресурс\путь).  
Назначение – конечная папка (диск:\путь или \\\сервер\общий ресурс\путь).  
Файл – копировать файлы (имена и подстановочные знаки: по умолчанию "\*.\*").  
Параметры копирования:  
/S – копировать вложенные папки, кроме пустых.  
/E – копировать вложенные папки, включая пустые.  
/LEV:n – копировать только верхние n уровней исходного дерева папок.  
/Z – копирование файлов с возобновлением.  
/B – копирование файлов в режиме архивирования.  
/ZB – используется режим с возобновлением; если доступ запрещен, используется режим архивации.

/J – копирование с использованием небуферизованного ввода-вывода (рекомендуется для больших файлов).

/EFSRAW – копирование всех зашифрованных файлов в режиме EFS RAW.

/COPY:флаги – копирования – что копируется для файлов (по умолчанию /COPY:DAT).

Флаги копирования: D=Данные, A=Атрибуты, T=Метки времени. S=Безопасность=NTFS ACLs, O=Сведения о владельце, U=Сведения аудита.

/SEC – копировать файлы с параметрами безопасности (эквивалентно /COPY:DATS).

/COPYALL – копировать все сведения о файле (эквивалентно /COPY:DATSOU).

/NOCOPY – не копировать никаких сведений о файле (полезно с параметром /PURGE).

/SECFIX – исправлять параметры безопасности для всех файлов, даже пропущенных.

/TIMFIX – исправлять атрибуты времени для всех файлов, даже пропущенных.

/PURGE – удалять файлы и папки назначения, которых больше не существует в источнике.

/MIR – создать зеркало дерева папок (эквивалентно /E с /PURGE).

/MOV – перемещать файлы (удаление из источника после копирования).

/MOVE – перемещать файлы и папки (удаление из источника после копирования).

/A+:[RASHCNET] – добавлять заданные атрибуты скопированным файлам.

/A-:[RASHCNET] – удалять заданные атрибуты из скопированных файлов.

/CREATE – создать только дерево папок и файлы нулевой длины.

/FAT – создать файлы назначения только в формате 8.3 FAT.

/256 – отключить поддержку длинных путей (> 256 знаков).

/MON:n – наблюдать за источником; перезапустить после n изменений.

/MOT:m – наблюдать за источником; перезапустить через m минут, если произошли изменения.

/RH:hhmm-hhmm – часы запуска - время, когда можно запускать новое копирование.

/PF – проверять часы запуска по файлам (не по проходам).

/IPG:n – интервал между пакетами (мс) для снижения нагрузки на сеть при низкоскоростных подключениях.

/SL – копирование самих символических ссылок вместо копирования целевого объекта этих ссылок.

/MT[:n] – выполнить многопоточное копирование с помощью n потоков (по умолчанию 8). n – должно быть не меньше 1 и не больше 128. Этот параметр несовместим с параметрами /IPG и /EFSRAW. Для повышения производительности перенаправьте вывод с помощью параметра /LOG.

/DCOPY:флаги копирования – что копировать для каталогов (по умолчанию /DCOPY:DA). Флаги копирования: D=Данные, A=Атрибуты, T=Метки времени.

/NODCOPY – не копировать никаких сведений о каталоге (по умолчанию выполняется /DCOPY:DA).

/NOOFFLOAD – копирование файлов без использования механизма разгрузки копий Windows.

Параметры выбора файлов:

/A – копировать только файлы с установленным атрибутом "Архивный".

/M – копировать только файлы с атрибутом "Архивный" и сбросить его.

/IA:[RASHCNETO] – включить файлы, у которых установлен какой-либо из заданных атрибутов.

/XA:[RASHCNETO] – исключить файлы, у которых установлен какой-либо из заданных атрибутов.

/XF file [файл]... – исключить файлы, соответствующие заданным именам, путям и подстановочным знакам.

/XD dirs [папки]... – исключить папки, соответствующие заданным именам и путям.

/XC – исключить измененные файлы.

/XN – исключить более поздние файлы.

/XO – исключить более ранние файлы.

/XX – исключить дополнительные файлы и папки.

/XL – исключить отдельно расположенные файлы и папки.

/IS – включить те же файлы.

/IT – включить оптимизированные файлы.

/MAX:n – максимальный размер файла – исключить файлы, размер которых более n байт.

/MIN:n – минимальный размер файла – исключить файлы, размер которых менее n байт.

/MAXAGE:n – максимальный возраст файла – исключить файлы, возраст которых превышает n дней.

/MINAGE:n – минимальный возраст файла – исключить файлы, возраст которых менее n дней.

/MAXLAD:n – наиболее поздняя дата последнего обращения – исключить файлы, которые не использовались с даты n.

/MINLAD:n – наиболее ранняя дата последнего обращения – исключить файлы, которые использовались после даты n. (Если n < 1900, то n = n дней, в противном случае n – дата в формате ДДММГГГГ).

/XJ – исключить точки соединения. (по умолчанию обычно включаются).

/FFT – использовать время файлов FAT (двухсекундная точность).

/DST – учитывать одночасовую разницу при переходе на летнее время.

/XJD – исключить точки соединения для папок.

/XJF – исключить точки соединения для файлов.

Параметры повторных попыток:

/R:n – число повторных попыток для неудавшихся копий: по умолчанию – 1 миллион.

/W:n – время ожидания между повторными попытками: по умолчанию – 30 секунд.

/REG – сохранить /R:n и /W:n в реестре как параметры по умолчанию.

/TBD – ждать, пока будут определены имена общих ресурсов (ошибка повторной попытки 67).

Параметры ведения журнала:

/L – только список - файлы не копируются, не удаляются, не помечаются метками времени.

/X – сообщать обо всех дополнительных файлах, а не только о выбранных.

/V – подробный вывод с указанием пропущенных файлов.

/TS – включать в вывод метки времени исходных файлов.

/FP – включать в вывод полные пути файлов.

/BYTES – печатать размеры в байтах.

/NS – без размера – не заносить в журнал размер файлов.

/NC – без класса – не заносить в журнал классы файлов.

/NFL – без списка файлов – не заносить в журнал имена файлов.

/NDL – без списка папок – не заносить в журнал имена папок.

/NP – без хода процесса – не отображать число скопированных процентов.

/ETA – показывать оценку времени окончания копирования файлов.

/LOG:файл – записывать состояние в файл журнала (перезаписывать существующий журнал).

/LOG+:файл – записывать состояние в файл журнала (добавлять к существующему журналу).

/UNILog:файл – записывать состояние в файл журнала в формате Юникод (перезаписывать существующий журнал).

/UNILog+:файл – записывать состояние в файл журнала в формате Юникод (добавлять к существующему журналу).

/TEE – направлять выходные данные в окно консоли и в файл журнала.

/NJH – без заголовка задания.

/NJS – без сведений о задании.

/UNICODE – состояние вывода в формате Юникод.

Параметры задания:

/JOB:имя\_задания – взять параметры из указанного файла задания.

/SAVE:имя\_задания – сохранить параметры в указанный файл задания.

/QUIT – выйти после обработки командной строки (для просмотра параметров).

/NOSD – не указывается исходная папка.

/NODD – не указывается папка назначения.

/IF – включить следующие файлы.

Использование /PURGE или /MIR для корневого каталога тома приведет к тому, что Robocopy применит запрошенную операцию и к файлам внутри каталога System Volume Information. Если это нежелательно, можно воспользоваться параметром /XD, чтобы команда robocopy пропустила данный каталог.

Рассмотрите простой пример копирования содержимого каталога C:\A в каталог C:\B (включая файлы, атрибуты и метки времени), рекурсивно включая пустые каталоги (/E):

```
robocopy C:\A C:\B /E
```

Копировать содержимое каталога C:\A рекурсивно (/E), включая все атрибуты файлов (/COPYALL, эквивалентно /COPY:DATSOU, D=данные, A=атрибуты, T=метки времени, S=безопасность=списки контроля доступа NTFS, O=владелец, U=аудит), не повторять попытки для заблокированных файлов (/R:0) (по умолчанию задан один миллион повторных попыток копирования), сохранять оригинальные метки времени у каталогов (/DCOPY:T — начиная с версии XP026 или более поздней):

```
robocopy C:\A C:\B /COPYALL /E /R:0 /DCOPY:T
```

Рассмотрите пример создания зеркальной копии каталога C:\A в каталоге B на сетевом ресурсе \\backupserver. По заданию необходимо удалить из каталога B все отсутствующие в каталоге C:\A файлы (/MIR), использовать журнал возобновления (/Z) на случай потери сетевого соединения:

```
robocopy C:\A \\backupserver\B /MIR /Z
```

Для успешного выполнения третьего задания лабораторной работы рассмотрим некоторые возможности графической программы-надстройки, позволяющей использовать Robocopy без работы с командной строкой. Для администраторов, использующих Robocopy, но привыкших к графическому интерфейсу, фирма Microsoft предлагает специальный графический пользовательский интерфейс Robocopy [18].

Разработку оболочки с графическим интерфейсом (дополнение к Robocopy) выполнил Дерк Бениш (Derk Benisch), системный инженер группы MSN Search компании Microsoft. Программа позволяет пользователям настраивать свои сценарии Robocopy с использованием простого и понятного графического интерфейса (см. Рисунок 25).



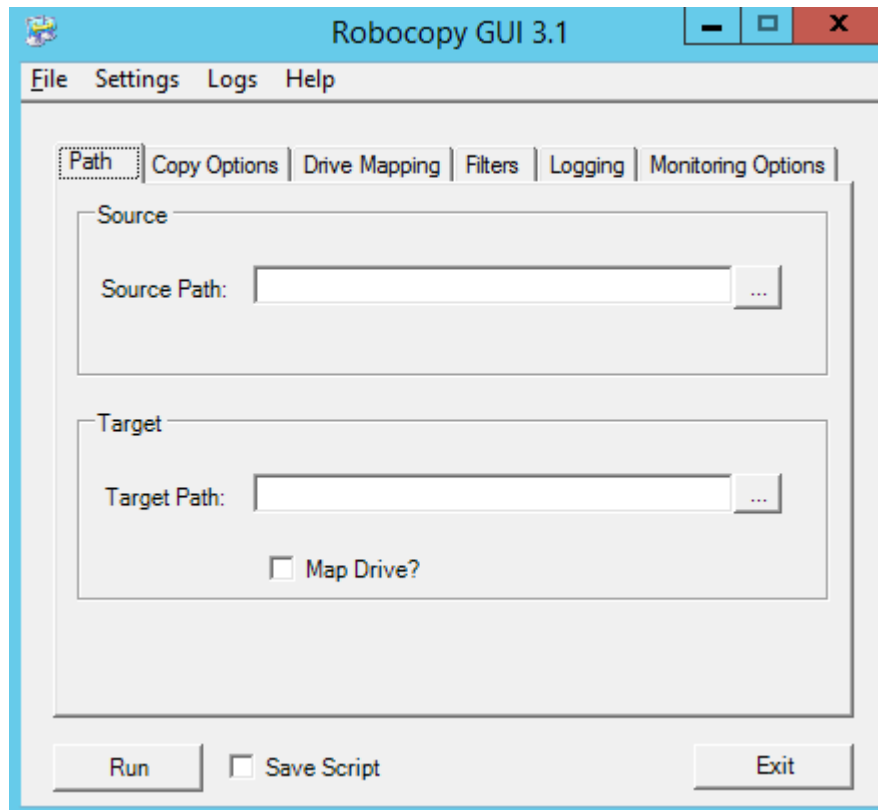


Рисунок 25 – Интерфейс Robocopy GUI 3.1

Графический интерфейс Robocopy, являясь многопоточным, эффективно расширяет возможности Robocopy, позволяя создавать сценарий Robocopy, выполнять его и начать создание другого сценария в процессе выполнения первого. Графический интерфейс Robocopy позволяет сохранять свои сценарии (даже без их фактического выполнения), что дает возможность системному администратору создать библиотеку стандартных сценариев, графический интерфейс Robocopy позволяет сохранять настройки по умолчанию с тем, чтобы не начинать каждый раз сеанс работы с программой с повторной установки данных настроек. Графический интерфейс Robocopy включает собственный файл справки, а также вложенную копию полного справочного руководства по Robocopy. Данный справочник содержит полный указатель всех команд и синтаксических структур Robocopy. Загрузить программу-надстройку с графическим интерфейсом для работы с Robocopy можно в разделе для загрузки программы на сайте Microsoft по приведенной ссылке [http://download.microsoft.com/download/f/d/0/fd05def7-68a1-4f71-8546-25c359cc0842/UtilitySpotlight2006\\_11.exe](http://download.microsoft.com/download/f/d/0/fd05def7-68a1-4f71-8546-25c359cc0842/UtilitySpotlight2006_11.exe).

### 4.3 Контрольные вопросы

1. Опишите назначение и основные возможности Robocopy.
2. Какие флаги копирования могут быть указаны в /DCOPY?
3. Опишите назначение и основные возможности Robocopy GUI.
4. Для чего предназначен параметр ведения журнала /X?
5. Для чего используется /EFSRAW?
6. Системный администратор ввел команду *robocopy C:\A C:\B /COPYALL /E /R:0 /DCOPY:T*, что произойдет в результате выполнения команды? Объясните назначение использованных ключей */COPYALL /E /R:0 /DCOPY:T*.
7. Системный администратор ввел команду *robocopy.exe S:\ g:\BC\MK\ /MIR /R:1 /W:1 /NP /TEE /LOG:g:\BC\00\_sync.log*, что произойдет в результате выполнения команды? Объясните назначение использованных ключей.
8. Перечислите этапы выполнения работы.
9. Какое средство виртуализации используете в ходе выполнения работы?
10. Какую информацию необходимо отразить в отчете о проделанной работе?

## **5 МИГРАЦИЯ ФИЗИЧЕСКОГО КОМПЬЮТЕРА В ВИРТУАЛЬНУЮ СРЕДУ С ПОМОЩЬЮ DISK2VHD**

В настоящее время системный администратор может сталкиваться не только с задачей, связанной с обеспечением создания по расписанию резервных копий, позволяющих в случае необходимости восстанавливать отдельные утраченные файлы или полностью восстанавливать операционную систему с прикладным программным обеспечением и файлы пользователей (что может быть актуальным если, например, вышел из строя физический диск сервера).

На предприятиях может работать достаточно много устаревающих компьютеров, требующих замены. Зачастую пользователи заменяемых компьютеров хотят, чтобы у них была возможность не только работать на новом оборудовании, но и оставалась возможность работы с программами заменяемого компьютера. В этом случае виртуализация физических дисков заменяемого компьютера, с последующим созданием на их основе виртуальной машины, может быть хорошим решением.

Виртуализация действующих серверов может потребоваться в случае, если планируется миграция в облако или необходимо создать виртуальные сервера для тестирования развертывания нового или апгрейда существующего программного обеспечения. Для виртуализации физических компьютеров (виртуализация типа P2V Physical-to-Virtual) могут использоваться программы различных производителей. Рассмотрим подробно работу с программой Disk2vhd.

### **5.1 Виртуализация компьютера с помощью Disk2VHD**

Disk2vhd (disk2vhd.exe) — бесплатная утилита Disk2vhd v2.0 предназначенная для конвертации физических дисков в виртуальные для платформы Microsoft Hyper-V. Утилита написана Марком Русиновичем и Брайсом Когсуэллом и доступна для загрузки по адресу <https://download.sysinternals.com/files/Disk2vhd.zip>.

Disk2vhd преобразует действующую физическую машину в виртуальный жесткий диск Virtual Hard Disk (VHD) в дисковом формате Microsoft Virtual Machine (VM). Disk2vhd можно запускать на устаревших операционных системах Windows XP SP2, Windows Server 2003 SP1 или более поздних версиях Windows,

включая 64-битные системы. Поддерживается формат использования утилиты в режиме командной строки:

*disk2vhd <[drive: [drive:]...][[\*]> <vhdfile>*

Например, *disk2vhd \* c:\vhd\snapshot.vhd*

Обратите внимание, что Disk2vhd позволяет сделать копию дисков работающей системы (виртуализацию диска или дисков) и записать ее на локальный диск в виде файла формата vhd или нового vhdx. Программа Disk2vhd не требует процедуры установки, в процессе работы ничего не записывает в системный реестр. Для того, чтобы программа Disk2vhd могла корректно создать образ диска, с которым работает операционная система и под управлением которой исполняется Disk2vhd, программа Disk2vhd должна быть запущена на выполнение с правами учетной записи системного администратора.

## **5.2 Выполнение практической работы по теме (Лабораторная работа 4).**

### **Создание виртуализированной копии физического компьютера в виртуальной среде с помощью Disk2VHD**

**Задание:** выполнить виртуализацию физического компьютера, используя программу Disk2vhd.

Согласно заданию лабораторной работы, необходимо виртуализировать только те разделы физического жесткого диска, которые используются для загрузки операционной системы. Например, виртуализируется физическая машина, на которой имеется один жесткий диск, разбитый на несколько разделов – виртуализируем только диск с операционной системой (пользователь видит три логических диска **C:**, **D:**, **F:**, операционная система установлена на диске **C:** – значит, следует виртуализировать только диск **C:** без диска **D:** и **F:**) и раздел, необходимый для загрузки операционной системы (как правило, он является скрытым – ему не присвоена буква).

Операционная система для виртуализации выбирается в соответствии с указаниями преподавателя. После того, как создан vhd диск, следует создать (используя Hyper-V) виртуальную машину, использующую этот диск. Проверить загрузку виртуализированной операционной системы.

### 5.3 Ход выполнения лабораторной работы

В ОС Windows физической машины, которая будет виртуализироваться, записываем программу Disk2vhd, разместив ее в отдельную папку. Запускаем программу Disk2vhd на выполнение из-под учетной записи, имеющей права системного администратора. После запуска программы (см. Рисунок 26) следует указать виртуализируемые разделы, проверить, что создается диск формата vhd (не установлен флажок Use Vhdx), проверить, на каком носителе будет создаваться виртуальный диск (обратите внимание, что если виртуализируется раздел C:, то указывать, что на нем будет создан виртуальный диск, нельзя). Так как выполняется виртуализация работающей операционной системы, то обязательно должен быть установлен флажок, разрешающий программе опцию теневого копирования (Use Volume Shadow Copy). После выбора и установки всех необходимых опций следует нажать кнопку *Create*. Контролируйте процесс создания виртуального жесткого диска (Индикатор Snapshotting volumes...), в отчете по лабораторной работе отметьте время, затраченное на создание виртуального жесткого диска. Утилита Disk2vhd создает один VHD-файл для каждого диска, на котором находятся выбранные пользователем тома. Disk2vhd сохраняет информацию о разделах диска, но копирует только данные, относящиеся к выбранному тому. Такая технология позволяет, например, включать в VHD-файл только системный том и исключать разделы с данными. Отметим, что если виртуализируется компьютер, на котором пользователь видит три логических диска C:, D:, F:, но указано виртуализировать только диск C:, то при загрузке виртуализированной операционной системы пользователь увидит в проводнике три логических диска C:, D:, F:, но при попытке обратиться к D: и F: получит сообщение, что данные носители не читаются, и предложение их отформатировать.

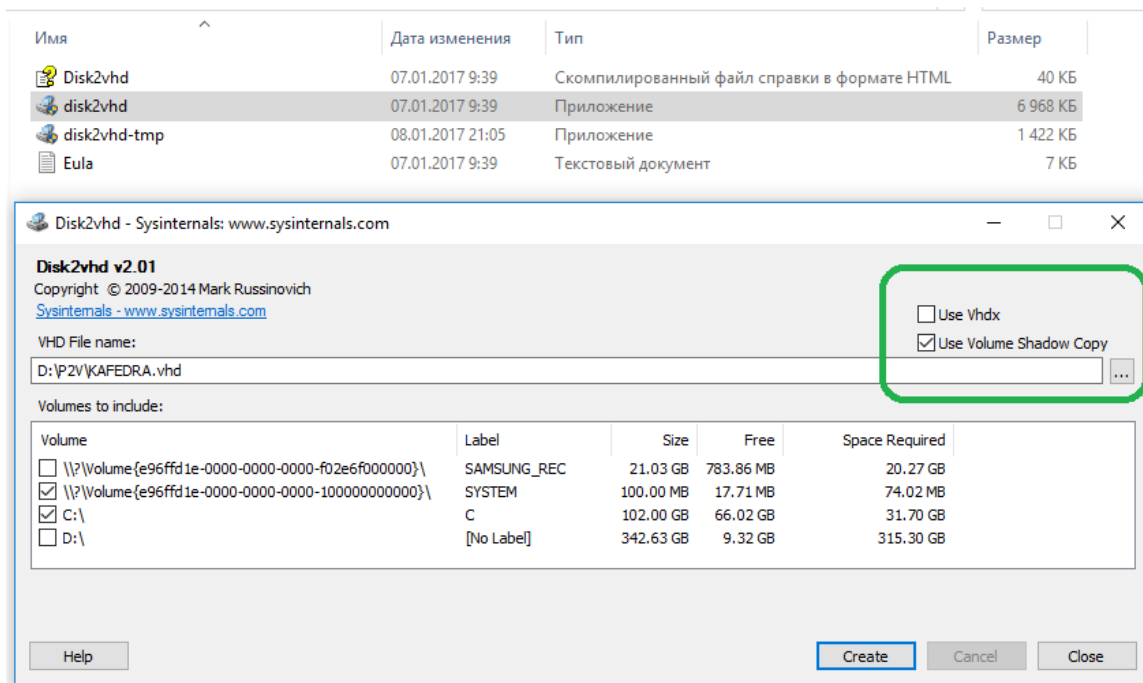


Рисунок 26 – Интерфейс программы Disk2vhd

После создания виртуального жесткого диска следует запомнить место расположения файла и загрузиться под другой загрузочной записью (обычно в лабораторных классах на одном физическом компьютере установлено несколько операционных систем) с операционной системой Windows Server. Используя консоль управления Hyper-V, следует создать новую виртуальную машину, указав, что в качестве виртуального жесткого диска следует использовать диск, созданный на предыдущем этапе выполнения лабораторной работы с помощью программы Disk2vhd.

## 5.4 Контрольные вопросы

1. Назначение программы Disk2vhd, особенности работы с программой.
2. Что такое виртуализация типа P2V? Для чего она используется?
3. Назовите этапы создания виртуальной машины, используя консоль управления Hyper-V.
4. Какие данные программа Disk2vhd записывает в системный реестр в процессе установки?
5. Перечислите этапы выполнения работы. Какое средство виртуализации используете в ходе выполнения работы? Какую информацию необходимо отразить в отчете о проделанной работе?

## Заключение

В пособии рассмотрено несколько достаточно часто используемых подходов к созданию резервных копий данных в процессе работы пользователей с ОС Windows. Отмечено, что при выборе оптимального средства резервного копирования и восстановления данных следует учитывать ряд факторов. Во-первых, следует обратить внимание, работают ли в процессе создания архивной копии с копируемыми данным какие-либо программы, в том числе в режиме монопольного использования (в этом случае выбираемое средство создания архивных копий должно поддерживать режим теневого копирования). Во-вторых, следует учитывать, сколько времени можно выделить на выполнение операции копирования. Если промежуток времени (“окно копирования”), за который необходимо создать архивную копию, небольшой, то можно увеличить скорость резервного копирования, отказавшись от режима сжатия архивируемых данных, однако это приведет к увеличению размера создаваемого архива. В случае, если не удастся создать резервную копию штатными средствами ОС Windows за ограниченный временной интервал, за который должна быть создана архивная копия данных, следует рассмотреть выбор альтернативных программных и программно-аппаратных решений, используемых для этой цели, от других производителей.

Выбирая средства резервного копирования и восстановления данных, следует учитывать требуемый уровень автоматизации процесса создания и восстановления – от частичного до полной автоматизации. Разработчики ПО для создания архивных копий предлагают решения, позволяющие создавать и успешно реализовывать гибкие сценарии резервного копирования и восстановления данных. Поддерживаются режимы оперативного информирования системных администраторов с использованием электронной почты, sms-информирования, мессенджеров, push уведомлений на мобильные устройства и т.д.

При выборе средств резервного копирования следует учитывать не только то, насколько быстро можно создать резервную копию и какой может быть максимальный коэффициент сжатия архивируемых данных, но и насколько быстро и просто можно выполнить обратный процесс восстановления данных из резервной копии.

В пособии рассмотрены примеры использования программ резервного копирования и восстановления файлов для ОС Windows и выполняющихся под ее управлением приложений. Учитывая, что современные программные решения часто являются много платформенными, отмечено, что для данных и файлов,

обрабатываемых в других операционных системах, используются аналогичные подходы и решения. Например, для создания архивных копий в ОС класса Linux можно использовать такие программы как, Rsync, Fwbackups, Bacula, Backupninja, Simple Backup Suite (sbackup), Kbackup, BackupPC (может работать в Unix/Linux, Windows и Mac OS X), Amanda (работает в Unix/GNU Linux и Windows) и другие. Некоторые решения распространяются свободно с открытым программным кодом. Для устройств, работающих с ОС Android, могут, например, использоваться такие программы, как Titanium Backup, Super Backup, Helium — App Sync and Backup, G Cloud Backup, SMS Backup & Restore, Autosync и другие.

В завершении отмечено, что операции резервного копирования и восстановления данных, несмотря на их важность для обеспечения безопасности данных, сами по себе не могут выступать гарантией обеспечения безопасности данных, с которыми работает пользователь. Например, средства резервного копирования данных не обеспечивают защиту данных от несанкционированного доступа. Обеспечение безопасности данных пользователей должно быть комплексным решением, включающим в себя, кроме использования эффективных средств резервного копирования и восстановления данных, средства обеспечения отказоустойчивости (кластерные решения, RAID-массивы и т.д.), средства защиты от несанкционированного доступа и т.д.



## Литература

1. Kaspersky Internet Security 2019. Лаборатория Касперского. [Электронный ресурс]. URL: <http://www.kaspersky.ru/multi-device-security> (дата обращения: 15.07.2019).
2. Dr.Web Enterprise Security Suite. [Электронный ресурс]. URL: [http://products.drweb.com/enterprise\\_security\\_suite/](http://products.drweb.com/enterprise_security_suite/) (дата обращения: 15.07.2019).
3. Ананченко И.В., Active Directory – архитектура, планирование развертывания и внедрение. – СПб: Университет ИТМО, 2015. – 58 с.
4. Станек У.Р. Microsoft Windows 8.1. Справочник администратора. СПб.: БХВ-Петербург, 2015. – 400 с.
5. Станек У.Р. Microsoft Windows Server 2012 R2. Хранение, безопасность, сетевые компоненты. Справочник администратора СПб.: БХВ-Петербург, 2015. – 416 с.
6. Колисниченко Д.Н. Microsoft Windows 10. Первое знакомство. СПб.: БХВ-Петербург, 2015. – 160 с.
7. Иванов Н.А. Средства резервного копирования и восстановления данных в операционных системах Windows и Linux. Методические указания. Издательство МГСУ, 2015. – 40 с.
8. Леонтьев В.П. Windows 10. Новейший самоучитель. Издательство Эксмо, 2015. – 528 с.
9. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. Учебник. Издательство Питер, 2015. – 992 с.
10. Соболев Б.В., Доманин А.А., Герасименко М.С. Сети и телекоммуникации. Учебное пособие. Издательство Феникс, 2015. – 192 с.
11. Резервное копирование и восстановление системы компьютера. [Электронный ресурс]. URL: <https://support.microsoft.com/ru-ru/help/17127/windows-back-up-restore> (дата обращения: 15.07.2019).
12. Служба Azure Backup. [Электронный ресурс]. URL: <https://azure.microsoft.com/ru-ru/services/backup/> (дата обращения: 15.07.2019).
13. Резервное копирование компьютеров Windows с агентом Azure Backup MARS. [Электронный ресурс]. URL: <https://docs.microsoft.com/ru-ru/azure/backup/backup-configure-vault> (дата обращения: 15.07.2019).
14. Создайте бесплатную учетную запись Azure уже сегодня. Microsoft Azure. [Электронный ресурс]. URL: <https://azure.microsoft.com/ru-ru/free/>
15. Customize Client Backup - Windows Server Essentials. [Электронный ресурс]. URL: [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-8.1-and-8/dn236868\(v=win.10\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-8.1-and-8/dn236868(v=win.10)) (дата обращения: 15.07.2019).

16. Robosory — Википедия. [Электронный ресурс]. URL: <http://ru.wikipedia.org/wiki/Robosory> (дата обращения: 15.07.2019).
17. Используем Robosory. Примеры. [Электронный ресурс]. URL: <https://vladimirmalikov.com/используем-robosory-примеры/> (дата обращения: 15.07.2019).
18. Графический интерфейс Robosory. [Электронный ресурс]. URL: [https://docs.microsoft.com/ru-ru/previous-versions/technet-magazine/cc160891\(v=msdn.10\)](https://docs.microsoft.com/ru-ru/previous-versions/technet-magazine/cc160891(v=msdn.10)) (дата обращения: 15.07.2019).

Ананченко Игорь Викторович  
Зудилова Татьяна Викторовна  
Хоружников Сергей Эдуардович

Средства резервного копирования, восстановления, защиты данных в  
операционных системах Windows  
учебно-методическое пособие

В авторской редакции  
Редакционно-издательский отдел Университета ИТМО  
Зав. РИО Н. Ф. Гусарова  
Подписано к печати  
Заказ №  
Отпечатано на ризографе

**Редакционно-издательский отдел**  
**Университета ИТМО**  
197101, Санкт-Петербург, Кронверский пр., 49