



МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ  
ФГБОУ ВО БРЯНСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ

Институт энергетики и природопользования  
Кафедра информатики, информационных систем и технологий

**В.В. НИКУЛИН**  
**БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ**  
**Лабораторный практикум**



Учебно-методическое пособие для студентов направления подготовки  
09.04.03 «Прикладная информатика»

Брянская область,  
2021

УДК 004.056.5 (076)

ББК 32.97

Н 65

Никулин, В. В. Безопасность и защита информации. Лабораторный практикум: учебно-методическое пособие для студентов направления подготовки 09.04.03 Прикладная информатика / В. В. Никулин. – Брянск: Изд-во Брянский ГАУ, 2021. – 128 с.

Учебно-методическое пособие адресовано магистрам, обучающимся по направлению подготовки 09.04.03 «Прикладная информатика» изучающих дисциплину «Безопасность и защита информации», а также может быть использовано специалистами в области проектирования и организации систем информационной безопасности организаций.

Рецензенты:

к.т.н., доцент  
кафедры технического  
сервиса Брянского ГАУ

С.А. Феськов

Рекомендовано методической комиссией института энергетики и природопользования от 30.08.2021, протокол № 1

© Брянский ГАУ, 2021

© В.В. Никулин 2021

	Содержание	Стр
	Введение	4
<b>Раздел 1.</b>	<b>Информационная безопасность и защита информации</b>	<b>5</b>
	<i>Лабораторная работа 1. Анализ источников, каналов распространения и каналов утечки информации</i>	5
	<i>Лабораторная работа 2. Проведение анализа информации на предмет целостности</i>	13
	<i>Лабораторная работа 3. Оценка уязвимости информации</i>	15
<b>Раздел 2.</b>	<b>Уровни обеспечения информационной безопасности</b>	<b>23</b>
	<i>Лабораторная работа 1. Требования к безопасности информационных систем.</i>	22
	<i>Лабораторная работа 2. Требования к безопасности информационных систем в России.</i>	28
	<i>Лабораторная работа 3. Оценка состояния безопасности ИС США.</i>	31
	<i>Лабораторная работа 4. Определение классов защищенности средств вычислительной техники от несанкционированного доступа (НСД).</i>	35
	<i>Лабораторная работа 5. Определение требований к защите информации</i>	36
<b>Раздел 3.</b>	<b>Криптографическая защита информации</b>	<b>38</b>
	<i>Лабораторная работа 1. Анализ терминов и определений информационной безопасности</i>	38
	<i>Лабораторная работа 2. Работа с ГОСТами в области информационной безопасности</i>	39
	<i>Лабораторная работа № 3. Шифрование данных при хранении - EFS.</i>	40
<b>Раздел 4.</b>	<b>Вредоносные программы</b>	<b>54</b>
	<i>Лабораторная работа 1. Безопасность Windows и Windows Defender</i>	55
	<i>Лабораторная работа 2. Установка и предварительная настройка Антивируса Касперского</i>	73
	<i>Лабораторная работа 3. Профилактика проникновения вредоносного программного обеспечения</i>	90
<b>Раздел 5.</b>	<b>Информационная безопасность в глобальных сетях</b>	<b>99</b>
	<i>Лабораторная работа 1 Администрирование Windows 10</i>	99
	<i>Лабораторная работа 2. Резервное копирование в системе Windows Server 2012 R2</i>	117
	<i>Список литературы</i>	126

## Введение

Курс с названием «Информационная безопасность» (Information Security) входит в целый ряд государственных образовательных стандартов по различным специальностям, например: 090102 – «Компьютерная безопасность», 090105 – «Комплексное обеспечение информационной безопасности автоматизированных систем», 09.03.03; – «Информационная безопасность» 09.04.03 «Безопасность и защита информации» и других.

Тематика курса разрабатывается многими авторами, ими к настоящему времени подготовлено достаточно много книг, в том числе и учебных пособий. Обилие этих книг говорит об огромной величине рассматриваемой области, ее постоянном изменении и увеличении.

Актуальность тематики обеспечена высокой динамикой развития информационных технологий и большой зависимостью их от обеспечения информационной безопасности.

В качестве основы для курса были выбраны следующие книги.

Малюк А.А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах. – М.: Горячая линия – Телеком, 2001. – 148 с.

Галатенко В.А. Основы информационной безопасности: Курс лекций. – М.: ИНТУИТ. РУ, 2006. – 205 с.

Тихонов В.А., Райх В.В. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты: Учебное пособие. – М.: Гелиос АРВ, 2006. – 528 с.

Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие. – М.: ИД «ФОРУМ»: ИНФРА-М, 2008. – 416 с. 5

Все книги написаны известными специалистами в области информационной безопасности и во многом основаны на передовом зарубежном и отечественном опыте. Однако даже за прошедшее время с момента выхода книг произошли существенные изменения в данной области, например, вышли новые стандарты и рекомендации по вопросам информационной безопасности и новым технологиям, приняты новые законы и другие акты. В связи с этим должно быть переработано и дополнено содержание всех этих книг и курса на их основе. По-видимому, в последующем также надо будет учесть и процесс гармонизации международных и отечественных стандартов, особенности новых.

## **Раздел 1. Информационная безопасность и защита информации**

### ***Лабораторная работа 1. Анализ источников, каналов распространения и каналов утечки информации***

**Цель работы:** формирование навыка работы с нормативными документами по исследуемому вопросу; анализ угроз информационной безопасности

**Время выполнения:** 2 часа

**Оборудование:** учебный персональный компьютер.

#### **Теоретические основы**

Понятие «информационная безопасность» (ИБ) рассматривается как состояние защищенности потребностей личности, общества и государства в информации, при котором обеспечиваются их существование и прогрессивное развитие независимо от наличия внутренних и внешних информационных угроз.

Тогда с позиции обеспечения ИБ можно определить, что под информационной угрозой понимается воздействие дестабилизирующих факторов на состояние информированности, подвергающее опасности жизненно важные интересы личности, общества и государства.

В законе РФ «О безопасности» дано определение угрозы безопасности как совокупности условий, факторов, создающих опасность жизненно важным интересам личности, общества и государства.

Под угрозой информации в системах ее обработки понимается возможность возникновения на каком-либо этапе жизнедеятельности системы такого явления или события, следствием которого могут быть нежелательные воздействия на информацию.

К настоящему времени известно большое количество разноплановых угроз различного происхождения, таящих в себе различную опасность для информации.

Для системного представления их удобно классифицировать по виду, возможным источникам, предпосылкам появления и характеру проявления.

### ***Виды угроз***

Определив понятие «угроза государству, обществу и личности» в широком смысле, рассмотрим его относительно не посредственного воздействия на конфиденциальную информацию, обрабатываемую на каком-либо объекте (кабине те, предприятии, фирме). Анализируя возможные пути воздействия на информацию, представляемую как совокупность информационных элементов, связанных между собой логическими связями (рис. 1), можно выделить основные нарушения:

- физической целостности (уничтожение, разрушение элементов);
- логической целостности (разрушение логических связей);
- содержания (изменение блоков информации, внешнее навязывание ложной информации);
- конфиденциальности (разрушение защиты, уменьшение степени защищенности информации), — прав собственности на информацию (несанкционированное копирование, использование).

С учетом этого для таких объектов систем угроза информационной безопасности представляет реальные или потенциально возможные действия или условия, приводящие к овладению конфиденциальной информацией, хищению, искажению, изменению, уничтожению ее и сведений о самой системе, а также к прямым материальным убыткам.

Обобщая рассмотренные угрозы, можно выделить три наиболее выраженные для систем обработки информации:

- 1) подверженность физическому искажению или уничтожению;
- 2) возможность несанкционированной (случайной или злоумышленной) модификации;

3) опасность несанкционированного (случайного или преднамеренного) получения информации лицами, для которых она не предназначалась.

Кроме того, с точки зрения анализа процесса обработки информации выделяют такую угрозу, как блокирование доступа к обрабатываемой информации.

Угрозы безопасности информации в современных системах ее обработки определяются умышленными (преднамеренные угрозы) и естественными (непреднамеренные угрозы) разрушающими и искажающими воздействиями внешней среды, надежностью функционирования средств обработки информации, а также преднамеренным корыстным воздействием несанкционированных пользователей, целями которых являются хищение, уничтожение, разрушение, несанкционированная модификация и использование обрабатываемой информации. При этом под умышленными, или преднамеренными, понимаются такие угрозы, которые обуславливаются злоумышленными действиями людей. Случайными, или естественными, являются угрозы, не зависящие от воли людей. В настоящее время принята следующая классификация угроз сохранности (целостности)



Рисунок 1 – Угрозы сохранности информации

Под источником угроз понимается непосредственный исполнитель угрозы с точки зрения ее негативного воздействия на информацию.

Источники можно разделить на следующие группы:

- люди;
- технические устройства;
- модели, алгоритмы, программы;
- технологические схемы обработки;
- внешняя среда

### **Предпосылки появления угроз**

Существуют следующие предпосылки, или причины, появления угроз:

— объективные (количественная или качественная недостаточность элементов системы) — не связанные непосредственно с деятельностью людей и вызывающие случайные по характеру происхождения угрозы;

— субъективные — непосредственно связанные с деятельностью человека и вызывающие как преднамеренные (деятельность разведок иностранных государств, промышленный шпионаж, деятельность уголовных элементов и недобросовестных сотрудников), так и непреднамеренные (плохое психофизиологическое состояние, недостаточная подготовка, низкий уровень знаний) угрозы информации.

Перечисленные разновидности предпосылок интерпретируются следующим образом:

— количественная недостаточность — физическая не хватка одного или нескольких элементов системы обработки, вызывающая нарушения технологического процесса обработки или перегрузку имеющихся элементов;

— качественная недостаточность — несовершенство конструкции (организации) элементов системы, в силу чего может появляться возможность случайного или преднамеренного негативного воздействия на обрабатываемую или хранимую информацию;

— деятельность разведорганов иностранных государств — специально организуемая деятельность государственных органов разведки, профессио-



нально ориентированных на добывание необходимой информации всеми доступными способами и средствами;

— промышленный шпионаж: — негласная деятельность отечественных и зарубежных промышленных организаций (фирм), направленная на получение незаконным путем конфиденциальной информации, используемой для достижения промышленных, коммерческих, политических или подрывных целей;

— злоумышленные действия уголовных элементов — хищение информации, средств ее обработки или компьютерных программ в целях наживы или их разрушение в интересах конкурентов;

— плохое психофизиологическое состояние — постоянное или временное психофизиологическое состояние сотрудников, приводящее при определенных нестандартных внешних воздействиях к увеличению ошибок и сбоев в обслуживании систем обработки информации или непосредственно к разглашению конфиденциальной информации;

— недостаточная качественная подготовка сотрудников — уровень теоретической и практической подготовки персонала к выполнению задач по защите информации, недостаточная степень которого может привести к нарушению процесса функционирования системы защиты информации.

В современной литературе и нормативно-правовых актах в области информационной безопасности можно встретить такую классификацию угроз информации, которая делит их на внутренние и внешние. Одной из наиболее принципиальных особенностей проблемы защиты информации является формирование полного множества угроз информации, потенциально возможных на объекте ее обработки. В самом деле, даже одна неучтенная угроза может в значительной мере снизить эффективность защиты.

#### Возможные пути получения конфиденциальной информации

Анализ рассмотренных видов угроз позволяет сгруппировать их по двум основным областям:

- 1) угрозы нарушения физической и логической целостности, а также содержания информации (несанкционированная модификация). Их можно

объединить в причины нарушения целостности информации (ПНЦИ);

2) угрозы, следствием которых может быть получение защищаемой информации (хищение или копирование) лицами, не имеющими на это полномочий, — в каналы несанкционированного получения информации (КНПИ).

Под действием рассмотренных выше угроз может произойти утечка защищаемой информации, то есть несанкционированное, неправомерное завладение соперником данной информацией и возможность использования ее в своих, в ущерб интересам собственника (владельца) информации, целях. При этом образуется канал утечки информации, под которым понимается физический путь от источника конфиденциальной информации к злоумышленнику. Для его возникновения необходимы определенные пространственные, энергетические и временные условия, а также соответствующие средства восприятия и фиксации информации на стороне злоумышленника.

В зависимости от используемых соперником сил и средств для получения несанкционированного доступа к носителям защищаемой информации различают каналы агентурные, технические, легальные.

**Агентурные каналы утечки информации** — это использование противником тайных агентов для получения несанкционированного доступа к носителям защищаемой информации. В случае использования агентами технических средств разведки (направленные микрофоны, закладных устройств, миниатюрных видеокамер и др.) говорят о ведении агентурно-технической разведки.

**Технические каналы утечки информации** — совокупность технических средств разведки, демаскирующих признаков объекта защиты и сигналов, несущих информацию об этих признаках. Эти каналы образуются без участия человека в процессе обработки информации техническими средствами, а поэтому являются одними из наиболее опасных и требуют отдельного рассмотрения.

**Легальные каналы утечки информации** — это использование соперником открытых источников информации (литературы, периодических изданий и т. п.), обратный инжиниринг, выведывание под благовидным предлогом инфор-

мации у лиц, располагающих интересующей соперника информацией, и других возможностей. В основу классификации ПНЦИ положен показатель, характеризующий степень участия в этом процессе человека. В соответствии с таким подходом ПНЦИ делятся на два вида (объективные и субъективные) и на следующие классы (рис. 2).



Рисунок 2. - Классификация ПНЦИ

### *1.1. Субъективные преднамеренные.*

1.1.1. Диверсия (организация пожаров, взрывов, повреждение электропитания и др.).

1.1.2. Непосредственные действия над носителем (хищение, подмена носителей, уничтожение информации).

1.1.3. Информационное воздействие (электромагнитное облучение, ввод в компьютерные системы разрушающих программных средств, воздействие на психику личности психотропным оружием).

### *1.2. Субъективные непреднамеренные.*

1.2.1. Отказы обслуживающего персонала (гибель, длительный выход из строя).

1.2.2. Сбои людей (временный выход из строя).

1.2.3. Ошибки людей.

### *2.1. Объективные непреднамеренные.*

2.1.1. Отказы (полный выход из строя) аппаратуры, программ, систем питания и жизнеобеспечения.

2.1.2. Сбои (кратковременный выход из строя) аппаратуры, программ, си-

стем питания и жизнеобеспечения.

2.1.3. Стихийные бедствия (наводнения, землетрясения, ураганы).

2.1.4. Несчастные случаи (пожары, взрывы, аварии).

2.1.5. Электромагнитная несовместимость.

Для предотвращения возможной утечки конфиденциальной информации и нарушения ее целостности на объектах ее обработки разрабатывается и внедряется система защиты информации. Система защиты информации — совокупность взаимосвязанных средств, методов и мероприятий, направленных на предотвращение уничтожения, искажения, несанкционированного получения конфиденциальных сведений, отображенных физическими полями, электромагнитными, световыми и звуковыми волнами или вещественно-материальными носителями в виде сигналов, образов, символов, технических решений и процессов.

### **Задание**

Необходимо провести анализ защищенности объекта защиты информации по следующим разделам:

1. Виды возможных угроз
2. Характер происхождения угроз
3. Классы каналов несанкционированного получения информации
4. Источники появления угроз
5. Причины нарушения целостности информации
6. Потенциально возможные злоумышленные действия
7. Определить класс защищенности автоматизированной системы

### **Отчет**

Отчет должен содержать:

1. наименование работы;
2. цель работы;
3. задание;
4. последовательность выполнения работы;
5. ответы на контрольные вопросы;
6. вывод о проделанной работе.

### **Контрольные вопросы**

1. Что такое информационный риск?
2. В чем заключается задача управления информационными рисками?
3. Какие существуют методики оценки рисков и управления ими?
4. Какие формулы используются при количественной оценке информационных рисков?

## *Лабораторная работа 2. Проведение анализа информации на предмет целостности*

**Цель работы:** изучить понятие целостности информации, проанализировать риски информационной безопасности.

**Оборудование:** учебный персональный компьютер.

### **Теоретические основы**

Целостность информации условно подразделяется на статическую и динамическую.

**Статическая** целостность информации предполагает неизменность информационных объектов от их исходного состояния, определяемого автором или источником информации.

**Динамическая** целостность информации включает вопросы корректного выполнения сложных действий с информационными потоками, например, анализ потока сообщений для выявления некорректных, контроль правильности передачи сообщений, подтверждение отдельных сообщений и др.

Целостность является важнейшим аспектом информационной безопасности в тех случаях, когда информация используется для управления различными процессами, например, техническими, социальными и т. д.

Так, ошибка в управляющей программе приведет к остановке управляемой системы, неправильная трактовка закона может привести к его нарушениям, точно также неточный перевод инструкции по применению лекарственного препарата может нанести вред здоровью. Все эти примеры иллюстрируют нарушение целостности информации, что может привести к катастрофическим последствиям. Именно поэтому целостность информации выделяется в качестве одной из базовых составляющих информационной безопасности.

**Целостность**— гарантия того, что информация сейчас существует в ее исходном виде, то есть при ее хранении или передаче не было произведено несанкционированных изменений.

Действия, направленные на нарушение целостности информации, подразделяются на субъективные преднамеренные и объективные преднамеренные.

### ***Субъективные преднамеренные:***

- диверсия (организация пожаров, взрывов, повреждений электропитания и др.);
- непосредственные действия над носителем (хищение, подмена носителей, уничтожение информации);
- информационное воздействие (электромагнитное облучение, ввод в компьютерные системы разрушающих программных средств, воздействие на психику личности психотропным оружием).

### ***Объективные непреднамеренные:***

- отказы (полный выход из строя) аппаратуры, программ, систем питания и жизнеобеспечения;
- сбои (кратковременный выход из строя) аппаратуры, программ, систем питания и жизнеобеспечения;
- стихийные бедствия (наводнения, землетрясения, ураганы); - несчастные случаи (пожары, взрывы, аварии); - электромагнитная несовместимость.

### **Практическое задание**

Составьте таблицу, содержащую причины нарушения целостности информации и мер предосторожности, применяемых для защиты информации от потери целостности.

### **Отчет**

Отчет должен содержать:

1. наименование работы;
2. цель работы;
3. задание;
4. последовательность выполнения работы;
5. ответы на контрольные вопросы;
6. вывод о проделанной работе.

### **Контрольные вопросы**

1. Что такое целостность информации?
2. Какие меры можно предпринять для защиты информации?

### Лабораторная работа 3. Оценка уязвимости информации

**Цель работы:** Ознакомиться с алгоритмами оценки уязвимости информационной безопасности.

**Оборудование:** учебный персональный компьютер.

#### Теоретические основы

Уязвимость информации есть событие, возникающее как результат такого стечения обстоятельств, когда в силу каких-то причин используемые в автоматизированных системах обработки данных средства защиты не в состоянии оказать достаточного противодействия проявлению дестабилизирующих факторов и нежелательного их воздействия на защищаемую информацию. Модель уязвимости информации в автоматизированных системах обработки данных в общем виде показано (рис.1).

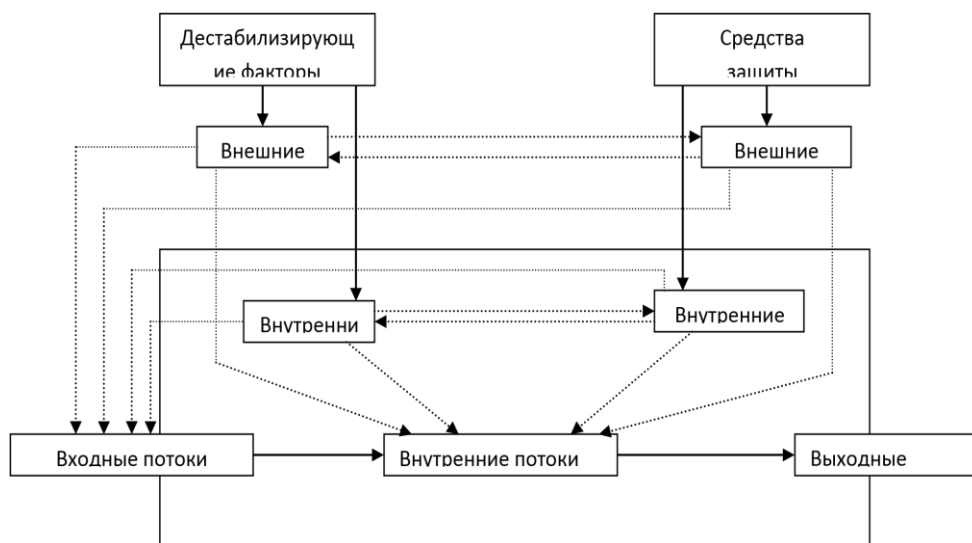


Рисунок 1 - Модель уязвимости информации в автоматизированных системах обработки данных

Данная детализируется при изучении конкретных видов уязвимости информации: нарушения физической или логической целостности, несанкционированной модификации, несанкционированного получения, несанкционированного размножения.

При детализации общей модели основное внимание акцентируется на том, что подавляющее большинство нарушений физической целостности ин-

формации имеет место в процессе ее обработки на различных участках технологических маршрутов. При этом целостность информации зависит не только от процессов, происходящих на объекте, но и от целостности информации, поступающей на его вход. Основную опасность представляют случайные дестабилизирующие факторы (отказы, сбои и ошибки компонентов автоматизированных систем обработки данных), которые потенциально могут проявиться в любое время, и в этом отношении можно говорить о регулярном потоке этих факторов. Из стихийных бедствий наибольшую опасность представляют пожары, опасность которых в большей или меньшей степени также является постоянной. Опасность побочных явлений практически может быть сведена к нулю путем надлежащего выбора места для помещений автоматизированной системы обработки данных и их оборудования. Что касается злоумышленных действий, то они связаны, главным образом, с несанкционированным доступом к ресурсам автоматизированной системы обработки данных. При этом наибольшую опасность представляет занесение вирусов. В соответствии с изложенным общая модель процесса нарушения физической целостности информации на объекте автоматизированной системы обработки данных может быть представлена схематично (рис.2).



Рисунок 2 – Общая модель процесса нарушения физической целостности информации на объекте АСОД

С точки зрения несанкционированного получения информации принципиально важным является то обстоятельство, что в современных автоматизиро-



ванных системах обработки данных оно возможно не только путем непосредственного доступа к базам данных, но и многими путями, не требующими такого доступа. При этом основную опасность представляют злоумышленные действия людей. Воздействие случайных факторов непосредственно не ведет к несанкционированному получению информации, оно лишь способствует появлению каналов несанкционированного получения информации, которыми может воспользоваться злоумышленник. Структурированная схема потенциально возможных злоумышленных действий в автоматизированных системах обработки данных для самого общего случая представлена (рис3):

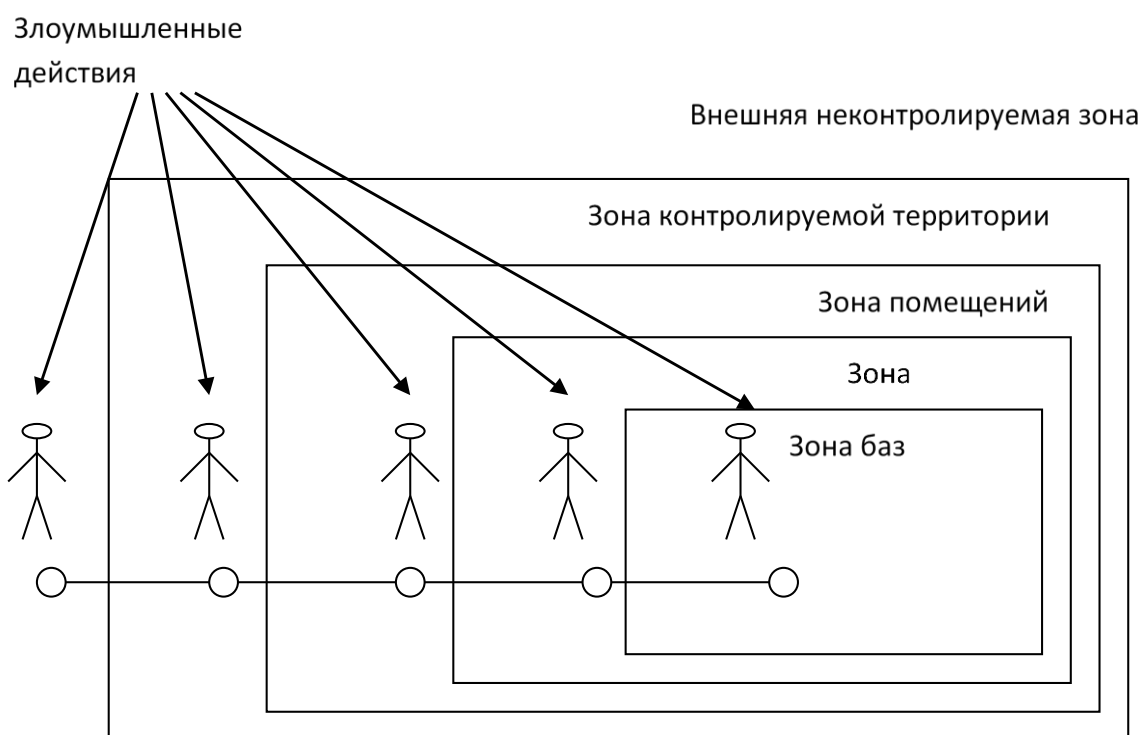


Рисунок 3 – Структурированная схема потенциально возможных злоумышленных действий в автоматизированных системах обработки данных

**Выделенные зоны определяются следующим образом:**

1) внешняя неконтролируемая зона — территория вокруг автоматизированной системы обработки данных, на которой персоналом и средствами автоматизированной системы обработки данных не применяются никакие средства и не осуществляется никакие мероприятия для защиты информации;

2) зона контролируемой территории — территория вокруг помещений автоматизированной системы обработки данных, которая непрерывно контролируется персоналом или средствами автоматизированной системы обработки данных;

3) зона помещений автоматизированной системы обработки данных — внутренне пространство тех помещений, в которых расположена система;

4) зона ресурсов автоматизированной системы обработки данных — та часть помещений, откуда возможен непосредственный доступ к ресурсам системы;

5) зона баз данных — та часть ресурсов системы, с которых возможен непосредственный доступ к защищаемым данным.

Злоумышленные действия с целью несанкционированного получения информации в общем случае возможны в каждой из перечисленных зон. При этом для несанкционированного получения информации необходимо одновременное наступление следующих событий: нарушитель должен получить доступ в соответствующую зону; во время нахождения нарушителя в зоне в ней должен проявиться (иметь место) соответствующий канал несанкционированного получения информации; соответствующий канал несанкционированного получения информации должен быть доступен нарушителю соответствующей категории; в канале несанкционированного получения информации в момент доступа к нему нарушителя должна находиться защищаемая информация.

Рассмотрим далее трансформацию общей модели уязвимости с точки зрения несанкционированного размножения информации. Принципиальными особенностями этого процесса являются:

1) любое несанкционированное размножение есть злоумышленное действие;

2) несанкционированное размножение может осуществляться в организациях-разработчиках компонентов автоматизированной системы обработки данных, непосредственно в автоматизированной системе обработки данных и

сторонних организациях, причем последние могут получать носитель, с которого делается попытка снять копию как законным, так и незаконным путем.

Попытки несанкционированного размножения информации у разработчика и в автоматизированной системе обработки данных есть один из видов злоумышленных действий с целью несанкционированного ее получения и поэтому имитируются приведенной моделью. Если же носитель с защищаемой информацией каким-либо путем (законным или незаконным) попал в стороннюю организацию, то для его несанкционированного копирования могут использоваться любые средства и методы, включая и такие, которые носят характер научных исследований и опытно-конструкторских разработок.

В процессе развития теории и практики защиты информации сформировалось три методологических подхода к оценке уязвимости информации: эмпирический, теоретический и теоретико-эмпирический.

### **Эмпирический подход к оценке уязвимости информации**

Сущность эмпирического подхода заключается в том, что на основе длительного сбора и обработки данных о реальных проявлениях угроз информации и о размерах того ущерба, который при этом имел место, чисто эмпирическим путем устанавливаются зависимости между потенциально возможным ущербом и коэффициентами, характеризующими частоту проявления соответствующей угрозы и значения имевшего при ее проявлении размера ущерба. Наиболее характерным примером моделей рассматриваемой разновидности являются модели, разработанные специалистами американской фирмы ИВМ. Рассмотрим развиваемые этих моделях подходы.

Исходной посылкой при разработке моделей является почти очевидное предположение: с одной стороны, при нарушении защищенности информации наносит некоторый ущерб, с другой, обеспечение защиты информации сопряжено с расходом средств. Полная ожидаемая стоимость защиты может быть выражена суммой расходов на защиту и на потери от ее нарушения. Со-

вершено очевидно, что оптимальным решением было бы выделение на защиту информации средств в размере  $C_{\text{опт}}$ , поскольку при этом обеспечивается минимизация общей стоимости защиты информации.

Для того, чтобы воспользоваться данным подходом к решению проблемы, необходимо, во-первых, знать (или уметь определять) ожидаемые потери при нарушении защищенности информации, а во-вторых, в зависимости между уровнем защищенности и средствами, затрачиваемыми на защиту информации.

Решение первого вопроса, т.е. оценки ожидаемых потерь при нарушении защищенности информации, принципиально может быть получено лишь тогда, когда речь идет о защите промышленной, коммерческой и им подобной тайны, хотя и здесь встречаются весьма серьезные трудности. Что касается оценки уровня потерь при нарушении статуса защищенности информации, содержащей государственную, военную и им подобную тайну, то здесь до настоящего времени строгие подходы к их получению не найдены. Данное обстоятельство существенно сужает возможную область использования моделей, основанных на рассматриваемых подходах.

Для определения уровня затрат, обеспечивающих требуемый уровень защищенности информации, необходимо по крайней мере знать, во-первых, полный перечень угроз информации, во-вторых, потенциальную опасность для информации для каждой из угроз и, в-третьих, размеры затрат, необходимых для нейтрализации каждой из угроз.

$$R_i = 10^{(S_i + V_i - 4)}$$

Поскольку оптимальное решение вопроса о целесообразном уровне затрат на защиту состоит в том, что этот уровень должен быть равен уровню ожидаемых потерь при нарушении защищенности, достаточно определить только уровень потерь. Специалистами фирмы IBM предложена следующая эмпирическая зависимость ожидаемых потерь от  $i$ -й угрозы информации:

где  $S_i$  — коэффициент, характеризующий возможную частоту возникновения соответствующей угрозы;

$V_i$  — коэффициент, характеризующий значение возможного ущерба при ее возникновении. Предложенные специалистами значения коэффициентов:

Таблица 1 – Значения коэффициента  $S_i$

Ожидаемая (возможная) частота появления угрозы	Предполагаемое значение $S_i$
Почти никогда	0
1 раз в 1000 лет	1
1 раз в 100 лет	2
1 раз в 10 лет	3
1 раз в год	4
1 раз в месяц (примерно, 10 раз в год)	5
12 раза в неделю (примерно 100 раз в год)	6
3 раза в день (1000 раз в год)	7

Таблица 2 – Возможные значения коэффициента  $V_i$

Значение возможного ущерба при проявлении угрозы (доллары США)	Предполагаемое значение $V_i$
1	0
10	1
100	2
1 000	3
10 000	4
100 000	5
1 000 000	6
10 000 000	7

Суммарная стоимость потерь определяется формулой

$$R = \sum_{V_i} R_i$$

Таким образом, если бы удалось собрать достаточное количество фактических данных о проявлениях угроз и их последствиях, то рассмотренную модель можно было бы использовать для решения достаточно широкого круга задач защиты информации, причем, нетрудно видеть, что модель позволяет не только находить нужные решения, но и оценивать их точность. По России такая статистика в настоящее время практически отсутствует. В США же, например, сбору и обработке указанных данных большое внимание уделяет целый ряд

учреждений (Стэнфордский исследовательский институт и др.). В результате уже получены достаточно представительные данные по целому ряду угроз, которые могут быть положены в основу ориентировочных расчетов и для других стран.

### **Практическое задание**

1. Загрузите ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ.»
2. Ознакомьтесь с **Приложениями С, D и E** ГОСТа.
3. Выберите три различных информационных актива организации (см. вариант).
4. Из **Приложения D** ГОСТа подберите три конкретных уязвимости системы защиты указанных информационных активов.
5. Пользуясь **Приложением С** ГОСТа напишите три угрозы, реализация которых возможна пока в системе не устранены названные в пункте 4 уязвимости.
6. Пользуясь одним из методов, предложенных в **Приложении E** ГОСТа произведите оценку рисков информационной безопасности.
7. Оценку ценности информационного актива производить на основании возможных потерь для организации в случае реализации угрозы.

### **Отчет**

Отчет должен содержать:

1. наименование работы;
2. цель работы;
3. задание;
4. последовательность выполнения работы;
5. ответы на контрольные вопросы;
6. вывод о проделанной работе.

### **Контрольные вопросы**

Дайте определение понятиям:

1. Уязвимости системы защиты информации
2. Угрозы ИБ
3. Оценка рисков

## Раздел 2. Уровни обеспечения информационной безопасности

### *Лабораторная работа 1. Требования к безопасности информационных систем.*

**Цель работы:** закрепление теоретических знаний по вопросам сертификации средств защиты информации по требованиям безопасности информации.

**Оборудование:** учебный персональный компьютер.

#### **Теоретические основы**

Минимальные (базовые) требования безопасности формулируются в общем виде, без учета категории, присвоенной ИС. Они задают базовый уровень информационной безопасности, им должны удовлетворять все информационные системы. Результаты категорирования важны при выборе регуляторов безопасности, обеспечивающих выполнение требований, сформулированных на основе анализа рисков.

Организация должна разработать, документировать и обнародовать официальную политику безопасности и формальные процедуры, направленные на выполнение приведенных ниже требований, и обеспечить эффективную реализацию политики и процедур.

В компании необходимо периодически производить оценку рисков, включая оценку угроз миссии, функционированию, имиджу и репутации организации, ее активам и персоналу. Эти угрозы являются следствием эксплуатации ИС и осуществляемых при этом обработки, хранения и передачи данных.

Применительно к закупке систем и сервисов в компании необходимо:

1. выделить достаточный объем ресурсов для адекватной защиты ИС;
2. при разработке систем учитывать требования ИБ;
3. ограничивать использование и установку программного обеспечения;
4. обеспечить выделение внешними поставщиками услуг достаточных ресурсов для защиты информации, приложений и/или сервисов.

***В области сертификации, аккредитации и оценки безопасности в организации следует проводить:***

1. постоянный мониторинг регуляторов безопасности, чтобы иметь доверие к их эффективности;
2. периодическую оценку регуляторов безопасности, применяемых в ИС, чтобы контролировать их эффективность;
3. разработку и претворение в жизнь плана действий по устранению недостатков и уменьшению или устранению уязвимостей в ИС;
4. авторизацию введения в эксплуатацию ИС и установление соединений с другими информационными системами.

***В области кадровой безопасности необходимо:***

1. обеспечить надежность (доверенность) должностных лиц, занимающих ответственные посты, а также соответствие этих лиц предъявляемым к данным должностям требованиям безопасности;
2. обеспечить защиту информации и информационной системы при проведении дисциплинарных акций, таких как увольнение или перемещение сотрудников;
3. применять соответствующие официальные санкции к нарушителям политики и процедур безопасности.

***Организация должна обеспечить информирование и обучение сотрудников:***

1. чтобы руководители и пользователи ИС знали о рисках, связанных с их деятельностью, и о соответствующих законах, нормативных актах, руководящих документах, стандартах, инструкциях и т.п.;
2. чтобы персонал имел должную практическую подготовку для выполнения обязанностей, связанных с информационной безопасностью.

В области планирования необходимо разработать, документировать, периодически изменять и реализовать планы обеспечения безопасности ИС, описывающие регуляторы безопасности (имеющиеся и планируемые) и правила поведения персонала, имеющего доступ к ИС.



С целью планирования бесперебойной работы в компании следует установить, поддерживать и эффективно реализовать планы реагирования на аварийные ситуации, резервного копирования, восстановления после аварий, чтобы обеспечить доступность критичных информационных ресурсов и непрерывность функционирования в аварийных ситуациях.

***В плане реагирования на нарушения информационной безопасности организация должна:***

1. создать действующую структуру для реагирования на инциденты, имея в виду адекватные подготовительные мероприятия, выявление, анализ и локализацию нарушений, восстановление после инцидентов и обслуживание обращений пользователей;

2. обеспечить прослеживание, документирование и сообщение об инцидентах соответствующим должностным лицам организации и уполномоченным органам.

***С целью физической защиты организация должна:***

1. предоставлять физический доступ к ИС, оборудованию, в производственные помещения только авторизованному персоналу;

2. физически защищать оборудование и поддерживающую инфраструктуру ИС;

3. обеспечить должные технические условия для функционирования ИС;

4. защищать ИС от угроз со стороны окружающей среды;

5. обеспечить контроль условий, в которых функционирует ИС;

6. обеспечить управление доступом, предоставив доступ к активам ИС только авторизованным пользователям, процессам, действующим от имени этих пользователей, а также устройствам (включая другие ИС) для выполнения разрешенных пользователям транзакций и функций.

***Для обеспечения протоколирования и аудита необходимо:***

1. создавать, защищать и поддерживать регистрационные журналы, позволяющие отслеживать, анализировать, расследовать и готовить отчеты о незаконной, несанкционированной или ненадлежащей активности;

2. обеспечить прослеживаемость действий в ИС с точностью до пользователя (подотчетность пользователей).

***В плане управления конфигурацией в компании следует:***

1. установить и поддерживать базовые конфигурации;
2. иметь опись (карту) ИС, актуализируемую с учетом жизненного цикла, в которую входят аппаратура, программное обеспечение и документация;
3. установить и обеспечить практическое применение настроек для конфигурирования средств безопасности в продуктах, входящих в ИС.

В области идентификации и аутентификации необходимо обеспечить идентификацию и аутентификацию пользователей ИС, процессов, действующих от имени пользователей, а также устройств как необходимое условие предоставления доступа к ИС.

***Кроме того, необходимо:***

***Применительно к сопровождению:***

1. осуществлять периодическое и своевременное обслуживание ИС;
2. обеспечить эффективные регуляторы для средств, методов, механизмов и персонала, осуществляющих сопровождение.

***Для защиты носителей:***

1. защищать носители данных как цифровые, так и бумажные;
2. предоставлять доступ к данным на носителях только авторизованным пользователям;
3. санировать или уничтожать носители перед выводом из эксплуатации или перед передачей для повторного использования.

***С целью защиты систем и коммуникаций:***

1. отслеживать, контролировать и защищать коммуникации (то есть передаваемые и принимаемые данные) на внешних и ключевых внутренних границах ИС;
2. применять архитектурные и аппаратно-программные подходы, повышающие действующий уровень информационной безопасности ИС.

### *Для обеспечения целостности систем и данных:*

1. своевременно идентифицировать дефекты ИС и данных, докладывать о них и исправлять;
2. защищать ИС от вредоносного программного обеспечения;
3. отслеживать сигналы о нарушениях безопасности и сообщения о новых угрозах для информационной системы и должным образом реагировать на них.

### **Практическое задание**

Пользуясь учебником, опишите:

1. Виды и схемы сертификации средств защиты информации.
2. Функции ФСТЭК в области сертификации средств защиты информации.
3. Функции органов сертификации средств защиты информации.
4. Функции испытательных лабораторий (центров).
5. Функции заявителей.
6. Порядок проведения сертификации и контроля.
7. Перечень средств защиты информации, подлежащих сертификации.

### **Отчет**

Отчет должен содержать:

1. наименование работы;
2. цель работы;
3. задание;
4. последовательность выполнения работы;
5. ответы на контрольные вопросы;
6. вывод о проделанной работе.

### **Контрольные вопросы**

1. Сформулируйте цели системы сертификации средств защиты информации по требованиям безопасности информации.
2. Организационная структура системы сертификации средств защиты информации по требованиям безопасности информации.
3. Назовите виды и схемы сертификации средств защиты информации.

## *Лабораторная работа 2. Требования к безопасности информационных систем в России.*

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

**Оборудование:** учебный персональный компьютер.

### **Теоретические основы**

Подход к безопасности реализован в руководящем документе Государственной технической комиссией при Президенте РФ «Классификация автоматизированных систем и требований по защите информации», выпущенном в 1992 г. Требования всех приведенных ниже документов обязательны для исполнения только для тех государственных либо коммерческих организаций, которые обрабатывают информацию, содержащую государственную тайну. Для остальных коммерческих структур документы носят рекомендательный характер. В данном документе выделено 9 классов защищенности автоматизированных систем от несанкционированного доступа к информации, а для каждого класса определен минимальный состав необходимых механизмов защиты и требования к содержанию защитных функций каждого из механизмов в каждом из классов систем.

Классы систем разделены на три группы, причем основным критерием деления на группы приняты специфические особенности обработки информации, а именно:

**третья группа** — системы, в которых работает один пользователь, допущенный ко всей обрабатываемой информации, размещенной на носителях одного уровня конфиденциальности; к группе отнесены два класса, обозначенные 3Б и 3А;

**вторая группа** — системы, в которых работает несколько пользователей, которые имеют одинаковые права доступа ко всей информации, обрабатываемой и/или хранимой на носителях различного уровня конфиденциальности; к группе отнесены два класса, обозначенные 2Б и 2А;

**первая группа** — многопользовательские системы, в которых одновременно обрабатывается и/или хранится информация разных уровней конфиденциальности, причем различные пользователи имеют разные права на доступ к информации; к группе отнесено 5 классов: 1Д, 1Г, 1В, 1Б и 1А.

Требования к защите растут от систем класса 3Б к классу 1А.

*Все механизмы защиты разделены на 4 подсистемы следующего назначения:*

- управления доступом;
- регистрации и учета;
- криптографического закрытия;
- обеспечения целостности.

Содержание средств для каждой группы систем приведено в документе. Приведенная в руководящем документе Гостехкомиссии методика распространяется на защиту от несанкционированного доступа к информации, находящейся непосредственно в ЗУ ЭВМ и на сменных машиночитаемых носителях. Значительно раньше, в 1978 г., Гостехкомиссией были выпущены руководящие документы, определяющие требования к защите информации в автоматизированных системах от утечки по побочным электромагнитным излучениям и наводкам.

При разработке названных требований учитывались следующие факторы:

1. Доля грифовой информации в общем объеме обрабатываемой информации.
2. Интенсивность обработки грифовой информации, выражаемая относительной долей времени ее обработки в течение суток.
3. Условия расположения аппаратуры автоматизированной системы.

Наличие рассмотренных методик и закрепление их в официальных документах создает достаточно надежную базу для защиты информации на регулярной основе.

Однако нетрудно увидеть, что с точки зрения современной постановки задачи защиты информации имеющиеся методики являются недостаточными по ряду причин, а именно:

1) методики ориентированы на защиту информации только в средствах ЭВТ, в то время как имеет место устойчивая тенденция органического сращивания автоматизированных и традиционных технологий обработки информации;

2) учитываются далеко не все факторы, оказывающие существенное влияние на уязвимость информации, а поэтому и подлежащие учету при определении требований к защите;

3) в научном плане они обоснованы недостаточно за исключением требований к защите информации от утечки по техническим каналам.

### **Практическое задание.**

1. Воспользуйтесь поиском для получения таблицы характеристик классов подсистем защищенности
2. Проанализируйте данную таблицу
3. Выпишите основные требования к информационной безопасности.
4. На основе полученных данных сформулируйте рекомендации по информационной безопасности.

### **Отчет**

*Отчет должен содержать:*

1. наименование работы;
2. цель работы;
3. задание;
4. последовательность выполнения работы;
5. ответы на контрольные вопросы;
6. вывод о проделанной работе.

### **Контрольные вопросы**

1. Сколько классов защищенности существует?
2. Обязательно ли выполнение всех требований изученного документа?
3. Учтены ли в изученном документе новые методы получения доступа?

### *Лабораторная работа 3. Оценка состояния безопасности ИС США.*

**Цель работы** изучить Стандарт США "Критерии оценки гарантировано защищенных вычислительных систем в интересах министерства обороны США".

**Оборудование:** учебный персональный компьютер.

#### **Теоретические основы**

Наиболее известным документом, четко определяющим критерии, по которым должна оцениваться защищенность вычислительных систем, и те механизмы защиты, которые должны использоваться в системах обработки секретной (конфиденциальной — в более общей постановке) информации, является так называемая "Оранжевая книга", представляющая собой стандарт США "Критерии оценки гарантировано защищенных вычислительных систем в интересах министерства обороны США" (Trusted Computer Systems Evaluation Criteria — TCSEC), принятый в 1983 году. Его принятию предшествовали пятнадцатилетние исследования, проводившиеся специально созданной рабочей группой и национальным бюро стандартов США.

Стандартом предусмотрено шесть фундаментальных требований, которым должны удовлетворять те вычислительные системы, которые используются для обработки конфиденциальной информации.

Требования разделены на три группы:

стратегия,

подотчетность,

гарантии — в каждой группе по два требования следующего содержания.

#### **1. Стратегия.**

**Требование 1** — стратегия обеспечения безопасности: необходимо иметь явную и хорошо определенную стратегию обеспечения безопасности.

**Требование 2** — маркировка: управляющие доступом метки должны быть связаны с объектами.

## 2. Подотчетность.

**Требование 3** — идентификация: индивидуальные субъекты должны идентифицироваться.

**Требование 4** — подотчетность: контрольная информация должна храниться отдельно и защищаться так, чтобы со стороны ответственной за это группы имелась возможность отслеживать действия, влияющие на безопасность.

## 3. Гарантии.

**Требование 5** — гарантии: вычислительная система в своем составе должна иметь аппаратные/программные механизмы, допускающие независимую оценку на предмет достаточного уровня гарантий того, что система обеспечивает выполнение изложенных выше требований (с первого по четвертое).

**Требование 6** — постоянная защита: гарантировано защищенные механизмы, реализующие перечисленные требования, должны быть постоянно защищены от "взламывания" и/или несанкционированного внесения изменений.

В зависимости от конкретных значений, которым отвечают автоматизированные системы, они разделены на четыре группы (D, C, B, A), которые называются так:

D — минимальная защита;

C — индивидуальная защита;

B — мандатная защита;

A — верифицированная защита.

Группы систем делятся на классы, причем все системы, относимые к группе D, образуют один класс (D), к группе C — два класса (C1 и C2), к группе B — три класса (B1, B2 и B3), к группе A — один класс (A1 с выделением части систем вне класса).

Ниже рассмотрим названия и краткую характеристику перечисленных классов:



**D** — минимальная защита — системы, подвергнутые оцениванию, но не отвечающие требованиям более высоких классов;

**C1** — защита, основанная на индивидуальных мерах — системы, обеспечивающие разделение пользователей и данных. Они содержат внушающие доверие средства, способные реализовать ограничения по доступу, накладываемые на индивидуальной основе, т.е. позволяющие пользователям иметь надежную защиту их информации и не дающие другим пользователям считывать или разрушать их данные. Допускается кооперирование пользователей по уровням секретности;

**C2** — защита, основанная на управляемом доступе — системы, осуществляющие не только разделение пользователей как в системах C1, но и разделение их по осуществляемым действиям;

**B1** — защита, основанная на присваивании имен отдельным средствам безопасности — системы, располагающие всеми возможностями систем класса C, и дополнительно должны быть формальные модели механизмов обеспечения безопасности, присваивания имен защищаемым данным (включая и выдаваемые за пределы системы) и средства мандатного управления доступом ко всем поименованным субъектам и объектам;

**B2** — структурированная защита — системы, построенные на основе ясно определенной и формально задокументированной модели, с мандатным управлением доступом ко всем субъектам и объектам, располагающие усиленными средствами тестирования и средствами управления со стороны администратора системы;

**B3** — домены безопасности — системы, монитор обращений которых контролирует все запросы на доступ субъектов к объектам, не допускающие несанкционированных изменений. Объем монитора должен быть небольшим вместе с тем, чтобы его состояние и работу можно было сравнительно легко контролировать и тестировать. Кроме того, должны быть предусмотрены: сигнализация о всех попытках несанкционированных действий и восстановление работоспособности системы;

**A1** — верификационный проект — системы, функционально эквивалентные системам класса В3, но верификация которых осуществлена строго формальными методами. Управление системой осуществляется по строго определенным процедурам. Обязательно введение администратора безопасности.

### **Практическое задание**

1. Проанализируйте стандарт «Критерии оценки доверенных компьютерных систем Министерства обороны США.» (**Department of Defense Trusted Computer System Evaluation Criteria -TCSEC**).
2. Согласно требованиям, предоставленным в стандарте, составьте характеристику вычислительной системы для обработки конфиденциальной информации.
3. Обоснуйте свой выбор решений по защите информации.

### **Отчет**

Отчет должен содержать:

1. наименование работы;
2. цель работы;
3. задание;
4. последовательность выполнения работы;
5. ответы на контрольные вопросы;
6. вывод о проделанной работе.

### **Контрольные вопросы**

1. Что такое политика безопасности?
2. Какие элементы включает в себя политика безопасности?
3. Что такое классы безопасности и уровни доверия?
4. Какие требования определяются классами С1 и С2?
5. Какие требования определяются классами В1, В2 и В3?
6. Какие требования определяются классом А1?

## ***Лабораторная работа 4. Определение классов защищенности средств вычислительной техники от несанкционированного доступа***

**Цель работы:** изучить и проанализировать руководящий документ "Средства вычислительной техники. Защита от несанкционированного доступа к информации.

Показатели защищенности от несанкционированного доступа к информации".

**Оборудование:** учебный персональный компьютер.

### **Теоретические основы**

Теоретические основы представлены в руководящем документе "Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации"

### **Практическое задание**

1. Изучить документ "Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации"
2. Укажите, какие типы НСД рассмотрены в документе.
3. Составить презентацию на тему «Классы защищённости СВТ»

### **Отчет**

Отчет должен содержать:

1. наименование работы;
2. цель работы;
3. задание;
4. последовательность выполнения работы;

5. ответы на контрольные вопросы;
6. вывод о проделанной работе.

### **Контрольные вопросы**

1. Как проводится оценка защищённости от НСД?
2. Какие типы документации необходимы СВТ?
3. Чем отличаются классы защищённости СВТ?

### ***Лабораторная работа 5. Определение требований к защите информации***

**Цель работы:** изучить требования, предъявляемые к защите информации, изучить документацию по защите информации.

**Оборудование:** учебный персональный компьютер.

### **Теоретические основы**

***С позиций системного подхода*** для реализации приведенных принципов процесс, да и сама система защиты информации должны отвечать некоторой совокупности **требований**.

**Защита информации** должна быть:

**- централизованной;**

необходимо иметь в виду, что процесс управления всегда централизован, в то время как

структура системы, реализующей этот процесс, должна соответствовать структуре защищаемого объекта;

**- плановой;**

планирование осуществляется для организации взаимодействия всех подразделений

объекта в интересах реализации принятой политики безопасности; каждая служба, отдел, направление разрабатывают детальные планы защиты информации в сфере своей компетенции с учетом общей цели организации;

**- конкретной и целенаправленной;**

защите подлежат абсолютно конкретные информационные ресурсы, могущие

представлять интерес для конкурентов;

- *активной*;

защищать информацию необходимо с достаточной степенью настойчивости и целеустремленности. Это требование предполагает наличие в составе системы информационной безопасности средств прогнозирования, экспертных систем и других инструментариев, позволяющих реализовать наряду с принципом «обнаружить и устранить» принцип «предвидеть и предотвратить»;

- *надежной и универсальной*, охватывать весь технологический комплекс информационной деятельности объекта; методы и средства защиты должны надежно перекрывать все возможные каналы утечки

информации и противодействовать способам несанкционированного доступа независимо от формы представления информации, языка ее выражения и вида носителя, на котором она закреплена;

- *нестандартной* (по сравнению с другими организациями), разнообразной по используемым средствам;

- *открытой* для изменения и дополнения мер обеспечения безопасности информации;

- *экономически эффективной*; затраты на систему защиты не должны превышать размеры возможного ущерба

### **Практическое задание**

1. Воспользуйтесь поиском для составления сводной таблицы документов, регламентирующих требования к информационной безопасности
2. Укажите, какие документы необходимо учитывать при проектировании защиты документации на электронном носителе.
3. Смоделируйте последовательность действий для защиты от копирования информации.

### **Отчет**

Отчет должен содержать:

1. наименование работы;
2. цель работы;

3. задание;
4. последовательность выполнения работы;
5. ответы на контрольные вопросы;
6. вывод о проделанной работе.

### **Контрольные вопросы**

1. Перечислите виды защиты информации.
2. Назовите объекты защиты информации и дайте их определения.
3. Назовите способы защиты информации.
4. Назовите свойства информации, составляющие модель информационной безопасности.
5. Назовите основные принципы информационной безопасности.
6. Перечислите условия и требования к защите информации.
7. Дайте определения политики безопасности на объекте и сформулируйте требования, предъявляемые к плану защиты информации

## **Раздел 3. Криптографическая защита информации**

### *Лабораторная работа 1. Анализ терминов и определений информационной безопасности*

**Цель работы** проанализировать ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения.

**Оборудование:** учебный персональный компьютер.

#### **Теоретические основы**

Теоретические сведения предоставлены в ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения.

#### **Практическое задание**

1. Изучить ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации.

2. Изучить основные термины и определения
3. Составить глоссарий для памятки по информационной безопасности.

### **Отчет**

Отчет должен содержать:

1. наименование работы;
2. цель работы;
3. задание;
4. последовательность выполнения работы;
5. ответы на контрольные вопросы;
6. вывод о проделанной работе.

### **Контрольные вопросы**

1. Как называется умышленно искаженная информация?
2. Как называется информация, к которой ограничен доступ?
3. Какими путями может быть получена информация?
4. Как называются компьютерные системы, в которых обеспечивается безопасность информации?
5. Основной документ, на основе которого проводится политика информационной безопасности?

## ***Лабораторная работа 2. Работа с ГОСТами в области информационной безопасности***

**Цель работы** на основе ГОСТ Р 53114-2008 получить навыки составления документации в области информационной безопасности.

**Оборудование:** учебный персональный компьютер.

### **Практическое задание**

1. На основе ГОСТ Р 53114-2008 составить памятку об информационной безопасности для заведения, использующего электронный

документооборот.

2. Обосновать достаточность предлагаемых пунктов безопасности.
3. На примере продемонстрировать необходимость соблюдения правил информационной безопасности.

### **Отчет**

Отчет должен содержать:

1. наименование работы;
2. цель работы;
3. задание;
4. последовательность выполнения работы;
5. ответы на контрольные вопросы;
6. вывод о проделанной работе.

### **Контрольные вопросы**

1. Какие стандарты включены в ГОСТ Р 53114-2008?
2. Что такое приемлемость уровня риска?

### ***Лабораторная работа № 3. Шифрование данных при хранении - EFS.***

**Цель работы:** Научиться использовать EFS для шифрования файлов и папок

**Оборудование:** учебный персональный компьютер

Шифрующая файловая система (Encrypting File System – EFS) появилась в операционных системах семейства Windows, начиная с Windows 2000. Она поз-



воляет шифровать отдельные папки и файлы на томах с файловой системой NTFS. Рассмотрим этот механизм подробнее.

Система шифрования данных EFS шифрует информацию прозрачно для пользователя. То есть пользователь сказал, — «Зашифровать папку» и вся информация, находящаяся в ней будет зашифрована автоматически. При обращении к зашифрованным файлам они автоматически расшифруются. В этом и заключается одно из преимуществ EFS перед созданием архива с паролем.

Нет, архив — это конечно, удобно. Но не так универсально. Архив необходимо распаковать, поработать с файлами и не забыть заново запаковать. + ко всему, когда вы удаляете файлы из которых создали архив с паролем, они-то физически не удаляются. А это брешь в обороне.

Работает EFS следующим образом. Когда необходимо зашифровать файл система генерирует случайный ключ, называемый FEK — **File Encryption Key**. Этим ключом с помощью симметричного алгоритма шифрования кодируется файл. Симметричный — значит файл шифруется и расшифровывается одним ключом — FEK.

При первой необходимости шифрования информации Windows создает **два ключа** пользователя: **открытый и закрытый**. FEK шифруется с помощью асимметричного алгоритма с использованием открытого ключа пользователя. Асимметричный алгоритм шифрования значит, что файл шифруется одним ключом (в нашем случае открытым), а расшифровывается другим (закрытым). Зашифрованный ключ FEK записывается рядом с зашифрованным файлом.

Закрытый ключ шифруется с помощью пароля пользователя. Поэтому защищенность вашей информации на прямую зависит от сложности вашего пароля. Поэтому и рекомендуется задать его более чем из 8-ми символов, включая буквы в нижнем и верхнем регистрах, цифры и специальные символы.

Для расшифровки данных необходимо зайти под учетной записью пользователя, который зашифровал файлы. При этом автоматически при вводе правильного пароля расшифровывается закрытый ключ. С помощью последнего

расшифровывается FEK — File Encryption Key, которым расшифровывается нужный файл.

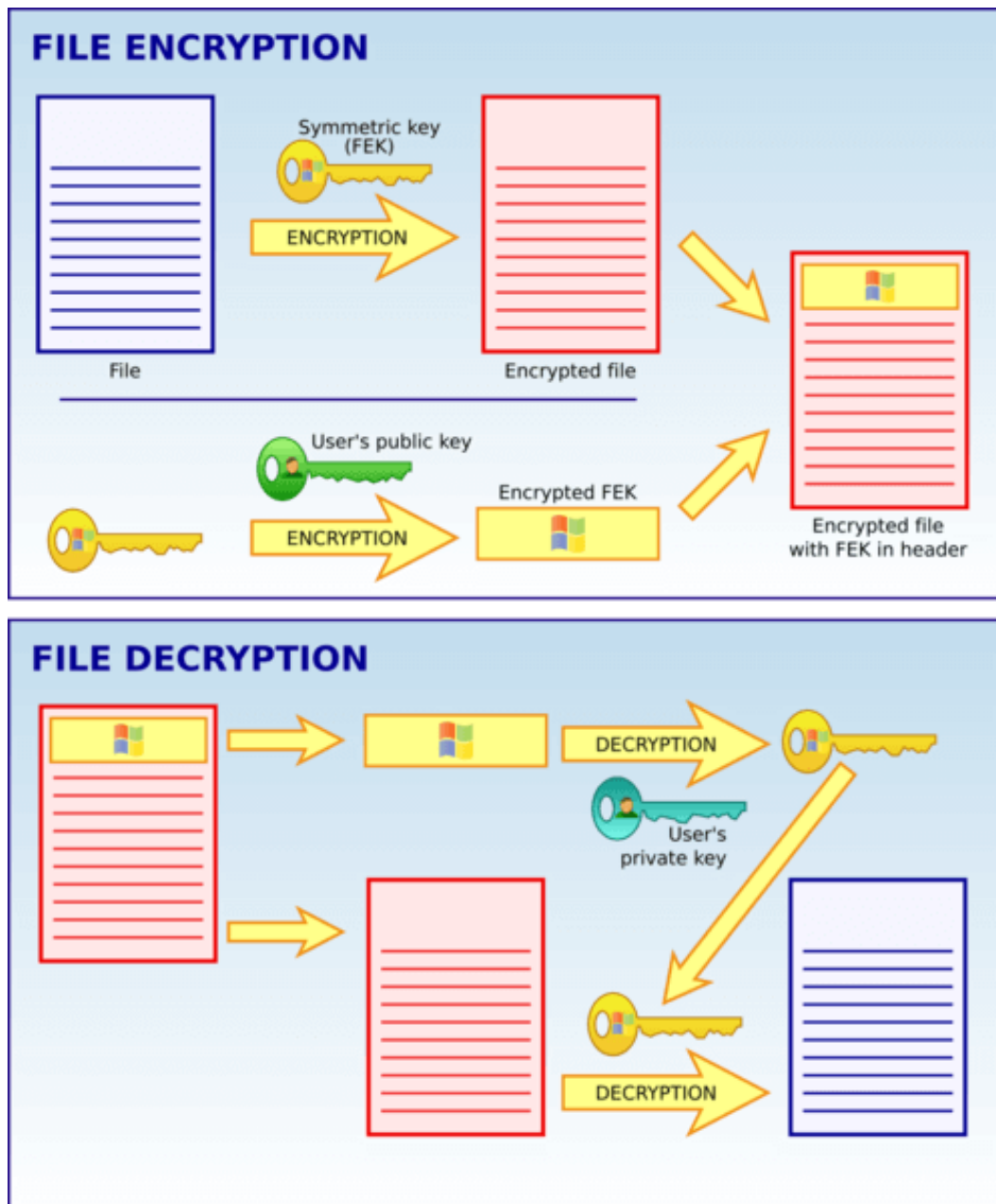


Рисунок 1 – Схема шифрования в EFS

## Шифрование файлов

Зашифровать файл можно следующим образом. С помощью правой кнопки мышки на файле вызываете контекстное меню и выбираете **Свойства**. На вкладке **Общие** в разделе **Атрибуты** нажимаем **Другие...**

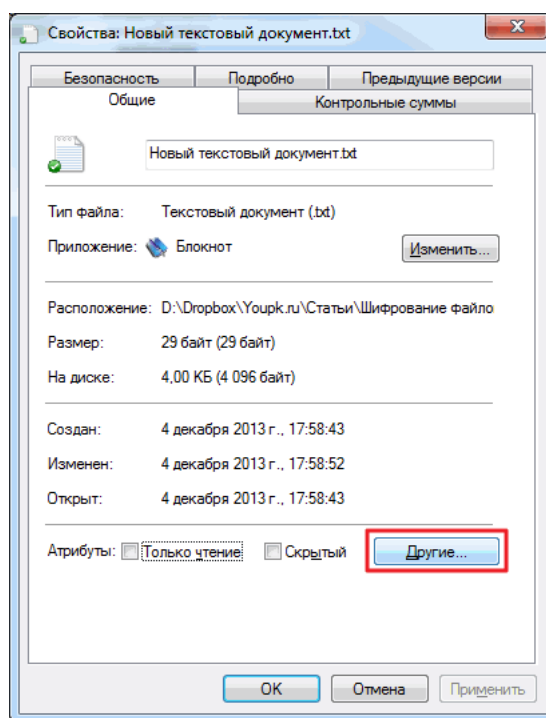


Рисунок 2 – контекстное меню Свойства документа

В открывшемся окошке ставим галочку **Шифровать содержимое для защиты данных**. И ОК

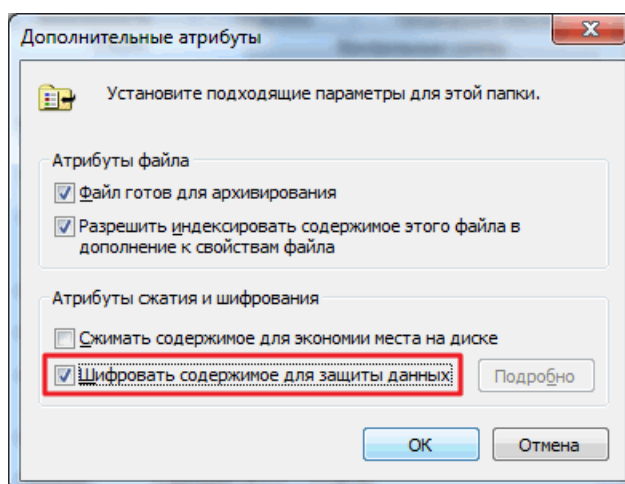


Рисунок 3 – Дополнительные атрибуты

Нажимаем применить или ОК в окошке свойств документа. Высвечивается предупреждение при шифровании, где **рекомендуется вместе с файлом зашифровать и содержащую его папку**. Выбираете рекомендуемый вариант и жмете ОК

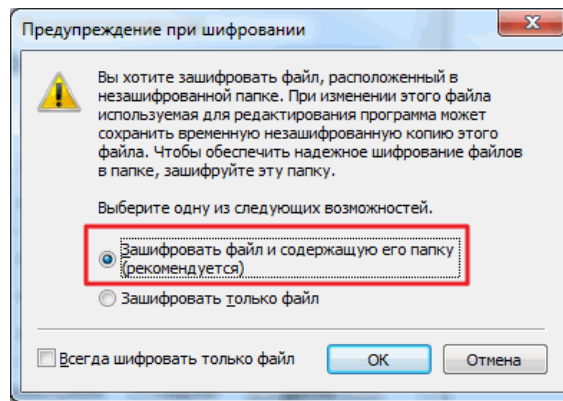


Рисунок 4 – Выбор шифрования

В этом же окошке поясняется зачем необходимо шифровать папку вместе с файлом — так как программы при редактировании создают временные файлы, которые не будут шифроваться. Обычно временные файлы удаляются, но возможен сбой программы или сбой в подаче питания к компьютеру, а вы без ИБП. В этом случае временный файл останется, и он будет не зашифрован, а это еще одна брешь во защите. Поэтому рекомендуется шифровать файл вместе с содержащей его папкой или шифровать полностью папку со всем содержимым.

Зашифрованные файлы обычно помечаются зеленым цветом если это указано в настройках

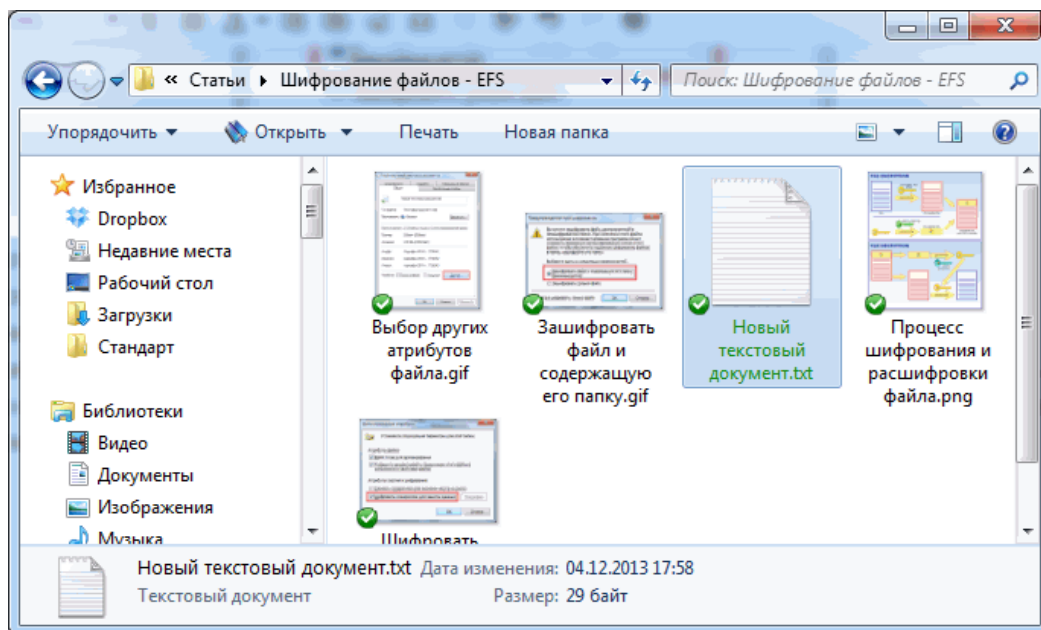


Рисунок 4 – Папка с зашифрованными файлами

Проверить это можно следующим образом. В проводнике на панели инструментов нажимаем **Упорядочить** и выбираем **Параметры папок и поиска**

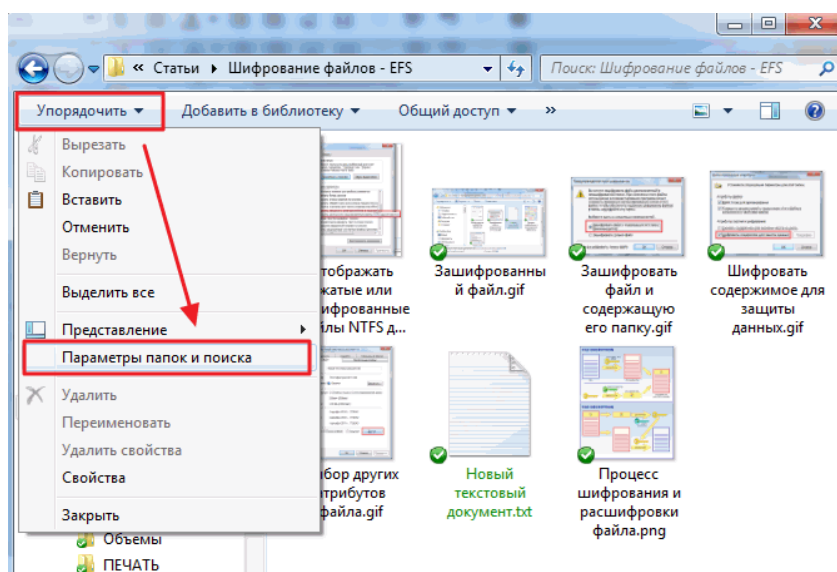


Рисунок 5 – Параметры папок и поиска

В окошке Параметры папок переходим на вкладку **Вид** и устанавливаем галочку **Отображать сжатые или зашифрованные файлы NTFS другим цветом**

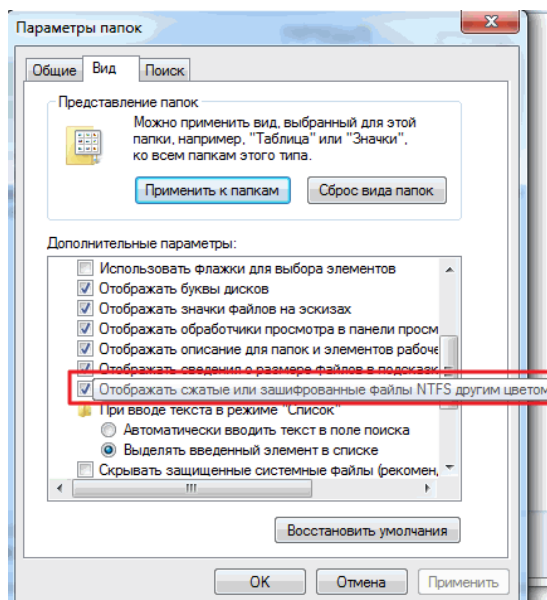


Рисунок 6 – Настройка параметров папок

Стоит отметить что в операционных системах Windows возможно или зашифровать файл, или сжать его для экономии места. Сомневаюсь, что кто то будет экономить в эпоху 3-х, 4-х и 5-ти терабайтных жестких дисков.

**Расшифровать файл** можно скопировав его в не зашифрованную папку и сняв соответствующий флажок в окошке Другие атрибуты.

Для удобства шифрования и дешифрования файлов можно включить в контекстном меню соответствующий пункт

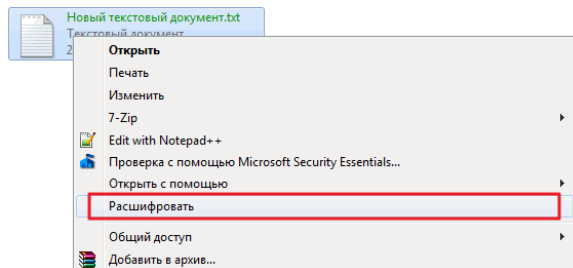


Рисунок 7 – Дешифрования файлов

Делается этого редактированием реестра. Вызываете утилиту regedit из поиска в меню Пуск

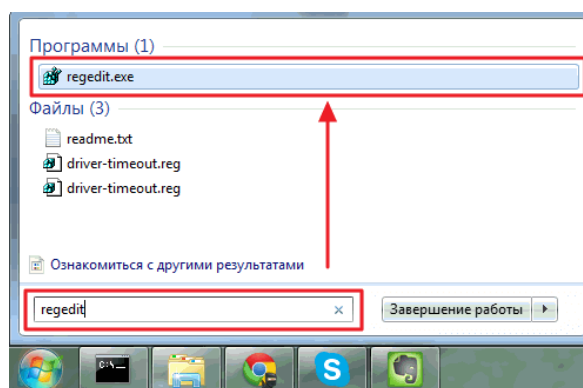


Рисунок 8 – Запуск редактора реестра

Переходите в раздел

**HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced**

и создаете параметр

**«EncryptionContextMenu»=dword:00000001**

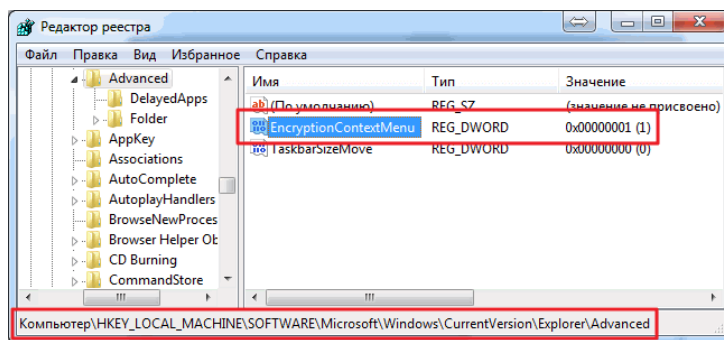


Рисунок 8 – Окно редактора реестра

Для того что бы создать параметр кликаем правой кнопкой мышки на пустом месте и выбираем **Создать > Параметр DWORD (32 бита)**

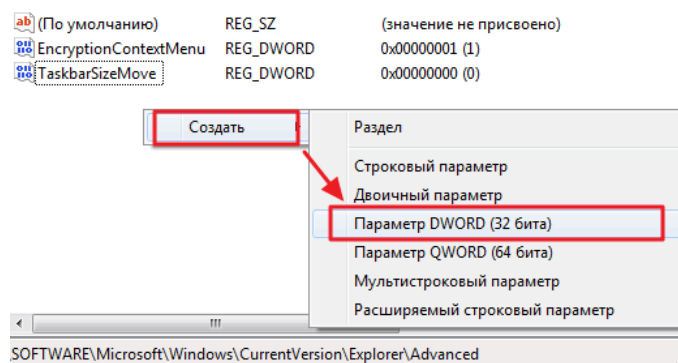


Рисунок 9 – Создание параметра в редакторе реестра

У меня работает, несмотря на то, что Windows 7 64-разрядный.

Теперь у вас в меню включены соответствующие пункты и шифровать станет еще проще.

## Сертификаты

При первом шифровании чего-либо создается два ключа: открытый и закрытый. Открытым происходит шифрация ключа FEK, а закрытым дешифрация. Оба этих ключа (открытый и закрытый) помещаются в сертификат. Соответственно эти сертификаты можно экспортировать для расшифровки данных на другом компьютере.

Делается это следующим образом.

С помощью поиска в меню Пуск запускаем консоль **mmc.exe**

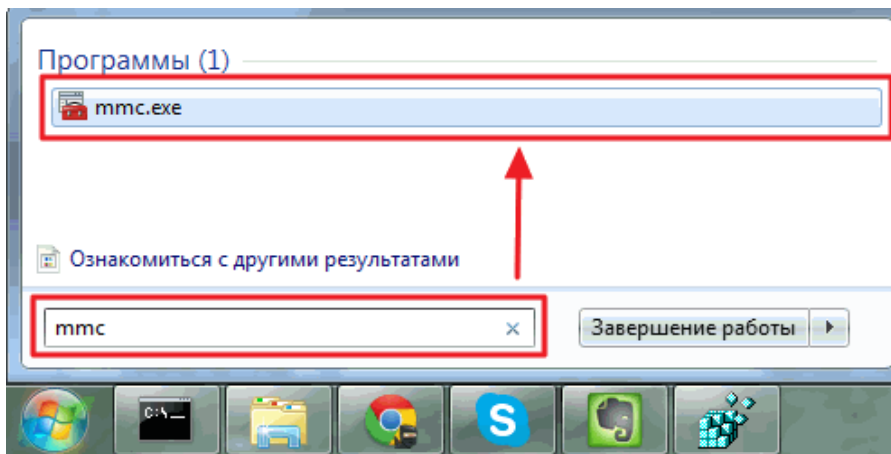


Рисунок 10 – Запуск консоли mmc

В открывшейся консоли нажимаете **CTRL+M** или переходите в меню **Файл > Добавить или удалить оснастку...**

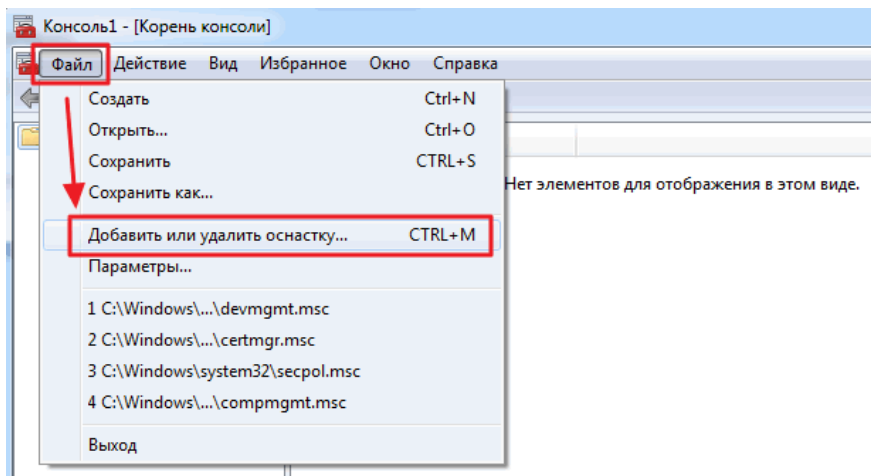


Рисунок 11 – Добавить или удалить оснастку

В открывшемся окошке в разделе **Доступные оснастки** выбираем **Сертификаты** и нажимаем **Добавить >**

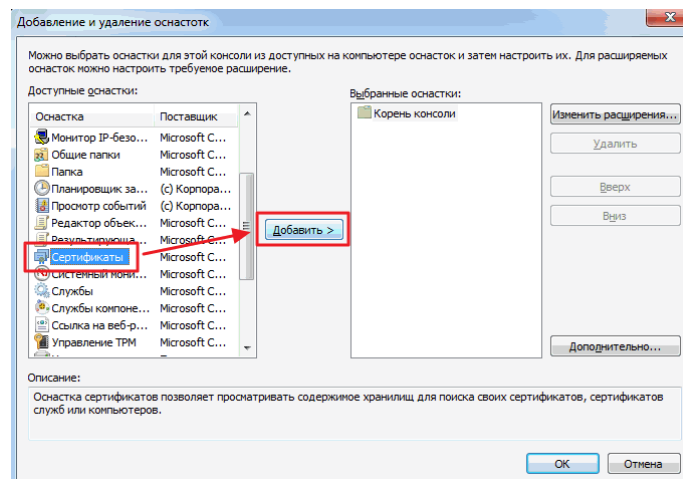


Рисунок 12 – Выбираем Сертификаты



В окошке проверяем что эта оснастка всегда будет управлять сертификатами моей учетной записи пользователя и жмем Готово

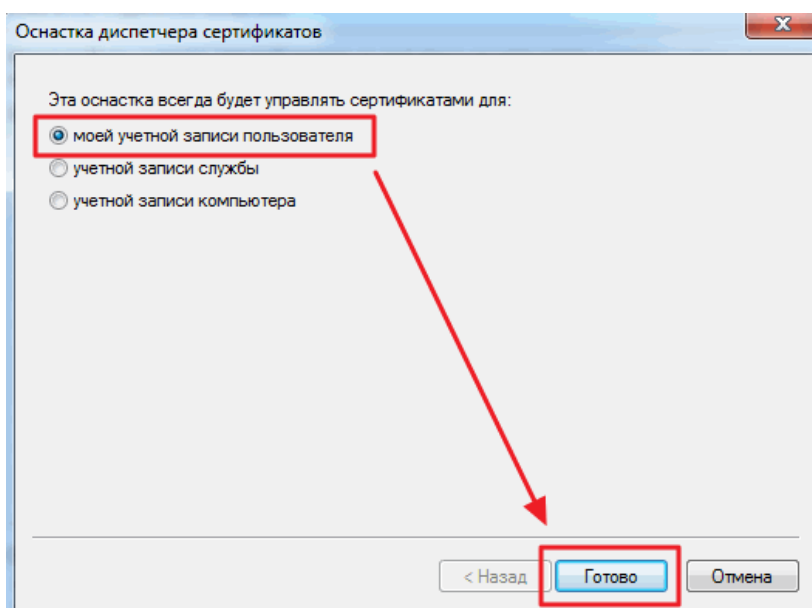


Рисунок 13 – Оснастка диспетчера сертификатов

Нажимаем ОК в приведенном ниже окошке

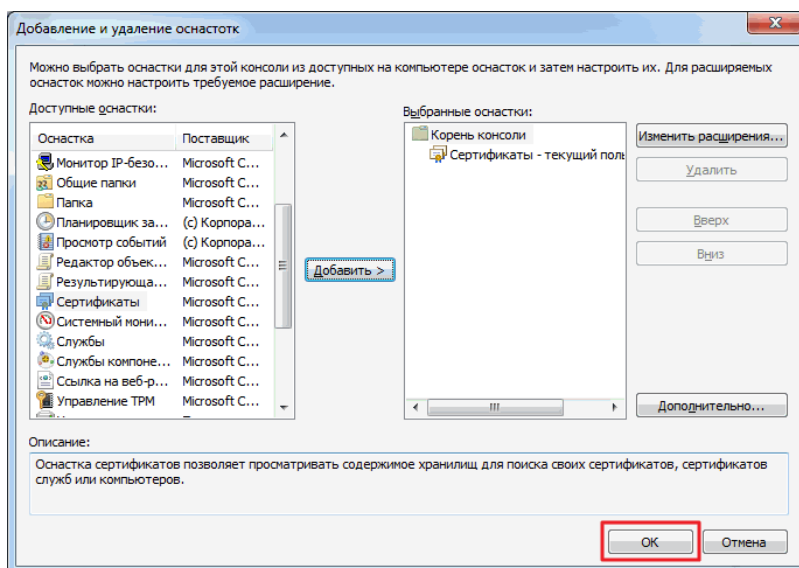


Рисунок 14 – Добавление оснастки сертификатов в корень консоли

В дереве консоли слева переходим по пути Сертификаты> Личное> Сертификаты. Выбираем созданный сертификат и вызываем на нем контекстное меню. Раскрываем раздел все задачи и выбираем Экспорт...

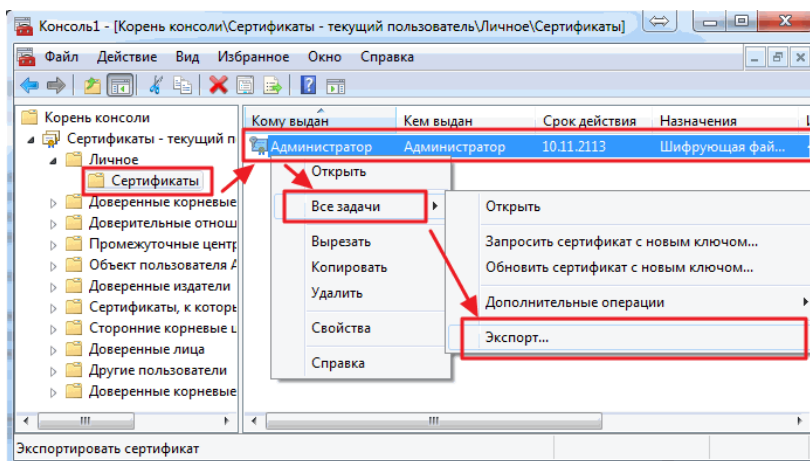


Рисунок 14 – Экспорт сертификатов

Открывается Мастер экспорта сертификатов. Нажимаем **Далее**>

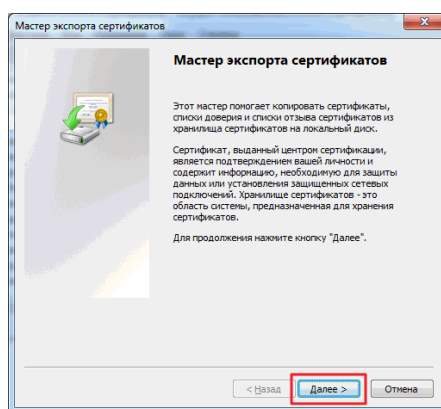


Рисунок 15 – Мастер экспорта сертификатов

Выбираем **Да, экспортировать закрытый ключ** и ждем **Далее**>

Вы сможете экспортировать только свои ключи для расшифровки своих файлов. То есть, если другой пользователь для вас установил свой сертификат с ключами для расшифровки своих файлов, вы его закрытый ключ не сможете экспортировать

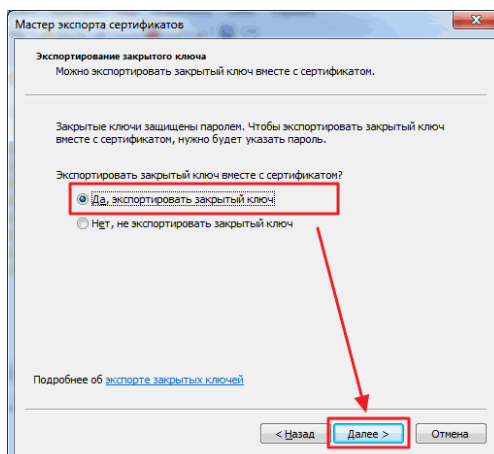


Рисунок 16 – Выбор экспорта закрытого ключа

В следующем окошке ничего не меняю жму **Далее >**

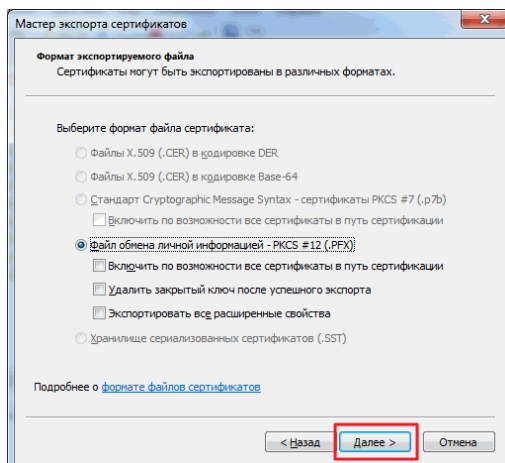


Рисунок 17 – Выбор формата экспортируемого файла

**Задаем пароль для защиты сертификата и вводим подтверждение пароля**

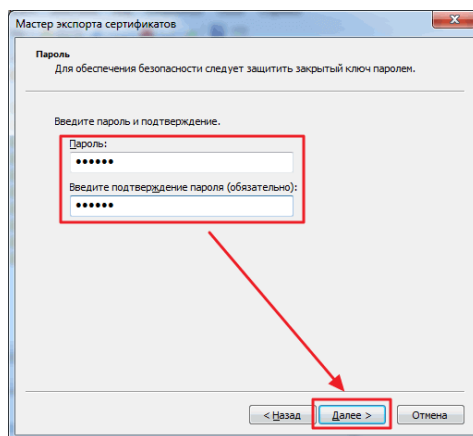


Рисунок 18 – Задаем пароль

Далее необходимо **указать расположение и имя экспортируемого файла**. Жмем **Обзор...**

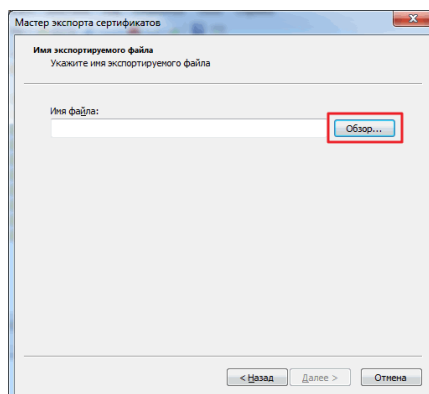


Рисунок 19 – Указываем расположение и имя экспортируемого файла

Выбираем, например, на Рабочий стол или на флешку. Задаем имя и ждем  
**Сохранить**

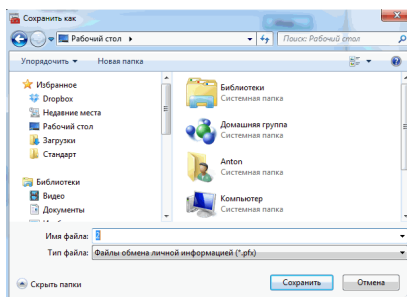


Рисунок 20 –Сохранение файла

Нажимаем **Далее >**

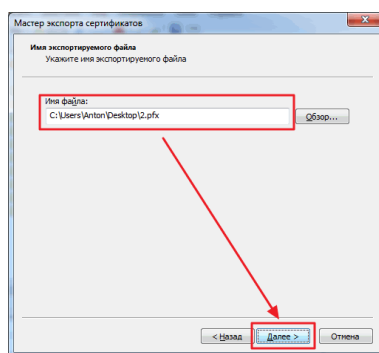


Рисунок 21 –Сохранение файла

В заключительном окошке нажимаем **Готово**

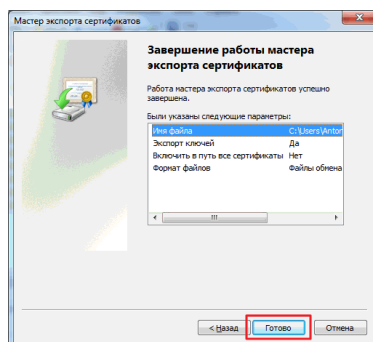


Рисунок 22 –Завершение работы мастера

Экспорт сертификата успешно выполнен в файл **.pfx**

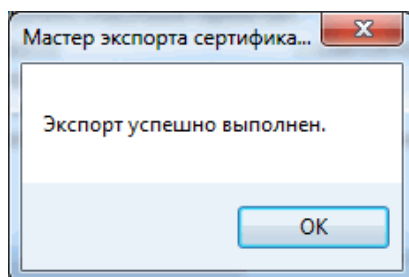


Рисунок 23 – Экспорт сертификата успешно выполнен в файл **.pfx**

Теперь его желательно спрятать в доступное только для вас место и не забыть пароль от него. Без пароля не получится импортировать сертификат на другой компьютер для расшифровки данных.

Для импорта сертификата на другом ПК достаточно запустить файл **.pfx** и следовать инструкциям мастера.

Без сертификата у вас не получится ни открыть файл, ни скопировать его. Будет возможность только удалить зашифрованный файл.

### **Практическое задание**

1. Работая под первой учетной записью, запросите сертификат (если он не был получен ранее), после чего зашифруйте папку с тестовым файлом, который не жалко потерять. Проверьте, что будет происходить при добавлении файлов, переименовании папки, копировании ее на другой диск с файловой системой NTFS на том же компьютере, копировании папки на сетевой диск или диск с FAT.
2. Убедитесь, что другой пользователь не сможет прочитать зашифрованный файл.
  1. Снова зайдите под первой учетной записью. В оснастке Certificates, удалите сертификат пользователя (несмотря на выдаваемые системой предупреждения). Завершите сессию пользователя в системе и войдите заново. Попробуйте открыть зашифрованный файл.
  2. Отредактируйте политику таким образом, чтобы убрать из системы агента восстановления (удалите в политике сертификат). Выполнив команду «gpupdate/force» (меню Start->run-> gpupdate /force) примените политику.
  3. Повторив действия из предыдущих заданий, убедитесь, что теперь только тот пользователь, который зашифровал файл, может его расшифровать.
  4. Теперь вернем в систему агента восстановления, но будем использовать новый сертификат. В редакторе политик находим политику Encrypting File System и в контекстном меню выбираем Create Data Recovery Agent. Это приведет к тому, что пользователь Administrator получит новый сертификат и с этого момента сможет восстанавливать шифруемые файлы.

5. Зашифруйте файл. Предоставьте другому пользователю, не являющемуся агентом восстановления, возможность также расшифровать данный файл. Проверьте работу выполненных настроек.

## **Отчет**

*Отчет должен содержать:*

1. наименование работы;
2. цель работы;
3. задание;
4. последовательность выполнения работы;
5. вывод о проделанной работе.

## **Раздел 4. Вредоносные программы**

### ***Лабораторная работа 1. Безопасность Windows и Windows Defender***

**Цель работы:** Научится использовать и настраивать защитника Windows Defender для защиты ПК от вредоносных программ.

**Оборудование:** учебный персональный компьютер.

#### ***Обзор службы безопасности Windows 10***

Безопасность Windows — это встроенная служба Windows 10, которая предлагает удобный интерфейс и инструменты для управления общими функциями безопасности операционной системы. Сюда относится «Защитник Windows», который предлагает защиту компьютера в реальном времени от вирусов и других вредоносных программ.

В этом руководстве мы расскажем, как начать работу с настройками безопасности Windows 10 и выполнять повседневные задачи с помощью встроенного антивируса, чтобы защитить свой компьютер от вредоносных программ и хакеров.

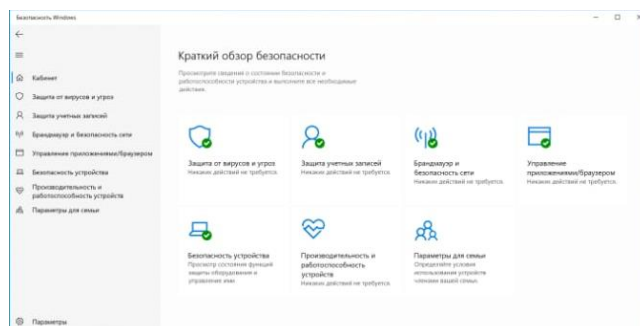
Прежде чем углубиться в руководство, необходимо понять разницу между терминами «Защитник Windows» (он же Windows Defender) и «Безопасность Windows»:

• **Безопасность Windows** — это служба, которая предлагает единый интерфейс для просмотра состояния и управления функциями безопасности, такими как антивирус, брандмауэр, производительность и прочие.

• **Защитник Windows** — это встроенное ПО, которое в реальном времени предлагает защиту от вредоносных программ, вирусов, шпионского ПО, программ-вымогателей и так далее.

Установка стороннего антивируса автоматически отключает Защитника, но не влияет на работоспособность службы «Безопасность Windows». Точно так же отключение встроенного антивируса или брандмауэра, не приведёт к отключению «Безопасности Windows».

Безопасность Windows — это простое интуитивно понятное приложение. Вы можете открыть его из меню «Пуск» или дважды щёлкнув значок щита в области уведомлений на панели задач.



На домашней странице можно смотреть состояние безопасности всех функций защиты, доступных по умолчанию в Windows 10. Здесь же отображаются предупреждения обо всех действиях, которые необходимо предпринять для обеспечения безопасности вашего компьютера.

Значок щита в области уведомлений панели задач также может предупредить вас, когда необходимо выполнить действие. Если имеется более одного предупреждения, отображается только самое серьёзное предупреждение.

Безопасность Windows включает семь областей защиты, которыми вы можете управлять:

- **Защита от вирусов и угроз** — содержит настройки встроенного антивируса. Он позволяет отслеживать защиту от вредоносных программ, сканировать устройство на наличие угроз, запускать автономное сканирование, настраивать расширенную функцию защиты от программ-вымогателей.
- **Защита учётных записей** — позволяет настаивать защиту своей учётную запись в Windows 10.
- **Брандмауэр и безопасность сети** — позволяет отслеживать сетевые подключения и настраивать различные параметры встроенного брандмауэра.
- **Управление приложениями и браузером** — помогает защититься от вредоносного кода, скрытого в приложениях, файлах или сайтах.
- **Безопасность устройства** — содержит функции безопасности на уровне оборудования, такие как изоляция ядра для защиты компьютера от атак.
- **Производительность и работоспособность устройства** — отчёт о работоспособности вашего компьютера.
- **Параметры для семьи** — предлагает лёгкий доступ к управлению устройствами семьи с помощью учётной записи Microsoft.

### **Как проверить компьютер на наличие вредоносных программ**

Windows 10 автоматически обновляет базы вредоносного ПО и регулярно сканирует устройство на наличие вредоносных программ. Но вы можете выполнять все эти проверки вручную.

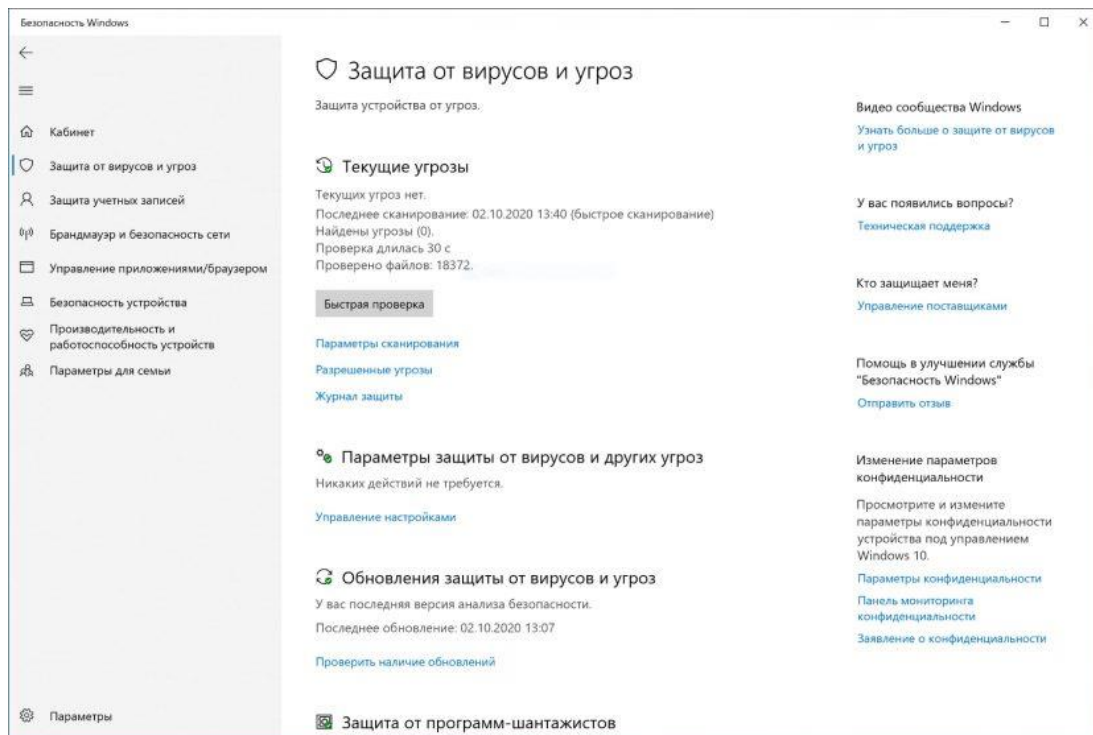
#### ***Быстрая проверка на вирусы***

Быстрое сканирование занимает меньше минуты и проверяет только те части системы, в которых наиболее вероятно могут скрываться вредоносные программы.

Чтобы запустить проверку на вирусы с помощью Microsoft Defender, выполните следующие действия:

1. Щёлкните **Защита от вирусов и угроз**.
2. Нажмите кнопку **Быстрая проверка**.





После выполнения этих шагов начнётся сканирование системы, а в разделе «Текущие угрозы» будут показаны обнаруженные угрозы, а также время, необходимое для завершения сканирования, и количество просканированных файлов.

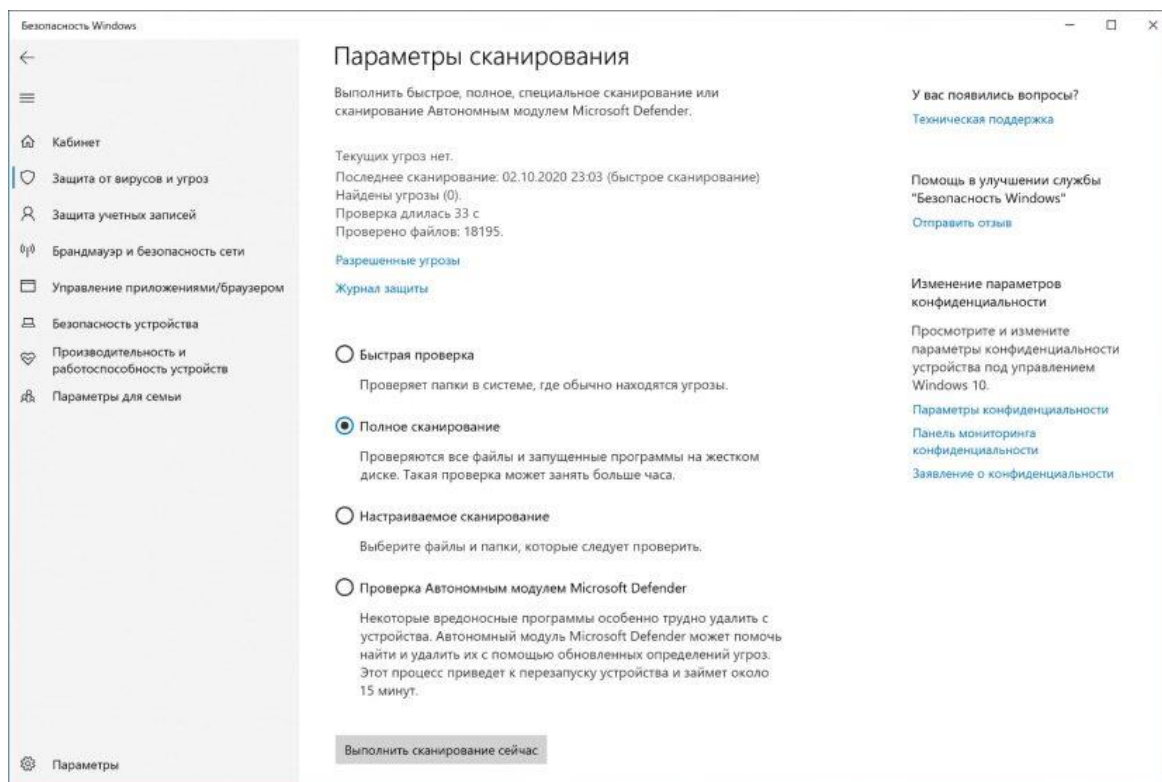
Если вы подозреваете, что на вашем компьютере есть вирус, попробуйте выполнить полное сканирование.

### ***Полная проверка на вирусы***

Полная проверка на вирусы занимает больше времени, но при этом проверяются все файлы, папки и приложения.

Чтобы запустить полную проверку на вирусы с помощью Microsoft Defender, выполните следующие действия:

1. Щёлкните **Защита от вирусов и угроз**.
2. В разделе «Текущие угрозы» щёлкните ссылку **Параметры сканирования**.
3. Выберите опцию **Полная проверка**, нажмите кнопку **выполнить сканирование сейчас**.



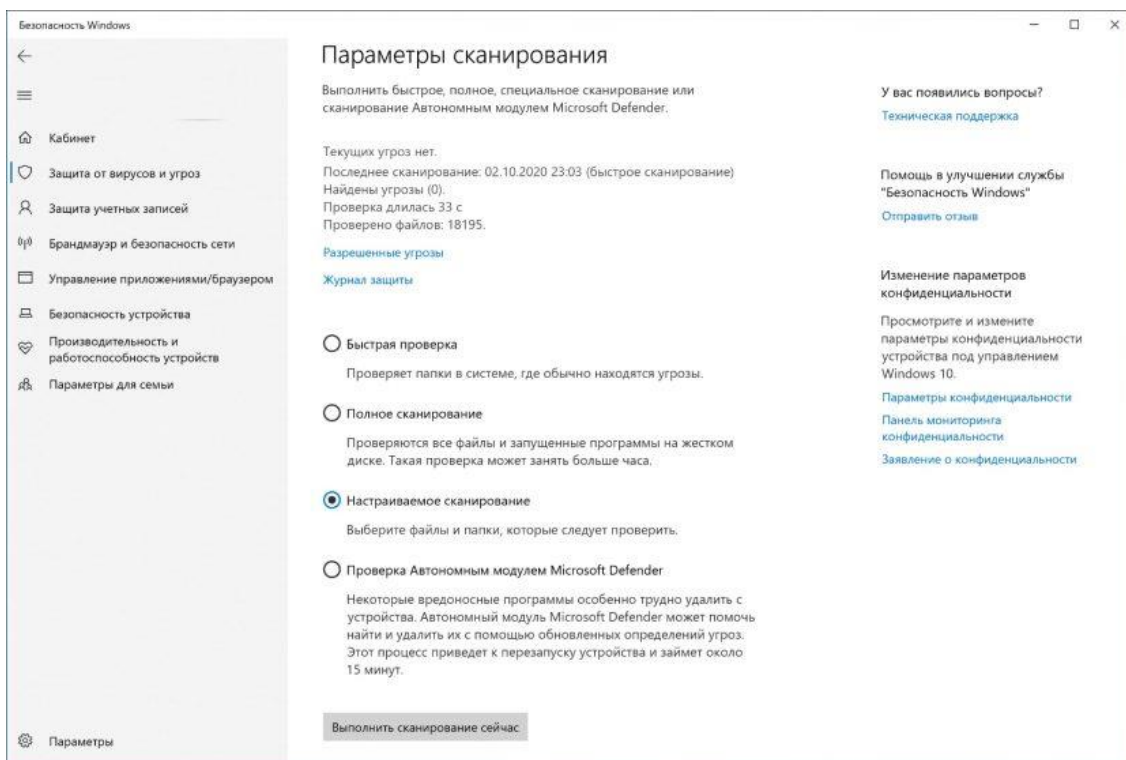
После выполнения этих шагов можно продолжить использование устройства, антивирус выполнит полное сканирование для обнаружения любых потенциальных вредоносных программ в фоновом режиме.

### ***Настраиваемое сканирование на вирусы***

Если вы хотите сканировать только определённую папку или файл, антивирус Windows 10 предоставляет возможность выполнить настраиваемое сканирование.

Для запуска настраиваемого сканирования на вирусы, выполните следующие действия:

1. Щёлкните **Защита от вирусов и угроз**.
2. В разделе «Текущие угрозы» щёлкните ссылку **Параметры сканирования**.
3. Выберите вариант **Выборочное сканирование**, нажмите кнопку **выполнить сканирование сейчас**.
4. Выберите место для сканирования и нажмите кнопку «**Выбор папки**».



Вы можете щёлкнуть правой кнопкой мыши диск, папку или файл и выбрать параметр **«Проверка с использованием Microsoft Defender»** в контекстном меню, чтобы выполнить выборочное сканирование.

### ***Проверка на вирусы автономным модулем***

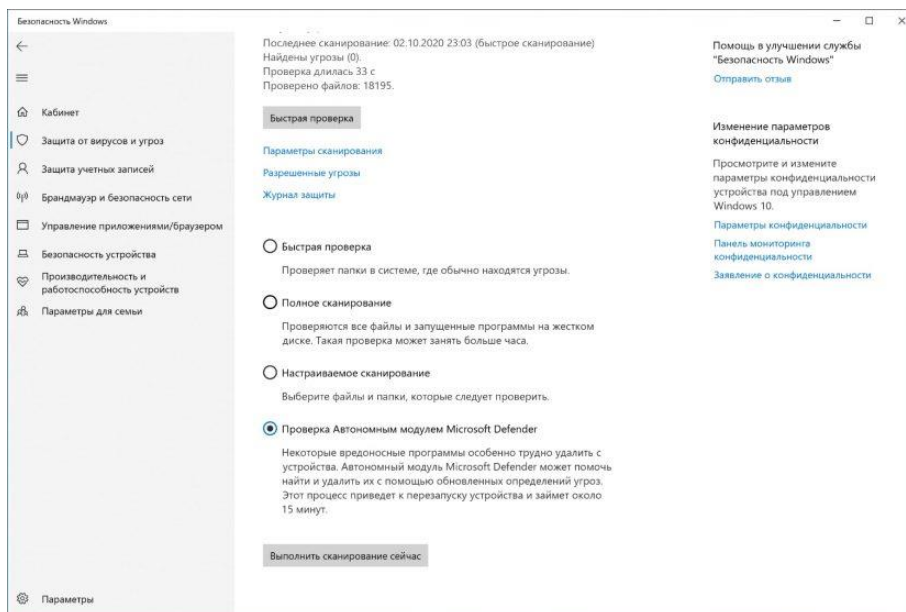
Иногда, если вы имеете дело с серьёзным вирусом или другим типом вредоносного ПО, антивирус может не удалить его во время работы Windows 10. В этом случае можно использовать Microsoft Defender для автономного сканирования.

При использовании функции автономного модуля компьютер автоматически перезагружается в среде восстановления и выполняет полное сканирование перед запуском Windows 10.

Чтобы запустить проверку на вирусы автономным модулем, выполните следующие действия:

1. Щёлкните **Защита от вирусов и угроз**.
2. В разделе «Текущие угрозы» щёлкните ссылку **Параметры сканирования**.
3. Выберите опцию **Проверка автономным модулем Microsoft Defender**.
4. Нажмите кнопку **выполнить сканирование сейчас**.

## 5. В открывшемся окне щёлкните кнопку **Проверка**.



После того, как вы выполните эти шаги, устройство перезагрузится и загрузится с автономным модулем антивируса Microsoft Defender, которая просканирует весь ПК. Если вредоносный код обнаружен, он будет автоматически удалён или помещён в карантин.

После сканирования устройство автоматически загрузит Windows 10, и вы сможете просмотреть отчёт в приложении «Безопасность Windows».

### **Как просмотреть журнал защиты**

В антивирусе Microsoft Defender есть область, в которой вы можете просматривать последние действия и рекомендации по защите.

Чтобы просмотреть журнал защиты, выполните следующие действия:

1. Щёлкните **Защита от вирусов и угроз**.
2. Щёлкните параметр **Журнал защиты**.
3. Щёлкните раскрывающееся меню «Фильтры» и выберите что хотите посмотреть: рекомендации, помещённые в карантин, удалённые или заблокированные файлы.

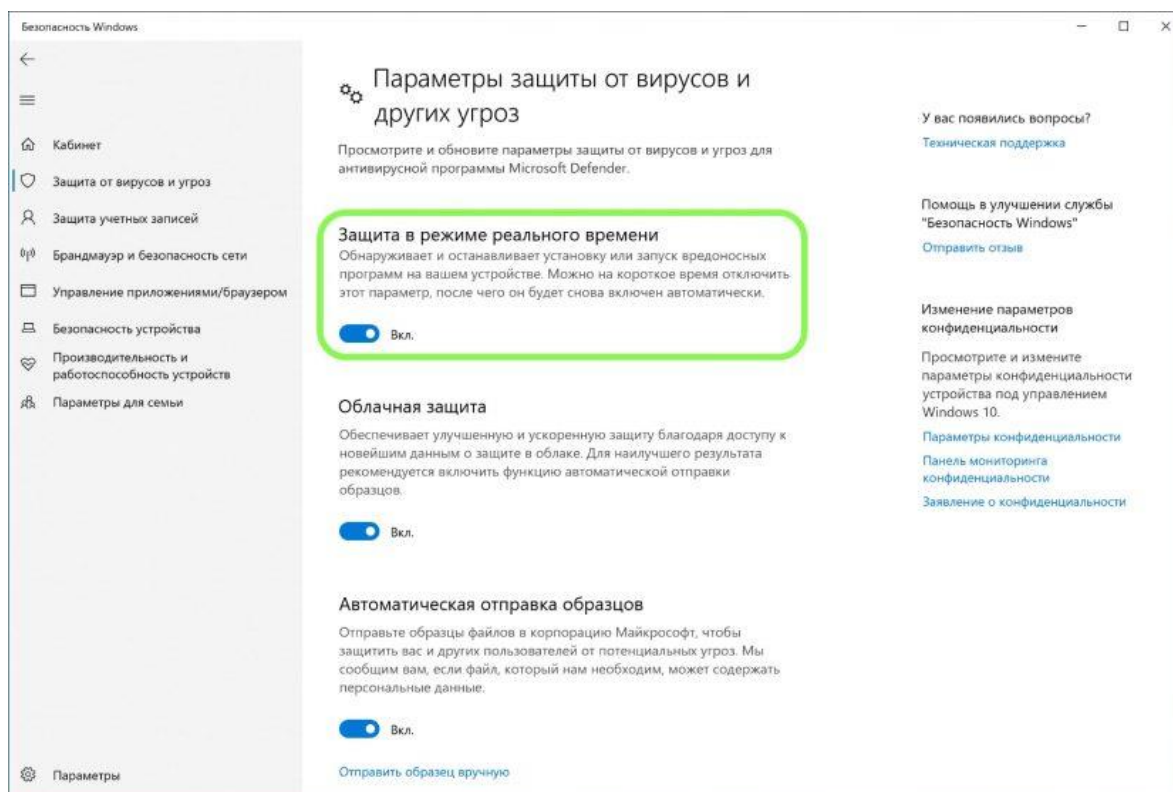
После выполнения этих шагов вы увидите отчёт с файлами, которые были удалены, очищены или всё ещё ждут вашего действия.

### **Как временно отключить антивирус Windows 10**

Не рекомендуется использовать компьютер без защиты от вредоносных программ, но иногда антивирус может мешать установке приложения или обновления программного обеспечения. В этом случае вы можете временно отключить антивирус Windows 10, чтобы завершить установку своего ПО.

Чтобы отключить антивирус Microsoft Defender, выполните следующие действия:

1. Щёлкните **Защита от вирусов и угроз**.
2. В разделе «Параметры защиты от вирусов и угроз» выберите параметр **«Управление настройками»**.
3. Выключите ползунок **Защита в режиме реального времени**.



Выполнив эти шаги, вы сможете выполнить задачи, которые конфликтовали с антивирусом.

Если не включить антивирус повторно, он будет автоматически активирован при перезагрузке компьютера.

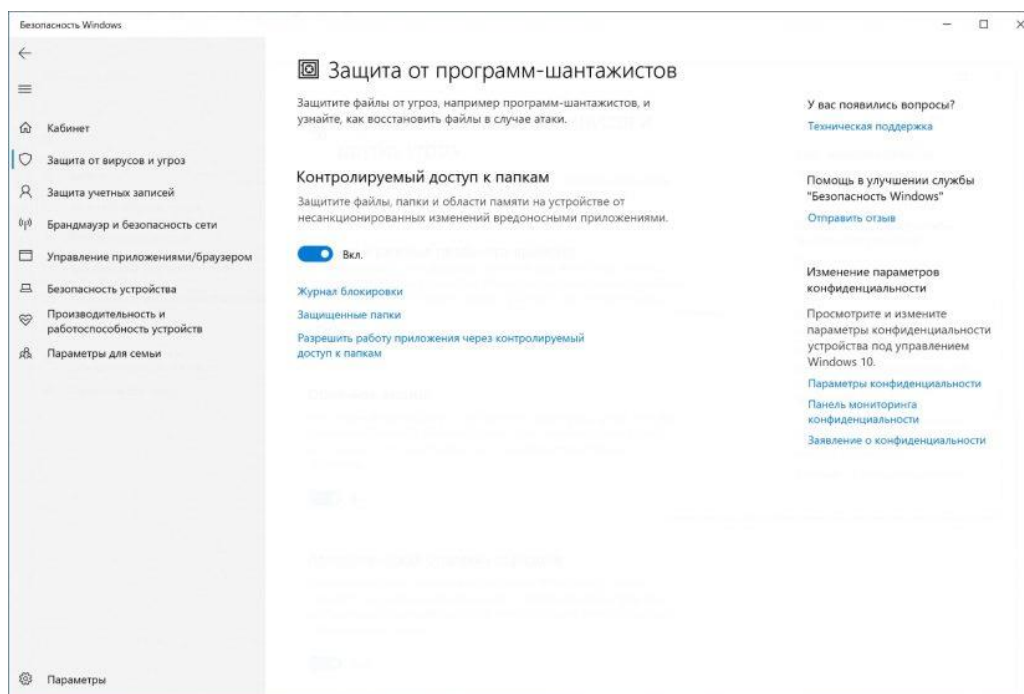
### ***Как включить защиту от программ-вымогателей***

Windows 10 включает функцию контролируемого доступа к папкам, предназначенную для мониторинга и защиты ваших данных от атак программ-вымогателей или нежелательных изменений со стороны вредоносных программ.

Поскольку эта функция может вызывать ложные срабатывания, она по умолчанию неактивна. Вам нужно включить её вручную с помощью приложения безопасности Windows.

Чтобы включить контролируемый доступ к папкам в Windows 10, выполните следующие действия:

1. Щелкните **Защита от вирусов и угроз**.
2. В разделе «Параметры защиты от вирусов и угроз» выберите параметр **«Управление параметрами»**.
3. В разделе «Контролируемый доступ к папкам» выберите опцию **Управление контролируемым доступом к файлам**.
4. Активируйте ползунок.



После выполнения этих шагов функция безопасности будет отслеживать приложения, пытающиеся внести изменения в файлы в защищённых папках.



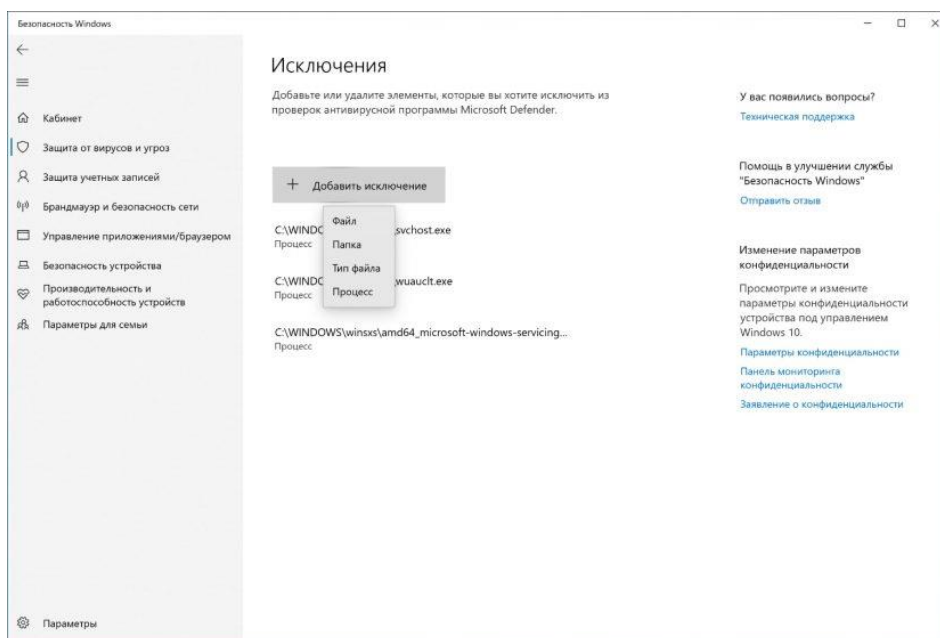
Если приложение помечено как вредоносное или неизвестное, контролируемый доступ к папке заблокирует попытку внесения изменений, а вы получите уведомление об этом.

### Как исключить файлы и папки для сканирования

Если у вас есть папка с файлами, которую вы не хотите проверять на вирусы, можно исключить её из процесса сканирования.

Чтобы антивирус не сканировал определённые папки, выполните следующие действия:

1. Щёлкните **Защита от вирусов и угроз**.
2. В разделе «Параметры защиты от вирусов и других угроз» выберите **«Управление настройками»**.
3. В разделе «Исключения» выберите параметр **«Добавление или удаление исключений»**.
4. Нажмите кнопку **Добавить исключение**.
5. Выберите тип исключения, который вы хотите настроить: файл, папка, тип файла, процесс и его расположение.



После того, как вы выполните эти шаги, антивирус не будет сканировать указанный файл, папку, тип файла или процесс.

За один раз можно добавить одно исключение. Чтобы добавить больше исключений, повторите шаги выше несколько раз.

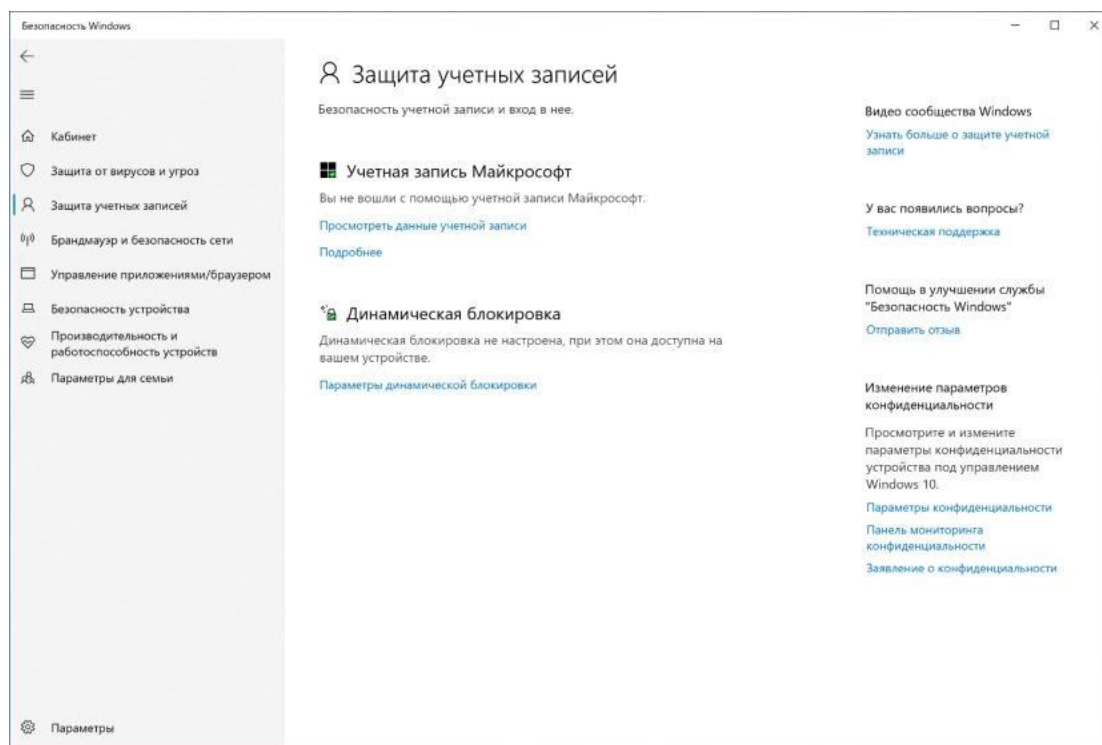
Рекомендуем ознакомиться про то, как сканировать на вирусы сетевые файлы в Windows 10.

### ***Как проверить защиту учётной записи***

Функция защиты учётной записи Windows 10 предназначена для отслеживания и уведомления о любых проблемах с вашей учётной записью.

Чтобы проверить защиту учётной записи в Windows 10, выполните следующие действия:

1. Щёлкните **Защита учётных записей**.
2. Убедитесь, что учётная запись Microsoft, Windows Hello и динамическая блокировка имеют зелёную отметку, указывающую на то, что всё работает правильно.



Если один из элементов защиты учётной записи требует вашего внимания, вы увидите предупреждение о необходимости принять меры по устранению проблемы.

Если вы используете пароль для входа в систему, система порекомендует настроить учётную запись с помощью одного из доступных методов проверки подлинности Windows Hello, таких как отпечаток пальца, распознавания лица или PIN-кода.



## Как управлять сетевой безопасностью с помощью брандмауэра

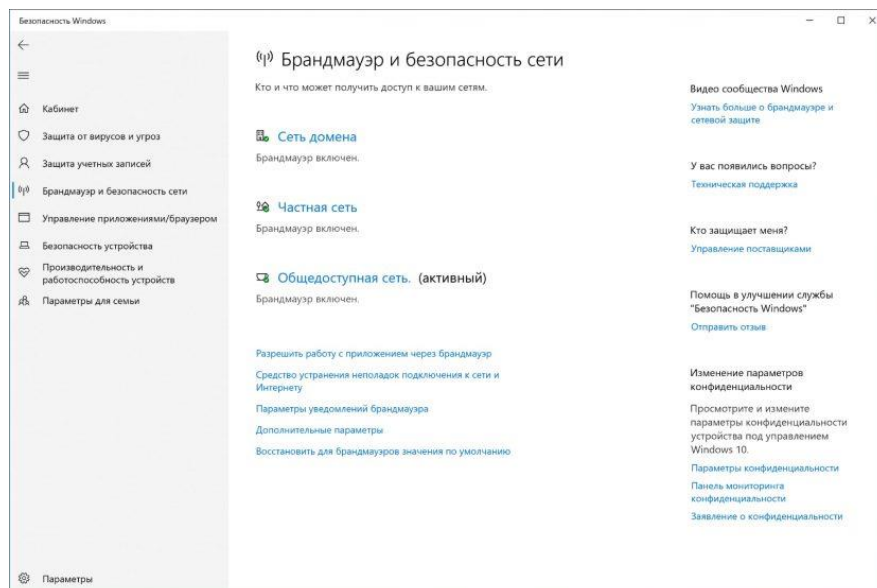
В приложении есть область для мониторинга и управления настройками брандмауэра Microsoft Defender.

### Просмотр статуса брандмауэра

Чтобы получить доступ к настройкам брандмауэра с помощью безопасности Windows, выполните следующие действия:

#### 1. Щёлкните **Брандмауэр и безопасность сети**.

На странице вы можете увидеть, какой сетевой профиль включён в данный момент. Тот, что отмечен как активный — это текущий сетевой профиль, который используется.

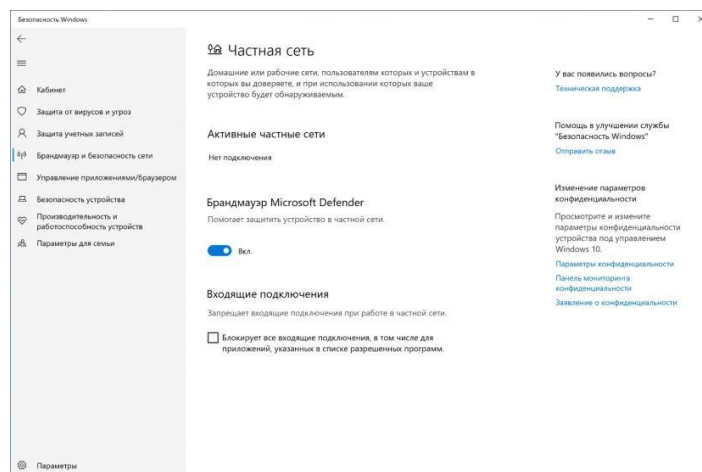


На странице также отображаются настройки параметров брандмауэра, позволяющие приложениям проходить через брандмауэр. Однако эти параметры являются ссылками для изменения конфигурации через Панель управления.

### Включить или отключить брандмауэр

Чтобы включить или отключить брандмауэр Защитника Windows, выполните следующие действия:

1. Щёлкните **Брандмауэр и безопасность сети**.
2. Щёлкните активный брандмауэр. Например, **Частная сеть**.
3. Включите или выключите тумблер **брандмауэра защитника Microsoft**.



Здесь же можно установить флажок, заблокировав все входящие подключения, включая те, что указаны в списке разрешённых приложений.

После того, как вы выполните эти шаги, на вашем компьютере отключится брандмауэр.

Если вы отключаете брандмауэр для тестирования приложения, не забудьте снова включить его после теста. Если проблема была в брандмауэре, лучше всего создать правило исключения, а не полностью отключать функцию безопасности.

### ***Как защитить устройство от вредоносного кода***

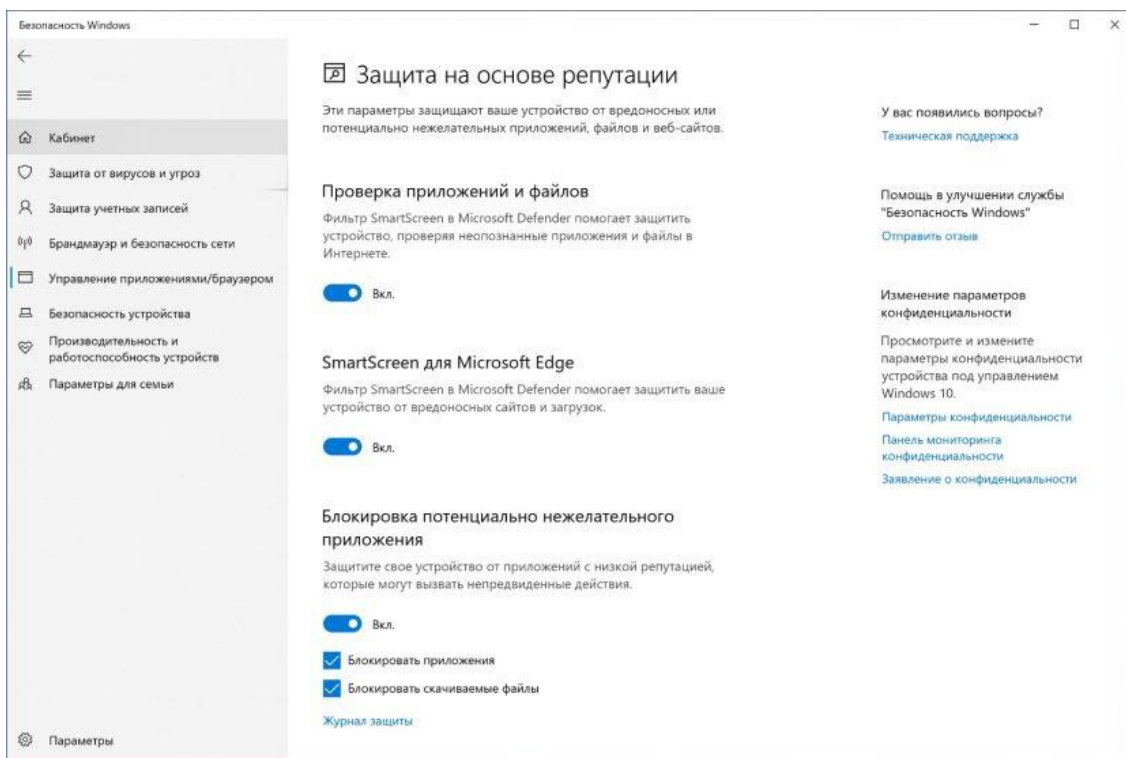
На странице «Управление приложениями/браузером» можно настроить защиту приложений и параметры безопасности в интернете, которые помогут защитить компьютер от сайтов, приложений и файлов с вредоносным кодом.

Параметры по умолчанию — это рекомендуемая конфигурация, которую вы должны использовать (их можно изменить в любой момент).

### ***Защита репутации***

Чтобы защитить устройство с помощью защиты на основе репутации, выполните следующие действия:

1. Откройте **Безопасность Windows**.
2. Щёлкните **Управление приложениями и браузером**.
3. Выберите **Параметры защиты на основе репутации**.
4. Включите или выключите нужные параметры в соответствии с вашими предпочтениями.



Доступны несколько вариантов:

- **Проверять приложения и файлы** — защита от нераспознанных приложений и файлов из Интернета.
- **SmartScreen для Microsoft Edge** — защищает устройство от вредоносных загрузок и сайтов.
- **Блокировка потенциально нежелательных приложений** блокирует приложения с низкой репутацией.
- **SmartScreen для приложений Microsoft Store** — проверяет веб-контент, который используют приложения из магазина Microsoft Store.

**Примечание:** Windows 10 по умолчанию имеет оптимальные настройки этой функции. Вы можете выборочно включать или отключать их в зависимости от личных предпочтений.

После выполнения этих действий антивирус Microsoft Defender защитит ваше устройство от нежелательных приложений, файлов и сайтов.

### Изолированный просмотр

Изолированный просмотр — это возможность редакций Windows 10 Pro, Education и Enterprise, которая разработана для изоляции браузера Microsoft

Edge на аппаратном уровне, чтобы защитить устройство и данные от вредоносных программ или атак нулевого дня.

Если этот параметр доступен, вы можете получить доступ к его настройкам в Защитнике Microsoft, выполнив следующие действия:

1. Щёлкните **Управление приложениями и браузером**.
2. Щёлкните параметр **Изменить параметры Application Guard**.

Если вы используете поддерживаемую версию Windows 10, то сможете получить доступ к настройкам, если компонент «Microsoft Defender Application Guard» включён с помощью функции «Включение или отключение компонентов Windows».

Выполнив эти шаги, вы можете начать новый сеанс безопасного просмотра, открыв новый браузер Microsoft Edge на базе движка Chromium, нажав кнопку главного меню (трехточечную) и выбрав параметр **«Новое окно Application Guard»**.

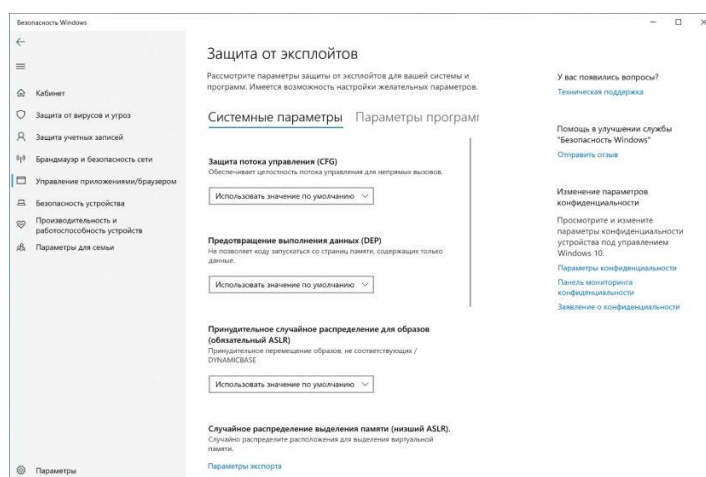
### **Защита от эксплойтов**

Защита от эксплойтов — это расширенная функция, которая может помочь уменьшить количество вредоносных программ и уязвимостей.

Windows 10 включает наиболее оптимальные настройки для защиты от эксплойтов. Не следует вносить какие-либо изменения в них, если вы не знаете, что делаете.

Чтобы настроить параметры защиты от эксплойтов, выполните следующие действия:

1. Щёлкните **Управление приложениями и браузером**.
2. Щёлкните параметр **Параметры защиты от эксплойтов**.
3. Выберите вкладку **Системные параметры** и настройте параметры в соответствии с личными предпочтениями.
4. Аналогично настройте вкладку **Параметры программы**.



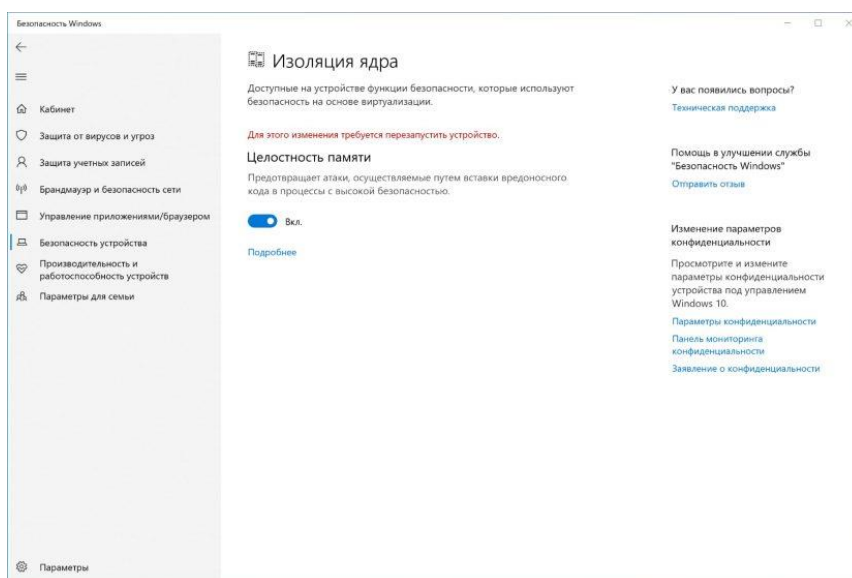
После выполнения этих шагов защита от эксплойтов будет работать на устройстве в соответствии с вашими настройками.

### ***Как включить изоляцию ядра в Windows Security***

Изоляция ядра — это технология виртуализации, которая добавляет дополнительный уровень защиты от сложных атак.

Как правило, не нужно беспокоиться об этой функции, но вы можете включить её, выполнив следующие действия:

1. Щёлкните **Безопасность устройства**.
2. Щёлкните параметр **Сведения об изоляции ядра**.
3. Включите ползунок **целостности памяти**.



После выполнения этих действий необходимо перезагрузить компьютер, чтобы изменения вступили в силу.

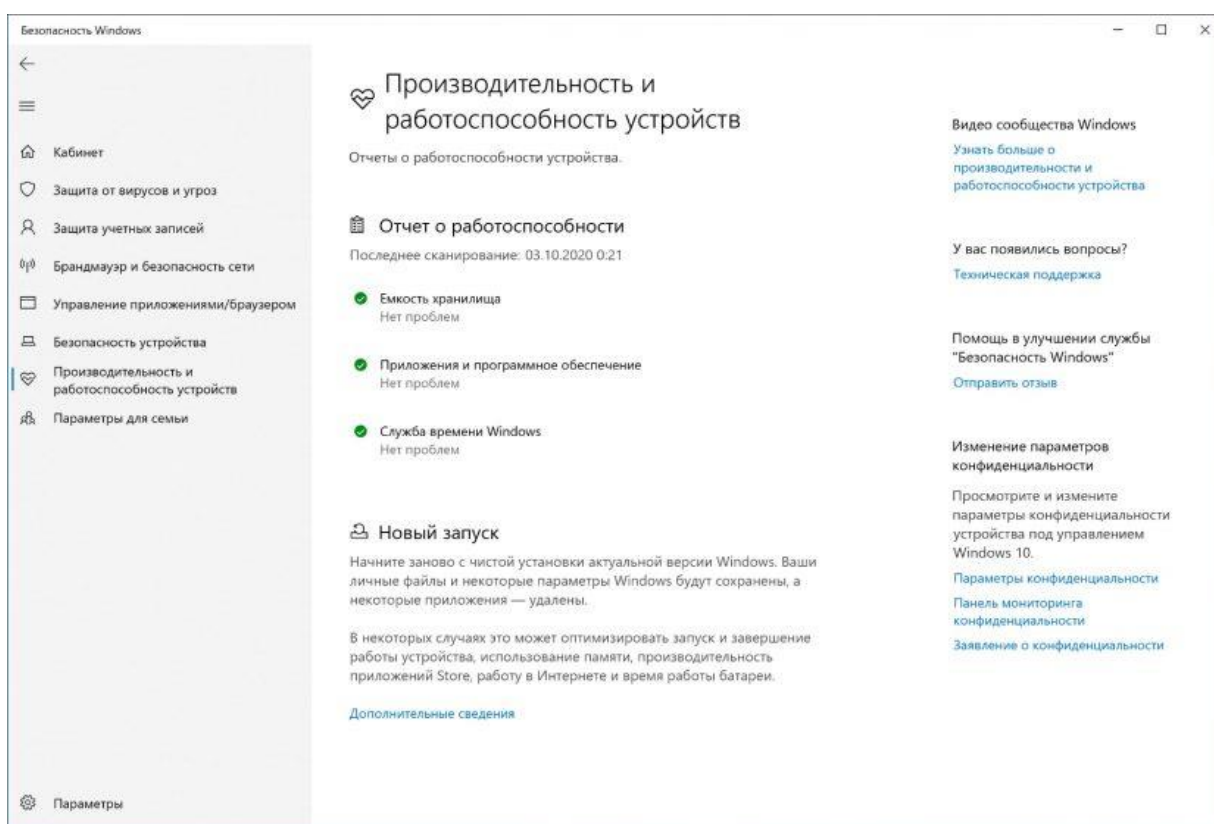
Если вы не видите этот параметр, скорее всего, виртуализация не включена в базовой системе ввода-вывода (BIOS) или унифицированном расширяемом интерфейсе микропрограмм (UEFI).

### ***Как просмотреть отчёт о работоспособности и производительности***

Служба безопасности Windows включает информацию о состоянии и производительности компьютера.

Чтобы просмотреть отчёт о работоспособности и производительности устройства, выполните следующие действия:

#### **1. Щёлкните Производительность и работоспособность устройств.**



В отчёт включены статусы Центра обновления Windows, хранилища, драйвера устройства и аккумулятора. Если необходимо предпринять какие-то действия, вы увидите предупреждение с рекомендациями по устранению проблемы.

Вот значения для каждого возможного состояния статуса:

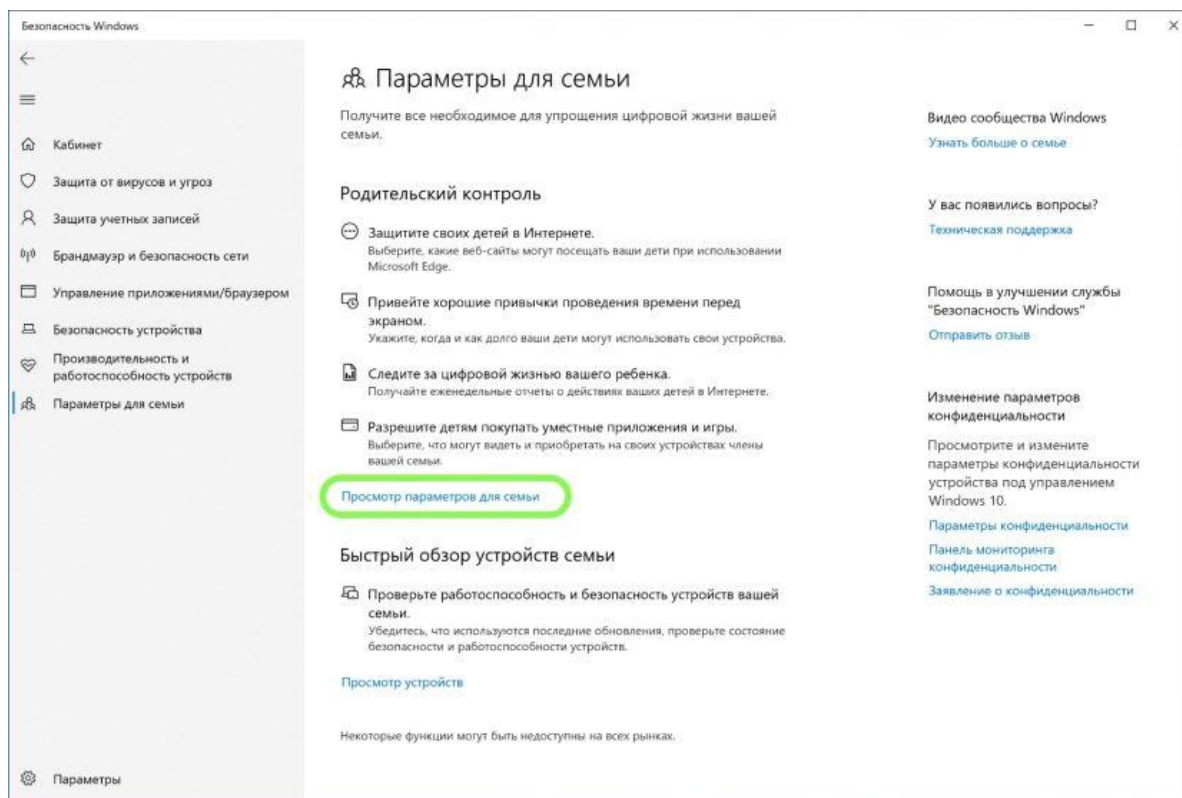
- **Зелёный:** всё работает правильно.
- **Жёлтый:** рекомендация доступна.
- **Красный:** предупреждение, требующее немедленного внимания.

### **Как управлять родительским контролем и отслеживать устройства**

Раздел «Параметры для семьи» — это не то место, где можно управлять какими-либо настройками. Здесь предлагается доступ к учётной записи Microsoft для управления родительским контролем и другими устройствами, подключёнными к учётной записи.

Чтобы получить доступ к семейным параметрам, выполните следующие действия:

1. Щёлкните **Параметры семьи**.
2. В разделе «Родительский контроль» выберите параметр «**Просмотр параметров семьи**», чтобы открыть эти параметры в своей учётной записи Microsoft в Интернете.
3. В разделе «**Быстрый обзор устройств семьи**» выберите «**Просмотр устройств**», чтобы открыть эти настройки в своей учётной записи Microsoft в Интернете.



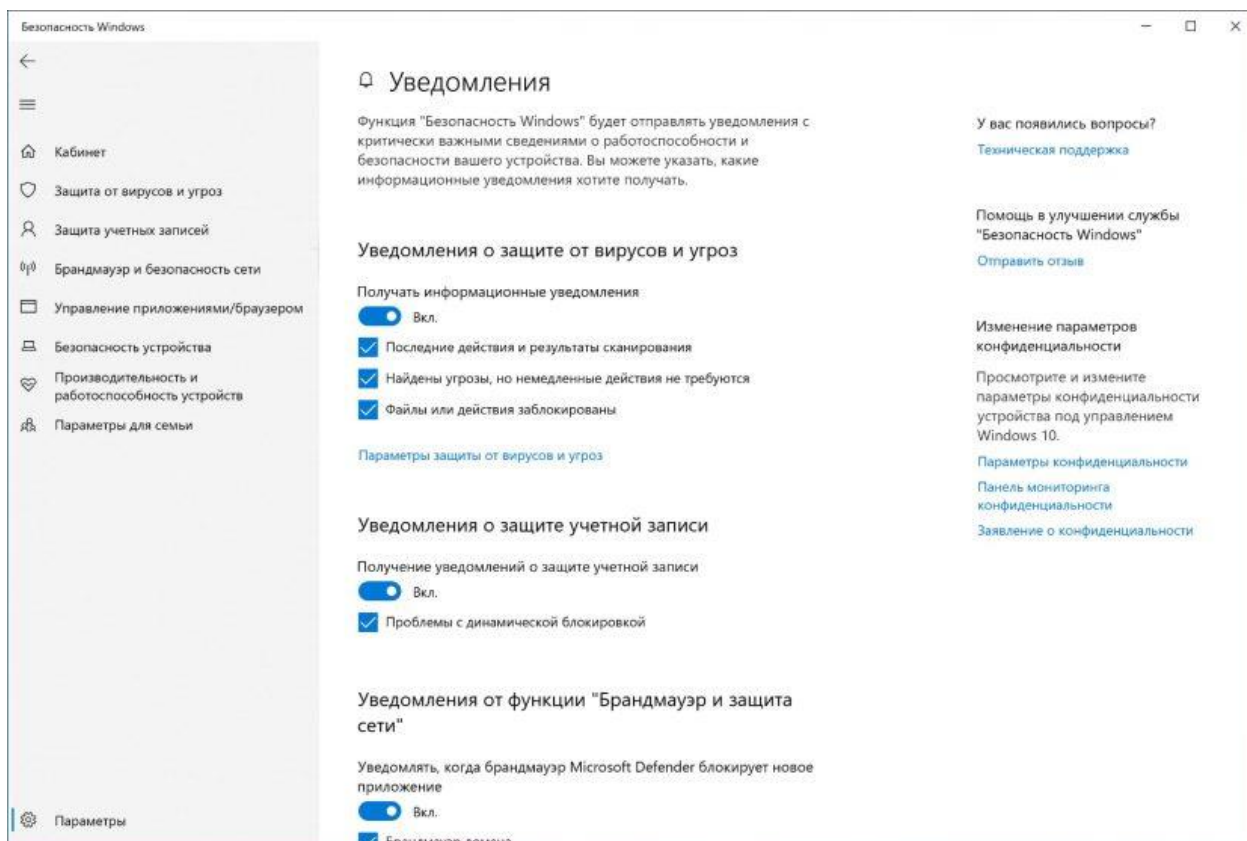
## Настройка уведомлений безопасности Windows

Есть страница настроек, которая позволяет управлять сторонним антивирусом и файрволом, а также настройками уведомлений.



Чтобы отключить уведомления защитника Windows 10, выполните следующие действия:

1. Нажмите кнопку «**Параметры**» в левом нижнем углу окна.
2. В разделе «Уведомления» выберите параметр «**Управление уведомлениями**».
3. Настройте уведомления в соответствии со своими предпочтениями.



После выполнения этих шагов уведомления будут вести себя в соответствии с вашей конфигурацией.

На странице настроек вы также заметите раздел «Обновления системы безопасности», который отображает список установленных сторонних решений безопасности — веб-защита, брандмауэр и антивирус. Здесь нельзя настраивать какие-либо параметры, но можно использовать эту страницу, чтобы открыть настройки в самом приложении.

Подводя итог стоит отметить, что вы можете использовать сторонние решения от популярных компаний, таких как Norton, AVG, Kaspersky, Avast, Bitdefender, но стандартные возможности Windows 10 предлагают хороший



набор инструментов с простым интерфейсом, которые работают быстро и могут конкурировать с любым другим решением.

### **Практическое задание**

1. Настроить защитника Windows на:
  - a) *Быструю проверку на вирусы*
  - b) *Полную проверку на вирусы*
  - c) *Настраиваемое сканирование на вирусы*
  - d) *Проверка на вирусы автономным модулем*
2. Просмотреть журнал защиты
3. Временно отключите антивирус Windows 10
4. Включите защиту от программ-вымогателей
5. Включите или отключите брандмауэр
6. Включите защиту от эксплойтов

### **Отчет**

*Отчет должен содержать:*

7. наименование работы;
8. цель работы;
9. задание;
10. последовательность выполнения работы;
11. ответы на контрольные вопросы;
12. вывод о проделанной работе.

### **Контрольные вопросы**

1. Сколько областей защиты включает Безопасность Windows
2. Как исключить файлы и папки для сканирования
3. Как проверить защиту учётной записи
4. Как управлять сетевой безопасностью с помощью брандмауэра
5. Как защитить устройство от вредоносного кода
6. Защита репутации
7. Защита от эксплойтов

8. Как включить изоляцию ядра в Windows Security
9. Как просмотреть отчёт о работоспособности и производительности
10. Как управлять родительским контролем и отслеживать устройства

## ***Лабораторная работа 2. Установка и предварительная настройка Антивируса Касперского***

**Цель работы:** Изучить системные требования антивируса и сравнить их с параметрами компьютера, установить и провести предварительную настройку Антивируса Касперского

**Оборудование:** учебный персональный компьютер

### **Введение.**

Основа антивирусной защиты компьютера - это использование надежной антивирусной программы. Антивирусные программы бывают разные - от простейших приложений для мобильных телефонов до корпоративных продуктов, обеспечивающие *безопасность* больших гетерогенных сетей. К каждому виду антивирусов, кроме общих надежности и незаметности для пользователя, предъявляются свои требования: в одном случае на первое *место* выдвигается необходимость работать с очень ограниченными системными ресурсами (*мобильный телефон*), в другом - оперировать с огромными базами данных, разрешать удаленное *централизованное управление* и предоставлять подробную статистику о вирусной ситуации в большой сети.

Эта и следующие две лабораторные работы посвящены изучению антивирусной защиты домашнего компьютера. Для такого антивируса важным параметром является наряду с надежностью удобный и понятный любому пользователю *интерфейс*, простота установки и настройки программы. Этими свойствами в полной мере обладает **Антивирус Касперского** (персональная версия), на основе которого и предлагается изучить работу с домашним антивирусом.

В первом задании этой лабораторной работы необходимо будет изучить *системные требования* антивируса и сравнить их с параметрами компьютера, на который он будет устанавливаться. Это обязательная процедура перед установкой любой программы и антивируса в том числе. Второе задание полностью посвящено процедуре инсталляции **Антивируса Касперского**, которая включает в себя непосредственно установку и следующую за ней первоначальную настройку продукта.

### **Подготовка**

Перед началом лабораторной работы убедитесь, что Ваш *компьютер*:

- Включен
- На нем загружена операционная система **Microsoft Windows 7** или **Microsoft Windows 10 Pro**.
- Выполнен вход в систему под учетной записью, обладающей правами администратора

### **Задание 1. Системные требования**

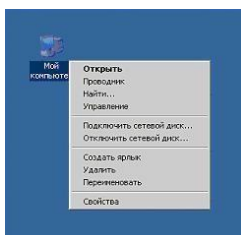
При создании любого приложения программисты дают гарантию, что их продукт будет работать на технике с определенными характеристиками: например, для работы браузера **Internet Explorer** необходимо наличие на компьютере установленной операционной системы семейства **Microsoft Windows**, на **Linux** и любой другой **\*nix** -операционной системе он работать не будет. Это требования к программному обеспечению. Бывают также требования к аппаратному обеспечению - в этом случае постулируется необходимость наличия на компьютере некоторого минимального объема оперативной памяти (если ее меньше, то *программа* будет очень медленно работать или же не запустится вообще), свободного пространства на диске (для размещения всех необходимых в работе приложения файлов), тактовой частоты процессора, от которой зависит *производительность* компьютера и другое.

В случае антивирусных программ часто выдвигается дополнительное требование отсутствия на компьютере другого антивирусного средства, *совместная работа* с которым может вызвать конфликты.

*Системные требования* обычно приводятся в сопровождающем *дистрибутив* текстовом файле и/или в документации к продукту. Также всегда с ними можно ознакомиться на сайте компании-производителя.

В этом задании нужно сравнить *системные требования Антивируса Касперского 6.0* с конфигурацией Вашего компьютера и убедиться, что установка этого приложения возможна.

1. Узнайте версию операционной системы, в которой Вы работаете. Для этого найдите иконку **Мой компьютер**, выведите ее контекстное меню (щелкнув на ней правой кнопкой мыши) и выберите пункт **Свойства**



2. Открывшееся окно **Свойства системы** содержит основные сведения о компьютере и установленной на нем операционной системе. На первой закладке, **Общие**, представлена сводная информация, в том числе название и версия операционной системы. На картинке это **Microsoft Windows 7**. Запомните название и версию Вашей операционной системы
- 3.

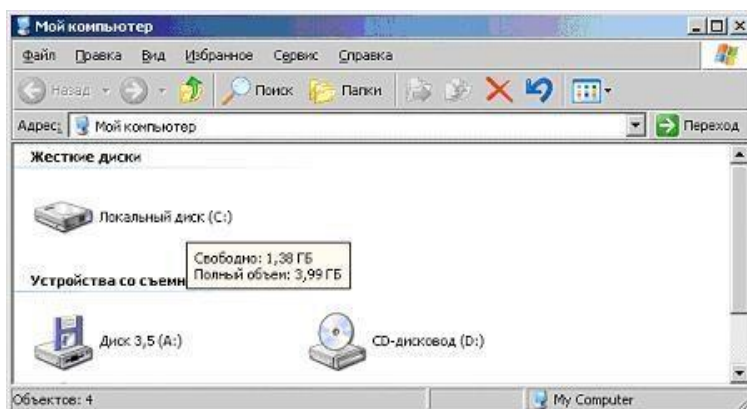


Теперь необходимо найти системные требования, предъявляемые **Антивирусом Касперского** при работе на компьютере под управлением Вашей операционной системы

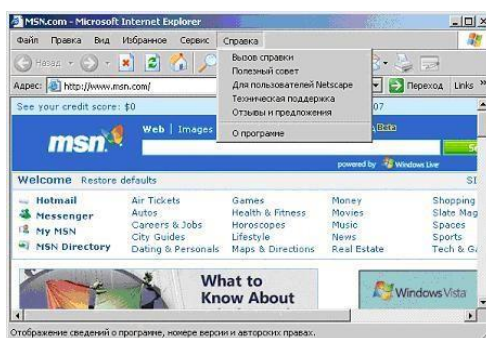
4. Откройте файл с документацией к **Антивирусу Касперского 6.0**, kav6.0ru.pdf.
5. Перейдите к разделу **2.3. Аппаратные и программные требования к системе** и найдите в списке операционных систем Вашу, например, **"Microsoft Windows 7 или 10**. Непосредственно после указания операционной системы будет идти перечень системных требований, предъявляемых к компьютеру с Вашей операционной системой. Соберите воедино все требования, предъявляемые к Вашей системе и заполните столбец "Требования Антивируса Касперского" следующей таблицы:

Параметр	Требования Антивируса Касперского	Параметры системы
Процессор		
Оперативная память		
Свободное место на диске		
Браузер		

6. Далее необходимо убедиться, что конфигурация системы позволяет установить **Антивирус Касперского**. Для этого вернитесь к окну **Свойства системы** (см. пункты 1 и 2 этого задания). В разделе **Компьютер** можно получить информацию и о процессоре, и об объеме оперативной памяти. В примере это Intel(R) Celeron(R) 1,70 ГГц и 192 МБ оперативной памяти. Внесите полученные данные в третий столбец "Параметры системы" таблицы пункта 5
7. Проверьте наличие свободного места на диске. Для этого откройте папку **Мой компьютер** и задержите на пару секунд курсор мыши над иконкой системного диска. В появившемся сообщении будет указан объем свободного пространства на нем и общий объем диска. На рисунке это локальный диск C: общей емкостью 3,99 ГБ, на котором свободно 1,38 ГБ. Занесите полученные Вами данные в общую таблицу в строку "Свободное место на диске"



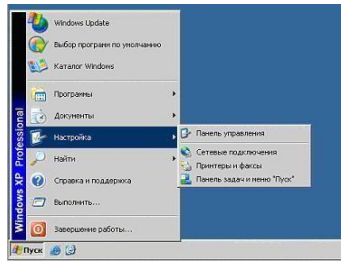
8. Узнайте версию установленного на Вашем компьютере браузера. Браузер **Internet Explorer** встроен в любую операционную систему семейства **Microsoft Windows**, однако версия его может отличаться от требуемой<sup>1</sup>. Запустите браузер, откройте меню **Справка** и выберите пункт **О программе**



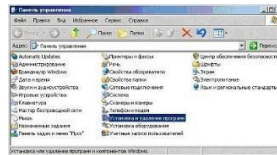
9. В открывшемся окне найдите версию **Internet Explorer**. Внесите это значение в таблицу из пункта 5 (графа "Браузер") и закройте приложение



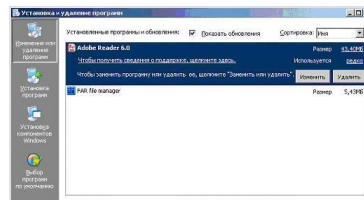
10. Проанализируйте заполненную таблицу и сделайте выводы о возможности установки **Антивируса Касперского 6.0** на Ваш компьютер
11. Далее необходимо ознакомиться со списком установленных на компьютер программ и убедиться, что среди них нет других антивирусов<sup>2</sup>. Для этого вызовите **Панель управления (Пуск / Настройка / Панель управления)**



12. В Панели управления найдите элемент **Установка и удаление программ** и откройте его



13. Ознакомьтесь со списком установленных на компьютере программ и убедитесь, что среди них нет других антивирусов



14. Обратите внимание на системную дату, установленную на Вашем компьютере. Для этого задержите на пару секунд курсор мышки над системным временем в правом нижнем углу экрана. Системная дата должна соответствовать реальной дате, это будет необходимо для корректной активации продукта



На этом подготовительный этап окончен и можно переходить непосредственно к установке.

## Задание 2. Установка

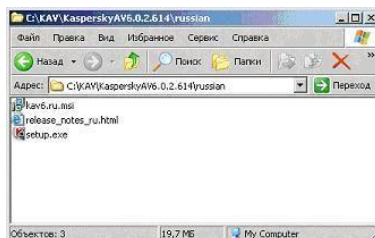
Большинство современных приложений перед запуском необходимо установить. Стандартная процедура установки включает в себя *копирование* необходимых в работе программы файлов на *диск* (в *нужное место*) и регистрацию

в реестре операционной системы. Иногда для завершения установки требуется перезагрузка компьютера.

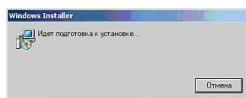
Для успешной установки **Антивируса Касперского** требуется *дистрибутив* и лицензионный *ключ* (файл с расширением. Key, содержащий данные, удостоверяющие легальность приобретенного продукта). Эти файлы обычно записываются на CD и передаются пользователю при покупке. В случае приобретения в Интернет-магазине, *дистрибутив* можно либо загрузить с сайта **Лаборатории Касперского**, либо заказать отправку почтой или курьером на CD, лицензионный *ключ* высылается *по e-mail*.

В этом задании необходимо произвести установку **Антивируса Касперского 6.0**. Для этого нужно запустить **Мастер установки** и проследовать за всеми его указаниями. *По* окончании установки запустится **Мастер настройки**. Он позволяет в режиме диалога с пользователем произвести настройку основных параметров работы антивируса. В большинстве случаев после этой процедуры дополнительная настройка *по* окончании инсталляции не требуется.

1. Откройте папку с дистрибутивом **Антивируса Касперского**. Ее расположение можно узнать у преподавателя<sup>3</sup>



2. Найдите файл **setup.exe** и запустите его<sup>4</sup>

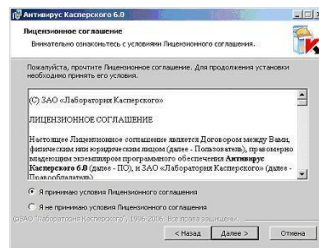


3. Если система удовлетворяет всем необходимым **Антивирусу Касперского** требованиям, запустится **Мастер установки**. В первом окне он поприветствует Вас и сообщит, что собирается сделать. Внимательно прочтите предложенный текст, выполните указание закрыть все сторонние открытые приложения (если таковые имеются) и нажмите кнопку **далее** для перехода к следующему окну **Мастера**

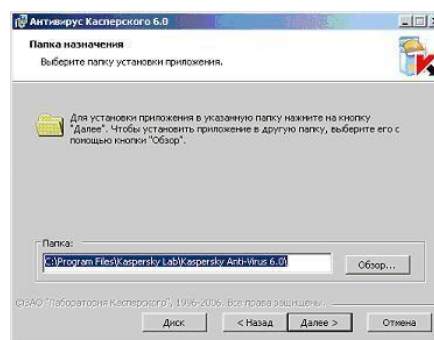




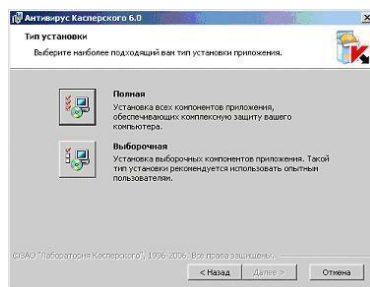
4. На втором шаге Мастера необходимо ознакомиться с Лицензионным соглашением между Вами и **Лабораторией Касперского**, производителем **Антивируса Касперского**. В нем описаны все права и обязанности обеих сторон, в том числе ответственность за нарушение авторских прав и самостоятельное изготовление копий антивируса. Внимательно прочтите его. Установку можно продолжить только, согласившись со всеми положениями, для этого нужно отметить пункт **Я принимаю условия Лицензионного соглашения** и нажать ставшую активной кнопку **Далее**



5. На следующем шаге нужно определить директорию, куда будут скопированы основные системные файлы антивируса. По умолчанию предлагается использовать **C:\Program Files\Kaspersky Lab\Kaspersky Anti-Virus 6.0\**. Если она по каким-то причинам не подходит, с помощью кнопки **Обзор** всегда можно выбрать другую. Для продолжения установки и перехода к следующему окну тут и в дальнейшем используйте кнопку **Далее**



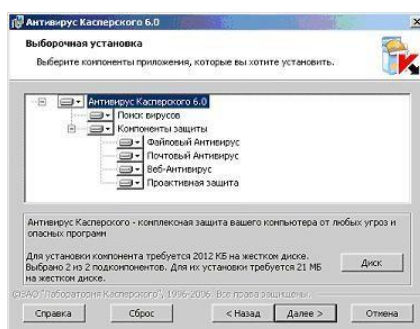
6. Далее нужно выбрать тип установки: полную или выборочную. Полная означает установку всех компонентов **Антивируса Касперского**, а выборочная позволяет некоторые из них отключить. Выберите **Выборочную**, нажав на квадратную кнопку слева от описания этого типа установки



7. Как и было обещано, в следующем окне можно указать какие компоненты **Антивируса Касперского** необходимо установить, а какие пропустить. На рисунке изображен вид этого окна по умолчанию, соответствующий полной установке.

Тут же можно получить краткое описание каждого компонента - для этого необходимо выделить (щелкнуть правой кнопкой мыши) интересующий компонент и внизу окна появится нужная информация. На рисунке выделен **Антивирус Касперского 6.0**, следовательно, внизу показано описание самой программы.

Оставьте установку всех компонентов и продолжите инсталляцию, нажав **Далее**

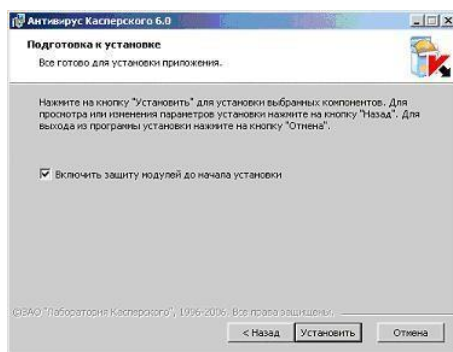


8. Далее **Мастер** проверяет наличие на компьютере других антивирусных программ, полный список которых можно найти в файле `release_notes.txt` в разделе " **Установка** ". Если такие найдутся, то пользователю будет выведе-

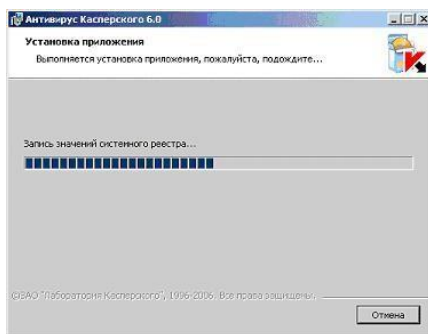
дено соответствующее уведомление с предложением их удалить. Но в нашем случае компьютер чист и этот этап в интерфейсе никак не отображается

9. На следующем этапе нужно подтвердить намерение установить программу, нажав **Установить**. После этого начнется непосредственное копирование файлов и регистрация программы в реестре, и вернуться к предыдущим окнам **Мастера** установки будет невозможно.

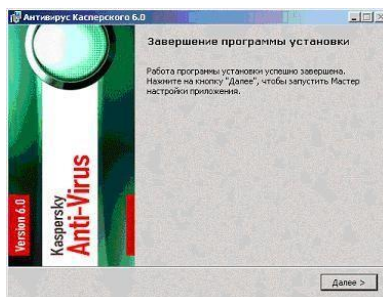
Расположенный в центре окна флаг **включить защиту модулей до начала установки** рекомендуется оставить включенным. Но в дальнейшем, при повторной инсталляции этой же версии **Антивируса Касперского** его следует очищать. Он отвечает за сохранность сделанных вовремя установки настроек, они могут потребоваться в дальнейшем для восстановления **Антивируса Касперского** в случае повреждения его программных модулей



10. Нажмите кнопку **Установить** и проследите за действиями **Мастера**. Они описываются непосредственно над индикатором процесса установки



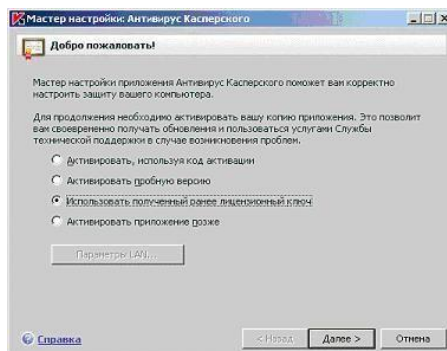
11. По окончании инсталляции **Мастер установки** выводит информационное окно. Вам необходимо ознакомиться с расположенным в нем текстом и запустить **Мастер настройки** приложения. Для этого нажмите **Далее**



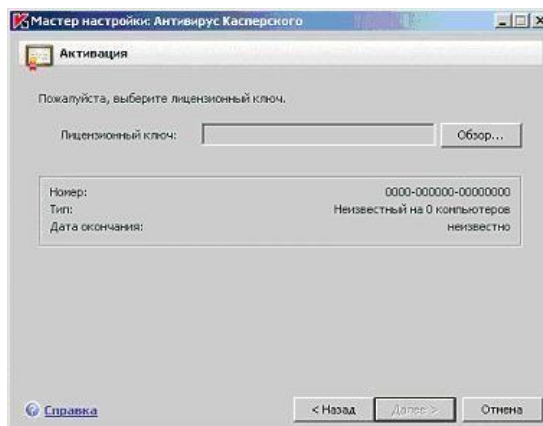
12. На первом этапе настройки нужно активировать приложение. Это можно сделать одним из четырех предложенных вариантов:

- Используя код активации, коммерческий или пробный. Такой код может быть выдан при покупке через Интернет, в этом случае активация происходит также через Интернет
- Активировать используя полученный ранее ключевой файл - именно этот способ будет использован в этой лабораторной работе
- Активировать позже - если ключевого файла нет, то можно установить антивирус в пробном режиме, но в этом случае не будет доступно обновление антивирусных баз и, следовательно, надежную защиту получить не получится

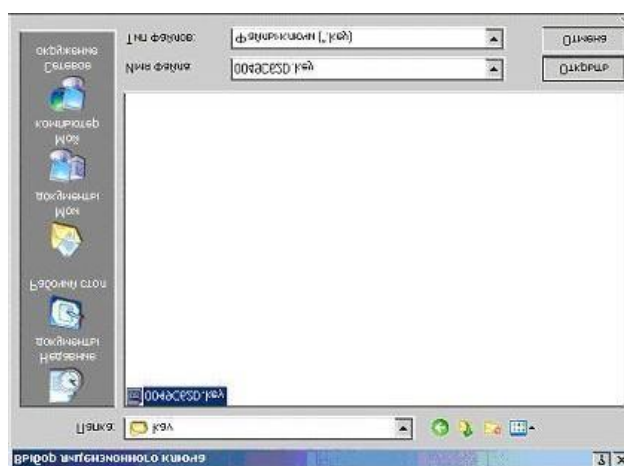
Выберите вариант **использовать полученный ранее лицензионный ключ** и нажмите **Далее**



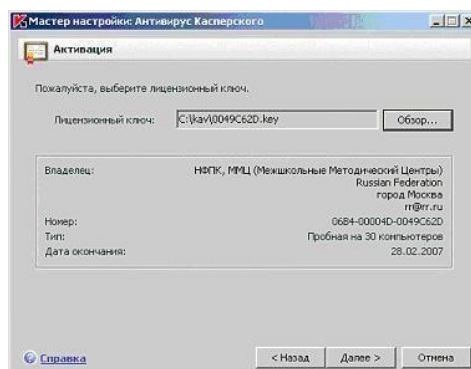
13. В следующем окне нужно указать путь к лицензионному файлу. Для этого нажмите кнопку **Обзор**



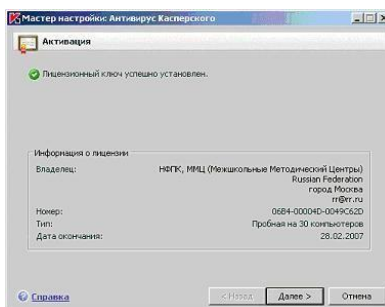
14. Перейдите к указанной преподавателем папке с ключевым файлом, выделите его и нажмите **Открыть**



15. После открытия выбранного файла, в окне **Мастера** появится информация о нем. Ознакомьтесь с ней и нажмите **Далее**



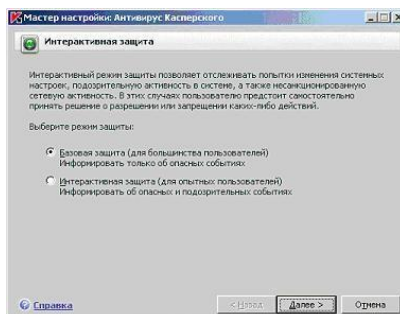
16. На этапе перехода к следующему окну проводится проверка открытого лицензионного ключа. Если он действителен, то происходит его активация. Для продолжения настройки нажмите **Далее**



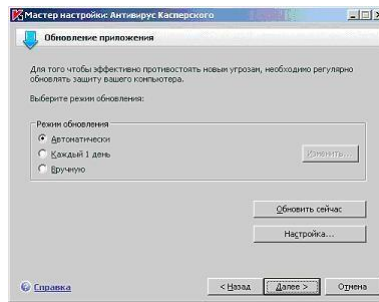
17. После активации начинается этап первоначальной настройки антивируса.

**Мастер установки** предлагает настроить только основные параметры работы приложения и все сделанные в ходе инсталляции настройки впоследствии можно будет легко изменить с помощью графического интерфейса.

Первое окно предлагает выбрать режим интерактивной защиты. Прочитайте описание различий между этими двумя режимами, оставьте выбранную по умолчанию **Базовую защиту** и нажмите **Далее**



18. Далее предлагается определить режим обновления, по умолчанию выбран пункт **Автоматически**. Он подходит для большинства пользователей. В этой лабораторной работе оставьте все настройки по умолчанию, поскольку задача обновления антивирусных баз будет подробно рассмотрена в одной из следующих лабораторных работ. Однако нужно знать, что в общем случае настроить и обновить антивирусные баз можно уже прямо в ходе установки (для этого предназначены кнопки **Настройка** и **Обновить сейчас** и меню выбора режима обновления)



19. В следующем окне можно задать настройки и расписание запуска проверки на наличие вирусов объектов автозапуска, критических областей и полной проверки компьютера.

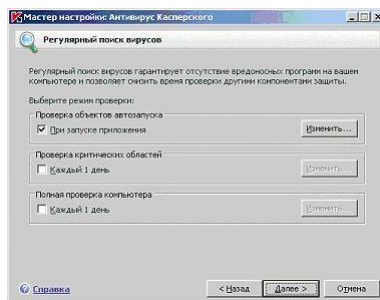
Для большинства пользователей рекомендуется настроить проверку объектов автозапуска (как наиболее часто поражаемой области компьютера) при каждой перезагрузке **Антивируса Касперского**. Это обычно соответствует каждой перезагрузке компьютера.

Под проверкой критических областей подразумевается поиск вирусов в важных системных областях. По умолчанию это системная память, объекты автозапуска, загрузочные секторы дисков и папки C:\Windows и C:\Windows\system32.

Полную проверку компьютера рекомендуется проводить раз в неделю. Однако поскольку она требует несколько больше системных ресурсов и соответственно может снижать общую производительность компьютера, оптимального расписания для всех пользователей нет. Поэтому если при установке на домашний компьютер Вы заранее знаете, что в определенный день и час полная проверка не будет мешать Вашей работе, то можете смело отмечать флаг **Каждый 1 день** в поле **Полная проверка компьютера** и с помощью размещенной рядом и ставшей активной кнопки **Изменить** устанавливать расписание - например, каждую пятницу в 20:00. Иначе необходимо помнить о важности регулярной полной проверки и запускать ее вручную, но опять же, не реже раза в неделю. В этой лабораторной работе оставьте отмеченным только флаг проверки объектов автозапуска

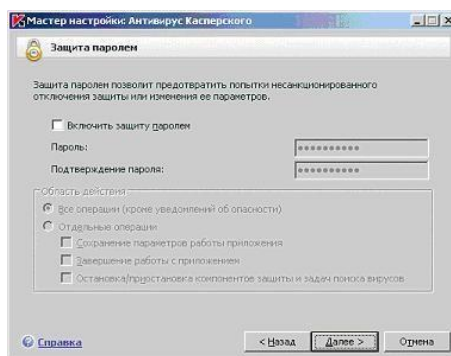
и нажмите **Далее**





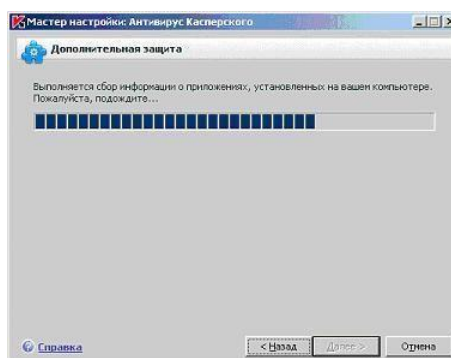
20. **Антивирус Касперского** позволяет поставить защиту паролем на ряд операций: изменения настроек, выгрузки антивируса или остановки работы компонентов и задач поиска вирусов. Если такая защита установлена, то при попытке совершить защищенную операцию будет предложено ввести пароль. Это может быть полезно, если компьютер используется несколькими пользователями и кому-то из них нельзя доверять.

В этой лабораторной работе устанавливать пароли не нужно, поэтому оставьте флаг **Включить защиту паролем** пустым и нажмите **Далее**



21. На последнем этапе **Мастер настройки** проводит анализ Вашей системы и собирает данные об установленных программах. В дальнейшем эта информация пригодится для контроля целостности приложений, дополнительного компонента антивирусной защиты.

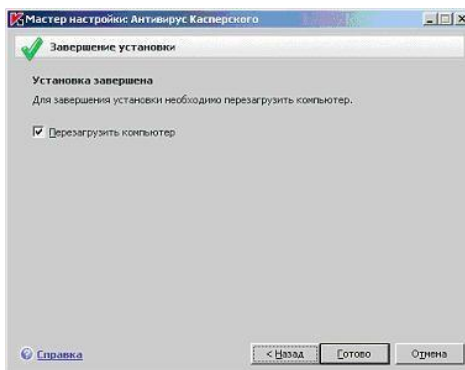
Дождитесь окончания сбора сведений о системе





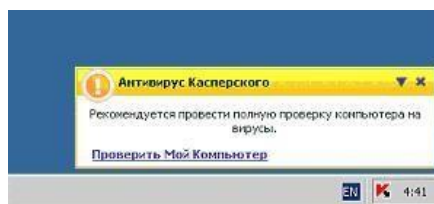
22. Следующее окно информирует, что установка завершена, но требует перезагрузки. Без перезагрузки установка **Антивируса Касперского** не может считаться завершенной. Поэтому убирать отметку с флага **Перезагрузить компьютер** можно только в исключительных случаях. В данном случае это не требуется.

Оставьте отмеченным флаг **Перезагрузить компьютер** и нажмите **Готово**



23. Дождитесь завершения перезагрузки компьютера и войдите в систему под своей учетной записью

24. Обратите внимание, что после перезагрузки в правом нижнем углу экрана появилось сообщение о необходимости провести полную проверку компьютера на вирусы. О том, как настраивать такие уведомления, пойдет речь в одной из следующих лабораторных работ



## Заключение

Эта лабораторная работа заканчивается полной установкой, включающей в себя предварительную настройку **Антивируса Касперского 6.0**. Если в ходе инсталляции **Мастер установки** не выводил сообщений об ошибках, она должна быть успешной. Однако на основе только этого нельзя судить об эффективности антивирусной защиты. Последним этапом установки любой программы является тестирование ее работы. Для **Антивируса Касперского** это проверка установки всех его компонентов и *диагностика* эффективности антивирусной защиты.

## *Лабораторная работа № 3. Профилактика проникновения вредоносного программного обеспечения*

**Цель:** практическое освоение студентами научно-теоретических положений дисциплины по вопросам защиты информации от воздействия вредоносного программного обеспечения на основе использования методов и средств профилактики вирусных атак, а также овладение ими техникой экспериментальных исследований и анализа полученных результатов, привитие навыков работы с вычислительной техникой.

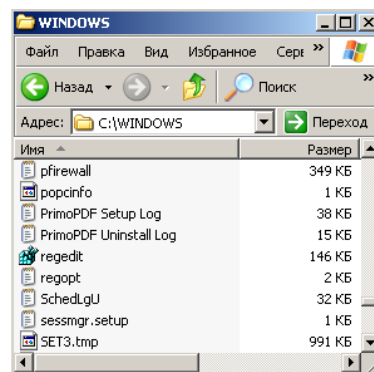
### **Часть № 1**

*Профилактика проникновения вредоносного программного обеспечения посредством исследования Реестра ОС Windows 7/10*

Краткие теоретические сведения

**Реестр операционной системы Windows** - это большая база данных, где хранится информация о конфигурации системы. Этой информацией пользуются как операционная система Windows, так и другие программы. В некоторых случаях восстановить работоспособность системы после сбоя можно, загрузив работоспособную версию реестра, но для этого, естественно, необходимо иметь копию реестра. Основным средством для просмотра и редактирования записей реестра служит специализированная утилита «**Редактор реестра**».

Файл редактора реестра находится в папке Windows. Называется он **regedit.exe**.



После запуска появится окно редактора реестра. Вы увидите список из 5

разделов (рисунок 1):

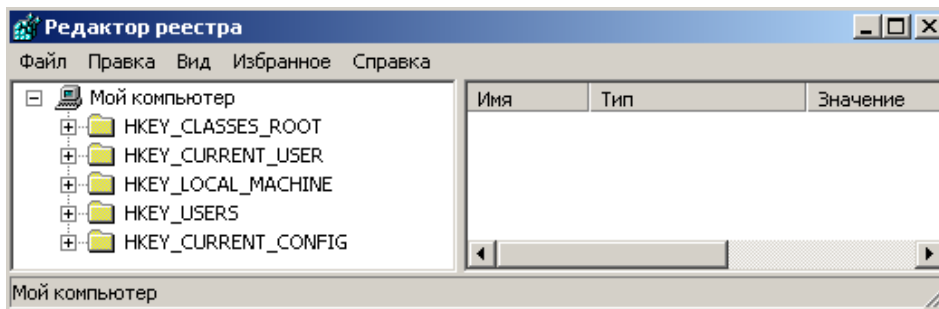


Рисунок 1 – Разделы реестра

HKEY\_CLASSES\_ROOT.

HKEY\_CURRENT\_USER.

HKEY\_LOCAL\_MACHINE.

HKEY\_USERS.

HKEY\_CURRENT\_CONFIG.

Работа с разделами реестра аналогична работе с папками в Проводнике. Конечным элементом дерева реестра являются ключи или параметры, делящиеся на три типа (рис. 2):

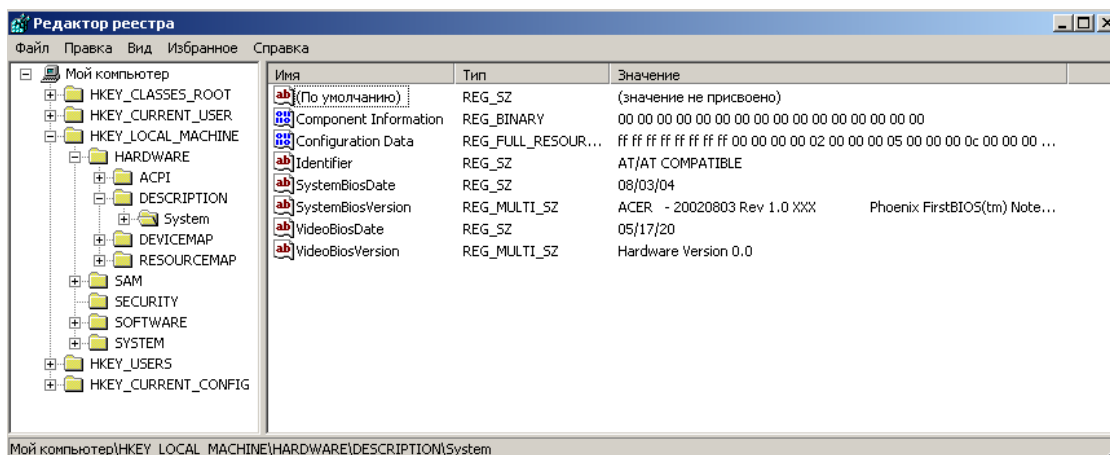


Рисунок 2 – Работа с разделами реестра

- строковые (напр. «C:\Windows»);
- двоичные (напр. 10 82 AO 8F);
- **DWORD** - этот тип ключа занимает 4 байта и отображается в шестнадцатеричном и в десятичном виде (например, 0x00000020 (32)).

В Windows системная информация разбита на так называемые ульи (*hive*). Это обусловлено принципиальным отличием концепции безопасности этих

операционных систем. Имена файлов ульев и пути к каталогам, в которых они хранятся, расположены в разделе

**HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\hivelist** (рис.3).

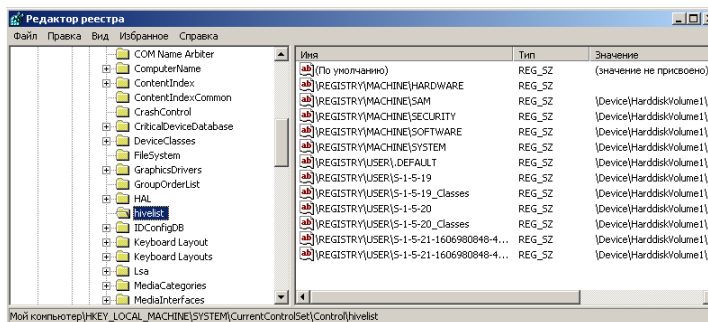


Рисунок 3 – Раздел реестра HKEY\_LOCAL\_MACHINE

В таблице 1 даны краткие описания ульев реестра и файлов, в которых хранятся параметры безопасности.

Таблица 1 Характеристика основных разделов системного Реестра

HKEY_LOCAL_MACHINE\SAM	Содержит информацию SAM (Security Access Manager), хранящуюся в файлах SAM, SAM.LOG, SAM.SAV в папке %System-root%\System32\Config
HKEY_LOCAL_MACHINE\SECURITY	Содержит информацию безопасности в файлах SECURITY.SECURITY.LOG, SECURITY.SAV в папке %Systemroot%\System32\Config
HKEY_LOCAL_MACHINE\SYSTEM	Содержит информацию об аппаратных профилях этого подраздела. Информация хранится в файлах SYSTEM.SYSTEM.LOG, SYSTEM.SAV в папке %Systemroot%\System32\Config
HKEY_CURRENT_CONFIG	Содержит информацию о подразделе System этого улья, которая хранится в файлах SYSTEM.SAV и SYSTEM.ALT в папке %Systemroot%\System32\Config
HKEY_USERS\DEFAULT	Содержит информацию, которая будет использоваться для создания профиля нового пользователя, впервые регистрирующегося в системе. Информация хранится в файлах DEFAULT, DEFAULT.LOG, DEFAULT.SAV в папке %Systemroot%\System32\Config
HKEY_CURRENT_USER	Содержит информацию о пользователе, зарегистрированном в системе на текущий момент. Эта информация хранится в файлах NTUSER.DAT и -NTUSER.DAT.LOG, расположенных в каталоге %Systemroot%\Profiles\User name, где User name — имя пользователя, зарегистрированного в системе на данный момент

Проверить потенциальные места записей вредоносного программного обеспечения в системном реестре операционной системы Windows 7/8/10.

### *Алгоритм выполнения работы*

Потенциальными местами записей «троянских программ» в системном

реестре являются разделы, описывающие программы, запускаемые автоматически при загрузке операционной системы от имени пользователей и системы.

1. Запустите программу **regedit.exe**.

2. В открывшемся окне выберите ветвь

**HKEY\_LOCAL\_MACHINE** и далее

Software\ Microsoft\WindowsNT\CurrentVersion\Winlogon.

3. В правой половине открытого окна программы **regedit.exe** появится список ключей.

4. Найдите ключ **Userinit (REG\_SZ)** и проверьте его содержимое.

5. По умолчанию (исходное состояние) 151 этот ключ содержит следующую запись

C:\WINDOWS\system32\userinit.exe (рис. 4).

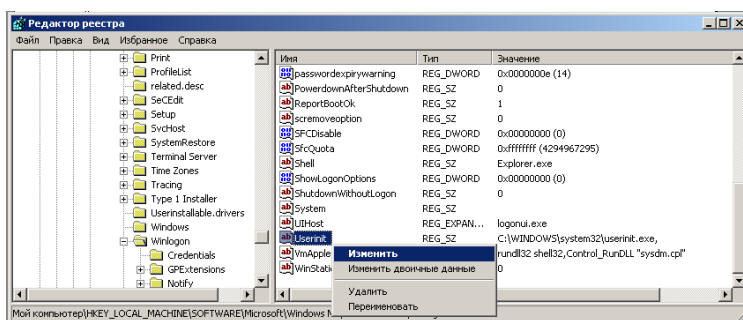


Рисунок 4 – ключ Userinit

6. Если в указанном ключе содержатся дополнительные записи, то это могут быть

«троянские программы».

7. В этом случае проанализируйте место расположения программы, обратив внимание на время создания файла и сопоставьте с Вашими действиями в это время.

8. Если время создания файла совпадает со временем Вашей работы в Интернете, то возможно, что в это время Ваш компьютер был заражен «троянским конем».

9. Для удаления этой записи необходимо дважды щелкнуть на названии ключа (или при выделенном ключе выбрать команду **Изменить** из меню **Правка** программы **regedit.exe**).

10. В открывшемся окне в поле **Значение**(рис. 5)удалите ссылку на подозрительный файл.

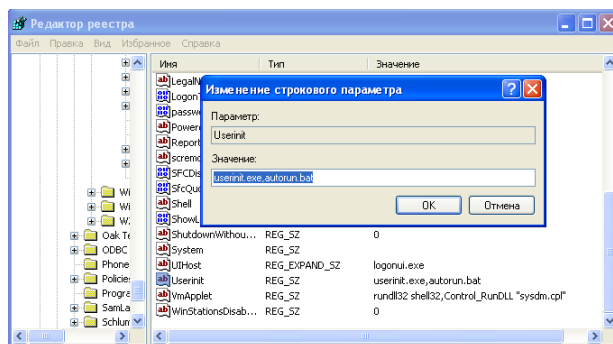


Рисунок 5 – Изменение строкового параметра

11. Закройте программу **regedit.exe**.
12. Перейдите в папку с подозрительным файлом и удалите его.
13. Перезагрузите операционную систему и выполните пункты задания 1-4.
14. Если содержимое рассматриваемого ключа не изменилось, то предполагаемый «троянский конь» удален из Вашей системы.

Еще одним потенциальным местом записей на запуск «троянских программ» является *раздел автозапуска Run*.

Для его проверки выполните следующее.

1. Запустите программу **regedit.exe**.
2. В открывшемся окне выберите ветвь **HKEY\_LOCAL\_MACHINE** и далее  
Software\Microsoft\Windows\CurrentVersion\Run\... (REG\_SZ) (рис. 6).

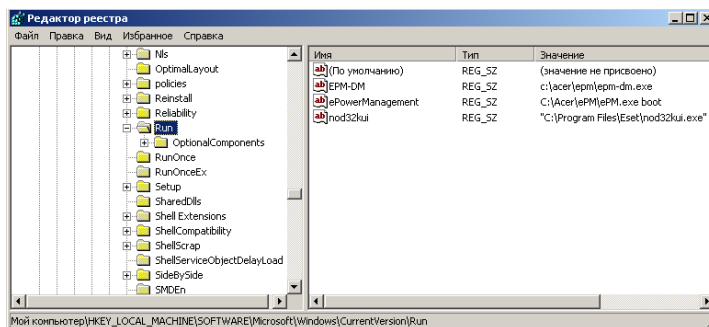


Рисунок 6 – Ветвь HKLM\ Software\Microsoft\Windows\CurrentVersion\Run\

3. В рассматриваемом примере автоматически запускается резидентный антивирус (nod32kui), а также утилита, относящаяся к программе контроля со-

стояния электропитания и заряда батареи (EPM-DM и ePowerManagement) .

4. Если в указанном разделе есть записи вызывающие подозрения, то выполните пункты 6-14 предыдущего задания.

## **Часть № 2**

*Профилактика проникновения вредоносного программного обеспечения посредством исследования организации защиты от макровирусов средствами MicrosoftWord (для Office)*

Краткие теоретические сведения

**Макрос** - макрокоманда или набор макрокоманд, используемый для автоматического выполнения некоторых операций. Макросы записываются на языке программирования Visual Basic для приложений.

**Макровирус** – вредоносная программа, прописанная в макросе.

**Цифровая подпись макроса.** Специально созданный фрагмент макроса, подтверждающий его подлинность и безопасность. Наличие цифровой подписи подтверждает, что макрос или документ был получен от владельца подписи и не был изменен.

**Цифровой сертификат** - вложение в файл, проект макроса или сообщение электронной почты, подтверждающее его подлинность, обеспечивающее шифрование или предоставляющее поддающуюся проверке подпись. Для цифрового подписания проектов макросов необходимо установить цифровой сертификат.

Макровирусы используют возможности макроязыков, встроенных в системы обработки данных (текстовые редакторы, электронные таблицы и т.д.).

*Для существования вирусов в конкретной системе* необходимо наличие встроенного в систему макроязыка со следующими возможностями:

- 1) привязка программы на макроязыке к конкретному файлу;
- 2) копирование макропрограмм (далее макросов) из одного файла в другой;

3) возможность получения управления макросом без вмешательства пользователя (автоматические или стандартные макросы).

Данным условиям удовлетворяют редакторы Microsoft Word и AmiPro, а также редактор электронных таблиц Excel. Эти системы содержат в себе макроязыки (Word - Word Basic, Excel - Visual Basic). В этих системах вирусы получают управление при открытии или закрытии зараженного файла, перехватывают стандартные файловые функции и затем заражают файлы, к которым каким-либо образом идет обращение.

Макровирусы активны не только в момент открытия/закрытия файла, но до тех пор, пока активен сам редактор.

В текстовом процессоре Microsoft Word определены, например, макросы, которые автоматически получают управление при вызове пользователем одной из стандартных команд — FileSave (Файл | Сохранить), FileSaveAs (Файл | Сохранить как), ToolsMacro (Сервис | Макрос | Макросы), ToolsCustomize (Сервис | Настройка) и т.д.

Документ Microsoft Office может также содержать макросы, автоматическиполучающие управление при нажатии пользователем определенной комбинации клавиш на клавиатуре или достижении некоторого момента времени (даты, времени суток).

Так как макровирусы распространяются под управлением прикладных программ, то этот факт делает их независимыми от операционной системы.

Наилучшим способом защиты от вредоносных макросов (макровирусов) в дополнение к административным мерам необходимо приобрести и установить специальное антивирусное программное обеспечение.

### **Исследовать порядок формирования политики защиты от макровирусов приложения Microsoft Word**

Алгоритм выполнения работы

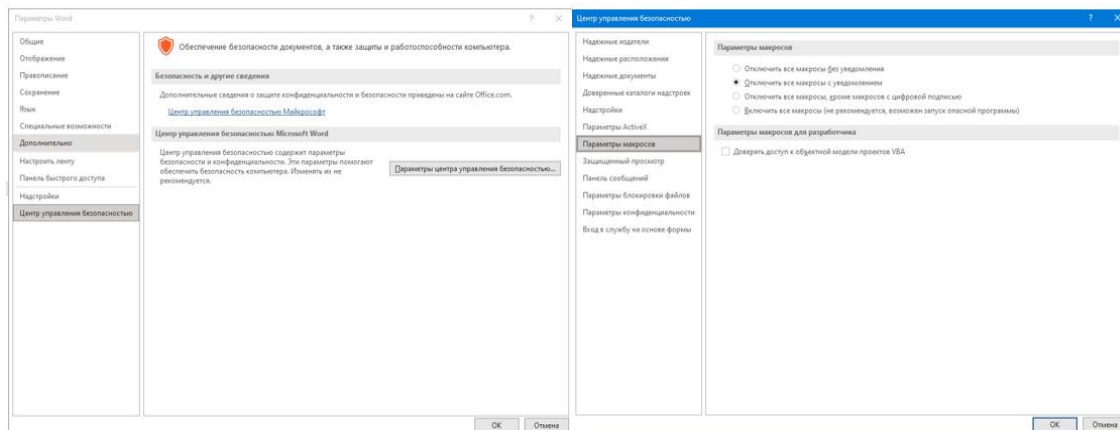
Запустите приложение Microsoft Word из пакета Microsoft Office.

Произвести настройку уровня безопасности при отработке макросов

1. В меню **Файл** выбрать команду **Параметры**.



## 2. Открыть вкладку **Центр управления Безопасностью**.



3. В группе **Параметры макросов** выбрать **отключить все макросы с уведомлением**.

4. Если снять флажок (5) «*Доверять доступ к объектам модели VBA*», то при запуске приложения загрузка всех прописанных в приложении макросов будут сопровождаться предупреждением системы безопасности. Данный шаг может производиться опытными пользователями при анализе причин неустойчивой работы приложения.

**В отчете отразить следующее:**

1. Сформулировать определение реестра операционной системы.  
Какая утилита применяется для просмотра реестра.
2. Исследовать содержимое ключа **Registered Organization** из каталога `HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion`
3. Дать определение вируса, макровируса. Сформулировать условия существования вирусов в конкретной системе.
4. Исследовать порядок формирования политики защиты от макровирусов при использовании приложения Microsoft Excel (из пакета Office XP) и описать маршрут действий пользователя при установке разрешения запуска только подписанных макросов из надежных источников при этом все неподписанные макросы должны отключаться автоматически.

**Задание**

1. Проверить потенциальные места записей вредоносного программного обеспечения в системном реестре операционной системы Windows 7/8/10.

2. Исследовать порядок формирования политики защиты от макровирусов при использовании приложения Microsoft Word

### Отчет

о выполнении лабораторной работы № \_\_\_\_\_

Тема: профилактика проникновения вредоносного программного обеспечения

<b>Реестр</b> операционной системы Windows представляет собой																			
Основным средством для просмотра и редактирования записей реестра является -																			
5. Исследовав содержимое ключа содержимое ключа <b>Registered Organization</b> из каталога HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\CurrentVersion мы открыли следующую запись в реестре:																			
Макросом называется -																			
Вирусом называется -																			
Существуют следующие условия существования вирусов в конкретной среде																			
Маршрут действий пользователя при установке разрешения запуска только подписанных макросов из надежных источников (при этом все неподписанные макросы отключаться автоматически)																			

Студент (ка) группы	(_____)
	номер группы                  роспись                  фамилия

Отметка преподавателя о сдаче лабораторной работы:
--

роспись, дата

## Раздел 5. Информационная безопасность в глобальных сетях

### Лабораторная работа 1. Администрирование Windows 10

**Цель работы:** Целью работы является освоение средств администрирования учётных записей пользователей и групп пользователей в ОС Windows 10, изучение основных параметров, определяющих взаимодействие пользователей с операционной системой, консолью управления и групповой политикой.

#### Краткие теоретические сведения

В операционной системе Windows 10 существует 2 группы пользователей:

- локальные учетные записи;
- учетные записи Microsoft.

Первая группа называется локальной, по причине того, что аутентификация происходит на локальном компьютере. Все учетные данные необходимые для этого (имя пользователя, пароль и параметры учетной записи) хранятся в нем.

В случае работы с учетной записью Microsoft — аутентификация пользователей происходит на сервере сети, то есть удаленно. Преимущество данного способа в том, что любой сотрудник предприятия может зайти в сеть с любого компьютера, а не только с закрепленного за ним. Сервер хранит все параметры пользователя, а также при необходимости и документы, с которыми он работает. Однако второй тип пользователей имеет свой недостаток - при отсутствии Интернет-соединения или коммутируемом (не устанавливаемом автоматически) соединении аутентификация будет невозможна.

Локальные учетные записи бывают трех видов:

- учетная запись администратора, создаваемая при установке системы и используемая при изменении параметров системы;
- учетная запись пользователя, позволяющая использовать установленные администратором из внешних источников программы и изменять параметры персонализации;
- гостевая учетная запись.

Консоль управления Microsoft Management Console (MMC) - это компонент операционных систем семейства Windows NT, предоставляющий администраторам графический интерфейс для настройки системных приложений и прикладных программ.

Оснастка - компонент для MMC, включающий набор параметров какого-либо модуля операционной системы (файловой системы, управления пользователями и т.д.) или прикладного приложения.

Набор параметров для прикладных программ может быть добавлен в оснастку при помощи административных шаблонов - особым образом структурированных файлов с расширением \*.adm.

Групповая политика - это набор правил или настроек, в соответствии с которыми производится настройка рабочей среды Windows.

#### Ход работы

Управление учётными записями локальных пользователей

Рассмотрите механизм работы с учетными записями пользователей, предлагаемых Windows 10. Для этого через меню «Пуск» перейдите к параметрам системы (рис. 1).

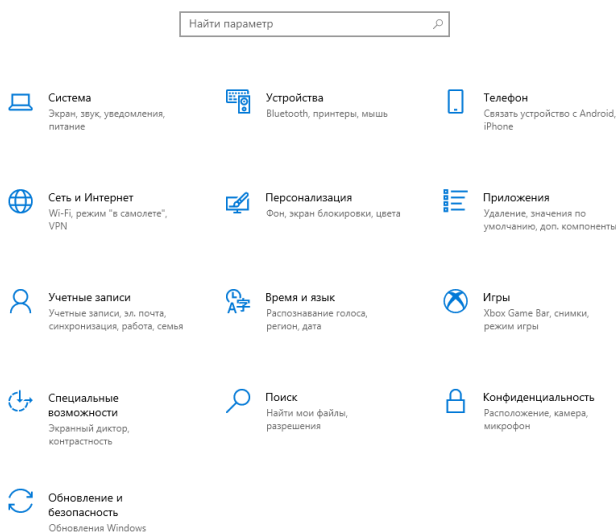


Рисунок 1 – Параметры Windows

Перейдите в раздел «Учётные записи». В данном разделе будет представлена информация о том, под какой учетной записью был осуществлен вход, представлены функции по изменению параметров входа, представлены учетные записи на данном компьютере (если таковые имеются) и предложено создать новых пользователей (рис. 2).

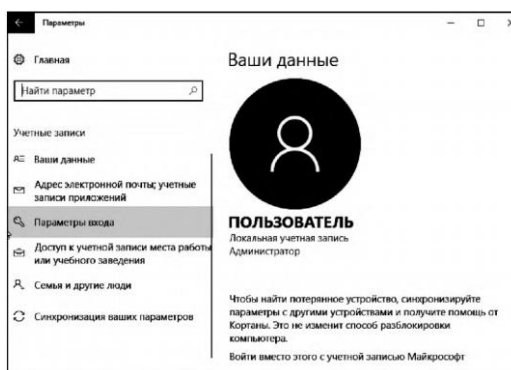


Рисунок 2. – Вкладка управления пользователями

Перейдите во вкладку «Семья и другие люди», нажмите на «Добавить нового пользователя для этого компьютера». В результате поступит предложение ввести электронный адрес или номер телефона для авторизации. Чтобы добавить локального пользователя нажмите на «У меня нет данных для данного человека» (рис. 3).

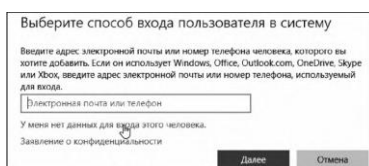


Рисунок 3 – Выбор способа входа в систему

Потом кликните по надписи: «Добавить пользователя без учётной записи» (рис. 4).

Создать учетную запись Майкрософт

Windows, Office, Outlook.com, OneDrive, Skype, Xbox — все они станут более удобными и персональными, если вы войдете в учетную запись Майкрософт \*.  
Дополнительные сведения

proverka@example.com

Получить новый адрес электронной почты

Пароль

Россия

\* Если вы уже используете службу Майкрософт, вернитесь на страницу входа и войдите в эту учетную запись.

Добавить пользователя без учетной записи Майкрософт

Далее Назад

Рисунок 4 – Добавление локального пользователя

После этого потребуется задать имя пользователя и пароль для него, а также подсказку для пароля. После завершения создания пользователя - соответствующая запись появится в перечне учетных записей на данном компьютере.

Запустите Microsoft Management Console (mmc) - компонент Windows, позволяющий администрировать систему. Откройте меню «Пуск - Выполнить - mmc». Для добавления необходимого набора оснасток в меню консоли выберите «Файл - Добавить или удалить оснастку». В результате будет предложен перечень, из которого пользователь может выбрать одну или несколько оснасток.

Нажмите «Файл» и перейдите в пункт «Параметры». Здесь можно выбрать режим работы пользователя с этой консолью: авторский режим, предоставляющий пользователю полный доступ ко всем функциям MMC, и пользовательский режим.

Существует три вида пользовательского режима:

- полный доступ (full access) даёт пользователю доступ ко всем командам MMC, но не позволяет добавлять или удалять оснастки, или изменять свойства консоли;

- ограниченный доступ, много окон (Limited Access Multiple Windows) позволяет пользователю осуществлять доступ только к областям дерева консоли, которые отображались при сохранении консоли, а также открывать новые окна;

- ограниченный доступ, одно окно (Limited Access Single Window) работает так же, как многооконный ограниченный доступ с той разницей, что пользователь не может открывать новые окна.

Сохраните консоль в авторском и пользовательских режимах (рис. 5). Выявите отличия работы консоли в различных режимах.

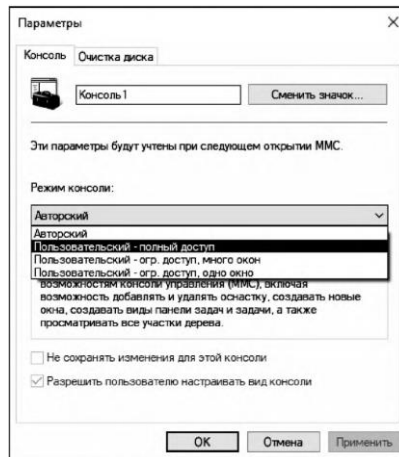


Рисунок 5 – Параметры режима консоли

Через пункт «Добавить или удалить оснастку» добавьте «Локальные пользователи и группы» (рис. 6).

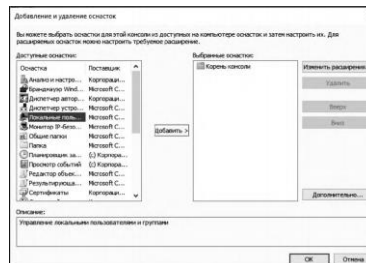


Рисунок 6 – Добавление оснастки

Через данную оснастку также возможно добавить нового пользователя (рис. 7).

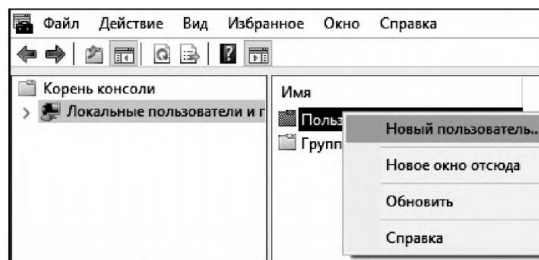


Рисунок 7 – Добавление пользователя через оснастку

В появившемся окне (рис. 8) введите имя учётной записи, а также пароль и его подтверждение. Если администратор устанавливает пользователю временный пароль, то для обязательной смены пароля необходимо включить параметр «Потребовать смену пароля при следующем входе в систему». Сразу после успешной аутентификации пользователь получает запрос на смену пароля, в ответ на который он должен задать новый пароль. Этот подход необходимо использовать в тех случаях, когда администратор системы не должен знать пароли пользователей.

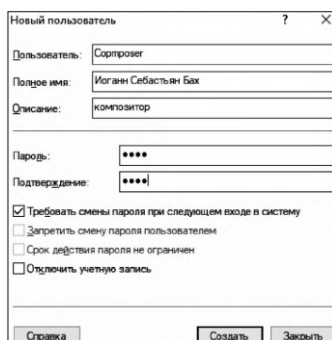


Рисунок 8 – Настройка параметров учётной записи при её создании

Если пользователь забыл свой пароль, то член группы «Администраторы» может сбросить его старый пароль при помощи функции «Задать пароль», доступной в контекстном меню учётной записи этого пользователя (рис. 8). Смените пароль у созданной учётной записи.

В данный момент времени учетная запись «Администратор» является заблокированной (рис. 10). Разблокируйте её, выбрав соответствующий пункт в свойствах учетной записи. Посмотрите какие еще параметры можно настроить через свойства.

Войдите в систему под созданной учётной записью. При первом входе пользователю будет выдано сообщение о необходимости ввести пароль (рис. 11) и окно смены пароля (рис. 12). Смените пароль созданной учётной записи. Здесь подтверждение действий осуществляется клавишей «Enter».

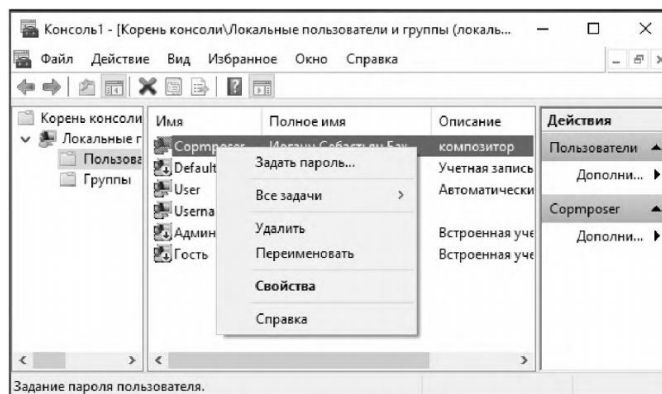


Рисунок 9 – Задание пароля пользователя администратором

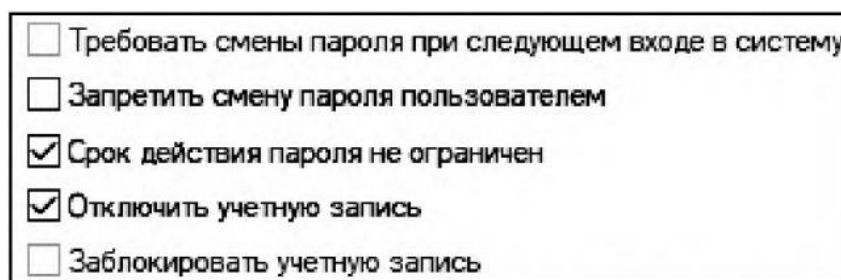


Рисунок 10 – Изменение свойств администратора



Рисунок 11 – Сообщение пользователю  
О необходимости смены пароля

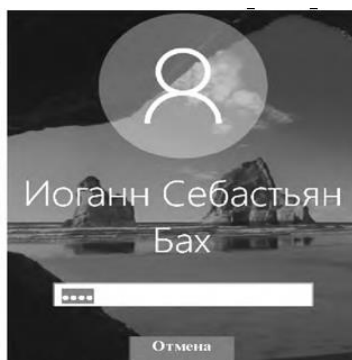


Рисунок 12 – Окно «Смена пароля»

Для применения к пользователю набора прав и ограничений можно включить его учётную запись в группу пользователей с соответствующим набором прав и ограничений.

Войдите в систему под учётной записью «Администратор». Откройте «Свойства» созданной учётной записи. На вкладке «Членство в группах» добавьте пользователя в группу «Опытные пользователи» (рис. 13). Имя группы можно ввести самостоятельно или выбрать из списка, предоставляемого после последовательного нажатия кнопок «Дополнительно» и «Поиск».

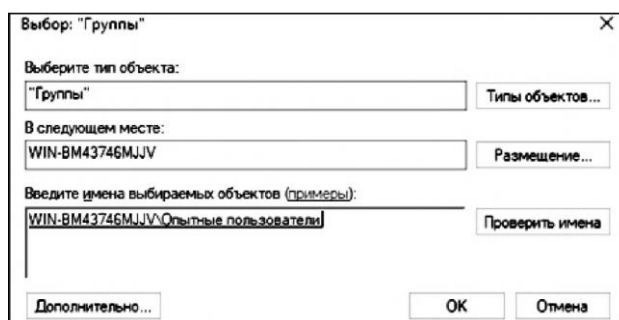


Рисунок 13 – Добавление группы

В разделе «Группы» откройте «Свойства» группы «Опытные пользователи» и проверьте наличие в группе добавленной учётной записи. Создайте новую группу и добавьте в неё этого же пользователя.

Вызовите командную строку и выполните команду «net user». Консоль выведет перечень всех имеющихся учетных записей (рис. 14)

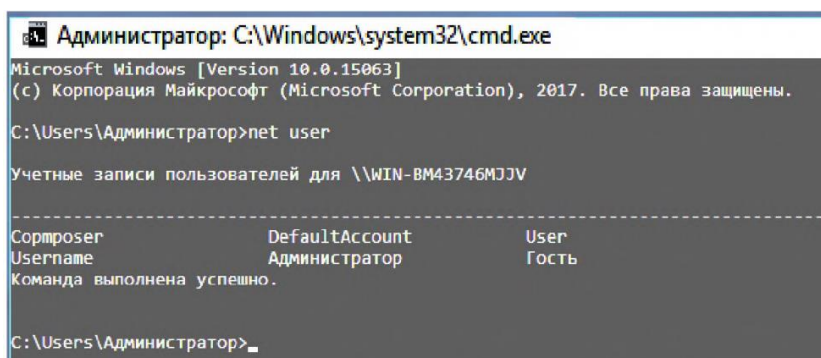
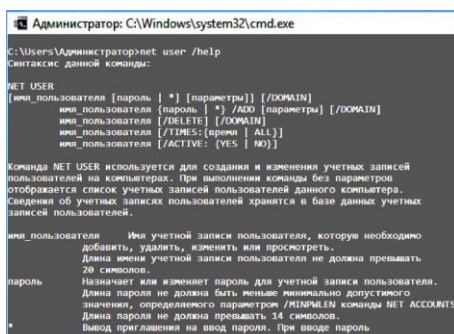


Рисунок 14 – Список пользователей в командной строке



Создание и изменение учётных записей осуществляется при помощи команды «net user». Подробную информацию о команде можно получить, введя «net user /help» (рис. 15). Изучите предлагаемые функции команды.



```
Администратор: C:\Windows\system32\cmd.exe
C:\Users\Администратор>net user /help
Синтаксис данной команды:
NET USER
[имя_пользователя [пароль | *] [параметры]] [/DOMAIN]
имя_пользователя [пароль | *] /ADD [параметры] [/DOMAIN]
имя_пользователя [/DELETE] [/DOMAIN]
имя_пользователя [/TIMES:{промежуток | ALL}]
имя_пользователя [/ACTIVE: {YES | NO}]

Команда NET USER используется для создания и изменения учетных записей
пользователей на компьютерах. При выполнении команды без параметров
отображается список учетных записей пользователей данного компьютера.
Сведения об учетных записях пользователей хранятся в базе данных учетных
записей пользователей.

имя_пользователя      Имя учетной записи пользователя, которую необходимо
добавить, удалить, изменить или просмотреть.
Длина имени учетной записи пользователя не должна превышать
20 символов.
пароль                Назначает или изменяет пароль для учетной записи пользователя.
Длина пароля не должна быть меньше минимально допустимого
значения, определяемого параметром /MINPWLEN команды NET ACCOUNTS.
Длина пароля не должна превышать 34 символов.
*                    Вывод приглашения на ввод пароля. При вводе пароль
не отображается.
```

Рисунок 15 – Справка по команде net user

Создайте учетную запись пользователя с именем, совпадающим с вашим именем в университетской сети, явно указав пароль. При создании дополнительно к логину укажите полное имя пользователя (рис.16).

Синтаксис команды net user при создании учетной записи пользователя:

```
net user имя_пользователя {пароль | *} /add [параметры]
```

Для добавления полного имени пользователя в качестве параметра нужно ввести: FullName: «имя».

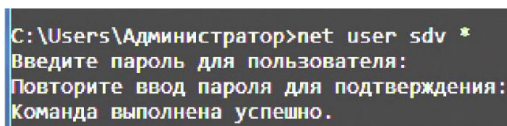


```
C:\Users\Администратор>net user XXX 12345 /add /fullname:"XXX YYY"
Команда выполнена успешно.
```

Рисунок 16 – Создание нового пользователя

Проверьте наличие созданной учётной записи в списке пользователей при помощи команды Net user. Команда Net user имя пользователя, введённая без параметров, позволяет просмотреть информацию об указанном пользователе. Просмотрите информацию о созданной учётной записи.

Возможен ввод пароля без отображения на экране - для этого вместо пароля нужно ввести «\*». Измените пароль созданного пользователя при помощи команды Net user имя пользователя \* (рис. 17).



```
C:\Users\Администратор>net user sdv *
Введите пароль для пользователя:
Повторите ввод пароля для подтверждения:
Команда выполнена успешно.
```

Рисунок 17 – Изменение пароля пользователя

Существует возможность установки ограничений на работу' пользователя в операционной системе по времени. Для этого используется параметр /TIMES: {промежуток | ALL}. Значение ALL указывает, что пользователь может

войти в систему в любое время, а пустое значение указывает, что пользователь не может войти в систему никогда. Ограничьте время работы созданного пользователя рамками рабочего времени (рис. 18). Переведите часы на время, не входящее в интервал рабочего, и протестируйте возможность входа пользователя в операционную систему.

```
C:\Users\Администратор>net user XXX /times:Пн-Пт,09:00-18:00
Команда выполнена успешно.
```

Рисунок 18 – Задание интервала действия учетной записи

В случае необходимости администратор может заблокировать учетную запись пользователя. Заблокируйте учетную запись созданного пользователя при помощи параметра /ACTIVE: {YES | NO} (рис. 19).

твой записи

Проверьте применение блокирования к учетной записи при помощи команды Net user имя пользователя. В выдаваемой о пользователе информации есть графа «Учетная запись активна», показывающая состояние блокирования учетной записи. Разблокируйте учетную запись пользователя.

Если пользователь временно работает в организации, то администратор может ограничить время действия учетной записи пользователя. Для этого служит параметр: /EXPIRES: {дата | NEVER}. Если используется значение NEVER, то время действия учетной записи не имеет ограничений срока действия. Ограничьте время действия учетной записи созданного пользователя (рис. 20). Установите системное время на срок более поздний, чем установленное ограничение. Попробуйте войти в систему под данной учетной записью - операционная система выдаст ошибку (рис. 21).

```
C:\Users\Администратор>net user XXX /expires:19.09.2017
Команда выполнена успешно.
```

Рисунок 20 – Ограничение времени действия учетной записи



Рисунок 21 – Ошибка при попытке входа под просроченной учетной записью

Команда Net localgroup служит для создания локальных групп и управления ими. При использовании этой команды без указания параметров выводится перечень групп пользователей, существующих в операционной системе (рис. 22). Выведите список всех существующих групп.

```
C:\Users\Администратор>net localgroup
Псевдонимы для \\WIN-BM43746MJJV
-----
*IIS_IUSRS
*Администраторы
*Администраторы Нурег-V
*Гости
*Криптографические операторы
*Операторы архива
*Операторы настройки сети
*Операторы помощи по контролю учетных записей
*Опытные пользователи
*Пользователи
*Пользователи DCOM
*Пользователи журналов производительности
*Пользователи системного монитора
*Пользователи удаленного рабочего стола
*Пользователи удаленного управления
*Репликатор
*Управляемая системой группа учетных записей
*Читатели журнала событий
Команда выполнена успешно.
```

Рисунок 22 – Список групп

Синтаксис команды Net net при создании локальной группы: Net localgroup имя группы {/ADD}. Создайте локальную группу Students (рис. 23).

```
C:\Users\Администратор>net localgroup students /add
Команда выполнена успешно.
```

Рисунок 23 – Создание групп

Проверьте наличие созданной группы пользователей при помощи команды Net localgroup. Добавление пользователей в группу осуществляется командой Net localgroup имя группы имя [...] {/ADD}, где имя [...] - имя одного или нескольких пользователей (имена разделяются пробелами).

Добавьте ранее созданного пользователя в группу Students. Команда Net localgroup имя группы выводит список пользователей, входящих в указанную группу. Выведите список пользователей группы Students (рис. 24).

```
C:\Users\Администратор>net localgroup Students
Имя псевдонима      Students
Комментарий

Члены
-----
XXX
Команда выполнена успешно.
```

Рисунок 24 – Просмотр списка пользователей заданной группы

Для удаления группы используется команда Net localgroup имя группы {/DELETE}. Удалите группу Students (рис. 25).

```
C:\Users\Администратор>net localgroup students XXX /delete
Команда выполнена успешно.
```

Рисунок 25 – Исключение пользователя из группы

Проверьте отсутствие группы Students, используя команду вывода списка существующих групп пользователей.

### 3.2. Настройка политики учётной записи

Откройте «Локальную политику безопасности», вызвав её запросом `secpol.msc` в меню «Пуск». Основное окно «Локальной политики безопасности» представлено на рисунке 27. Значения параметров, заданные при настройке политики, будут применяться ко всем пользователям локального компьютера.

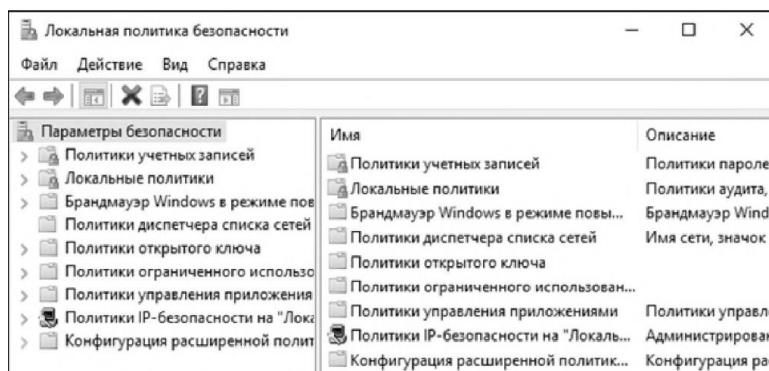


Рисунок 27 – Локальная политика безопасности

Раздел «Политики учётных записей» «Локальной политики безопасности» включает в себя настройки, применяющиеся к паролям пользователей.

Выберите раздел «Политика паролей» («Параметры безопасности - Политики учётных записей - Политика паролей»). Настройки, входящие в раздел «Политика паролей», представлены на рис. 28.

Выполните следующие задания:

- установите максимальный срок действия пароля - 30 дней;
- установите минимальную длину пароля - 10 символов;
- для параметра «Вести журнал паролей» установите значение 3 хранимых пароля, означающее, что новый пароль должен отличаться от 3 последних паролей пользователя;
- включите параметр «Пароль должен отвечать требованиям сложности».

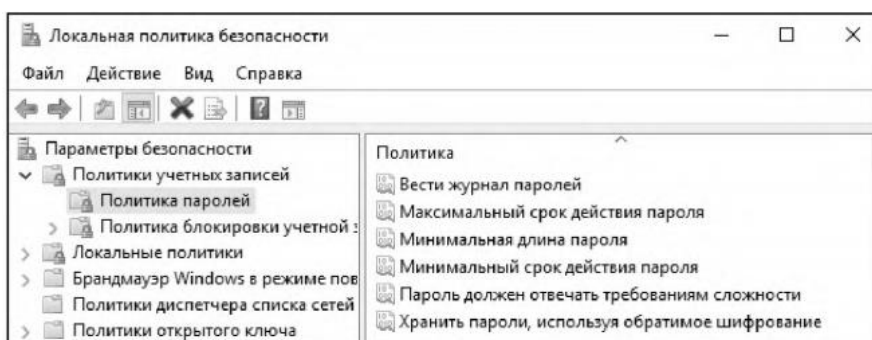


Рисунок 28 – Политика паролей

Параметр «Пароль должен отвечать требованиям сложности» определяет требования сложности для паролей. Если эта политика включена, то пароли должны удовлетворять следующим минимальным требованиям:

-пароль не может содержать имя учётной записи пользователя или какую-либо его часть:

- пароль должен состоять не менее чем из шести символов;

-в пароле должны присутствовать символы трёх категорий из числа следующих четырёх:

- а) прописные буквы английского алфавита от А до Z;
- б) строчные буквы английского алфавита от а до z;
- в) десятичные цифры (от 0 до 9);
- г) неалфавитные символы (например: ! \$, #, %).

Проверка соблюдения этих требований выполняется при изменении или создании паролей. При помощи этого параметра можно избавиться от легко подбираемых паролей типа «111», «qwerty», «12345» и т.д.

Убедитесь, что для пользователя не включена опция «Срок действия пароля неограничен» в оснастке «Локальные пользователи и группы». Переведите системное время более чем на 30 дней вперёд. Попробуйте войти под созданной учётной записью. Пользователю будет выдано сообщение об истечении срока действия пароля (рис. 29). При смене пароля попробуйте заменить пароль на более простой (например, abc12345 или включающий имя учётной записи)

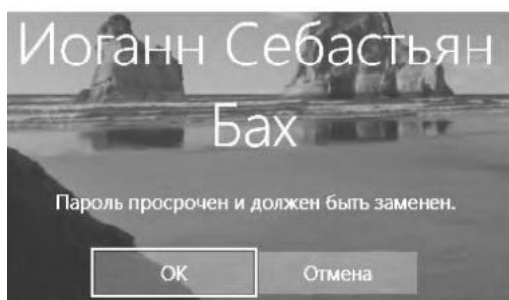


Рисунок 29 – Сообщение об истечении срока действия пароля

В этом случае пользователю будет выдано сообщение об ошибке при генерации пароля (рис. 30). Введите пароль, удовлетворяющий требованиям.

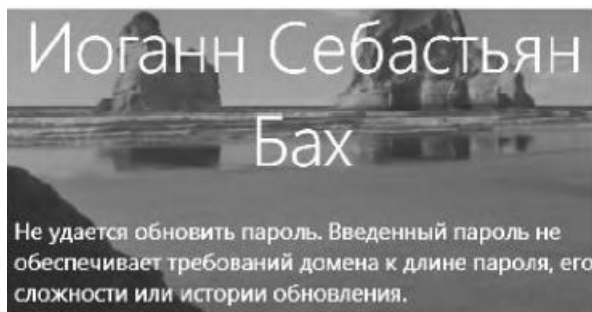


Рисунок 30 – Сообщение о несоответствии пароля требованиям

Войдите в систему под учётной записью «Администратор». Переведите системное время в исходное состояние. Выберите раздел «Политика блокиров-

ки учётной записи» («Параметры безопасности - Политики учётных записей - Политика блокировки учётной записи»). Настройки, входящие в раздел «Политика блокировки учётной записи», представлены на рисунке 31.

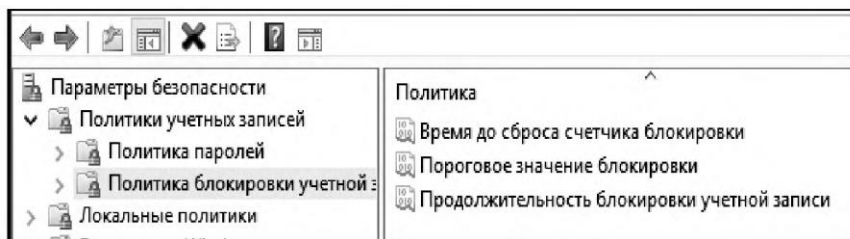


Рисунок 31 – Политика блокировки учетной записи

Настройте параметры следующим образом:

- установить пороговое значение блокировки, равное 3 ошибкам входа в систему (после 3 неудачных попыток входа учётная запись блокируется);

- установить длительность блокировки в параметре «Блокировка учётной записи на», равную 30 мин (значение 0 означает, что блокировку может снять только администратор);

- установите сброс счётчика блокировки через 15 мин. Если в течение установленного времени будет 3 неудачных попытки входа, то учётная запись блокируется. Если неудачных попыток в течение установленного времени будет меньше, то опять допускается 3 неудачных попытки (значение этого параметра не должно превышать длительность блокировки учётной записи).

Завершите сеанс учётной записи «Администратор». При входе в систему под созданной учётной записью три раза введите неправильный пароль. При следующей попытке входа в систему будет выдано сообщение о блокировании созданной учётной записи (рис. 32).

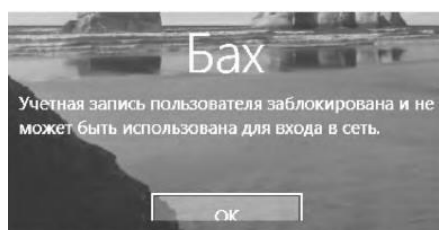


Рисунок 32 – Сообщение о блокировке учетной записи

Войдите в систему под учётной записью «Администратор». Разблокируйте созданную учётную запись. Для этого в окне «Свойства: этой учётной записи» отключите настройку «Заблокировать учётную запись».

Вызовите командную строку. Net accounts используется для обновления базы данных регистрационных записей и изменения параметров входа в сеть (LOGON) и требований к паролям для всех регистрационных записей. При использовании этой команды без указания параметров выводятся текущие значения параметров, определяющих требования к паролям и другие параметры. Выведите текущие параметры входа систему (рис. 33).

- максимальный срок действия пароля - 40 дней;
- запрет использования 3 последних паролей пользователя

```
C:\Users\Администратор>net accounts
Принудительный выход по истечении времени через:          Никогда
Минимальный срок действия пароля (дней):                   0
Максимальный срок действия пароля (дней):                   10
Минимальная длина пароля:                                  10
Хранение неповторяющихся паролей:                          3
Блокировка после ошибок ввода пароля:                       3
Длительность блокировки (минут):                           30
Сброс счетчика блокировок через (минут):                    15
роль компьютера:                                           РАБОЧАЯ СТАНЦИЯ
Команда выполнена успешно.
```

Рисунок 33 – Просмотр информации о требованиях к качеству паролей

Задайте следующие требования к паролю:

- минимальную длину - 6 символов;

Применение этих требований (рис. 34) производится при помощи следующих параметров команды Net accounts:

/MINPWLEN длина

/MAXWAGE: дни

/UNIQUEPW: число

```
C:\Users\Администратор>net accounts /minpwlen:6 /maxwage:40 /uniquepw:3
Команда выполнена успешно.
```

Рисунок 34 – Изменение требований к качеству паролей

### 3.3. Групповые политики

Откройте оснастку «Групповая политика» («Пуск - Выполнить - gpedit.msc»). Оснастка «Групповая политика» состоит из двух основных частей: конфигурация компьютера и конфигурация пользователя (рис. 35).

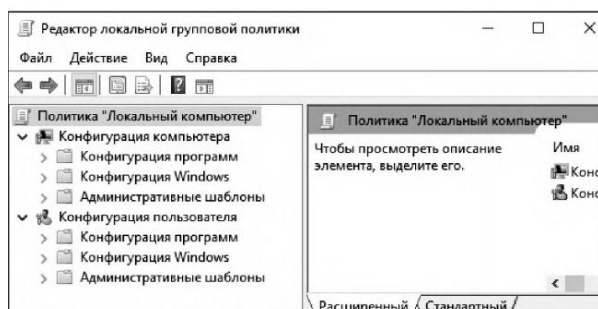


Рисунок 35 – Редактор групповой политики

«Конфигурация компьютера» используется для задания политики, применяемой к компьютерам, вне зависимости от того, какой пользователь работает на них. «Конфигурация пользователя» используется для задания политики, применяемой к пользователям независимо от того, какой компьютер используется для входа в систему.

Созданная групповая политика может быть экспортирована на другой локальный компьютер. Для того чтобы произвести экспорт данных необходимо в



оснастке «Групповая политика» выделить нужный узел и во вкладке «Действие» выбрать пункт «Экспортировать список». В появившемся окне выбрать путь сохранения и указать имя файла.

«Конфигурация компьютера» по умолчанию состоит из следующих разделов: конфигурация программ, конфигурация Windows и административные шаблоны (рис. 36).

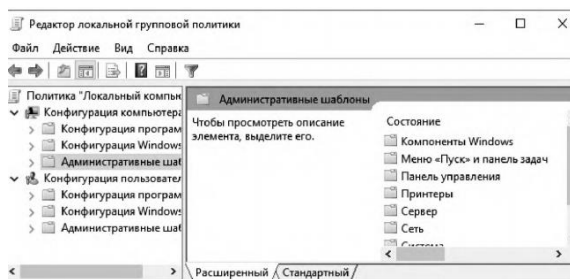


Рисунок 36 – Раздел «Административные шаблоны»

Средствами виртуальной машины подключите компакт-диск. В разделе «Административные шаблоны» выберите подраздел «Компоненты Windows» - «Политики автозапуска». Включите параметр «Выключение автозапуска» (рис. 37). Чтобы проверить выполнение данного параметра, необходимо повторно вставить диск в CD-привод. Система не будет производить его автозапуск, как это делалось раньше.

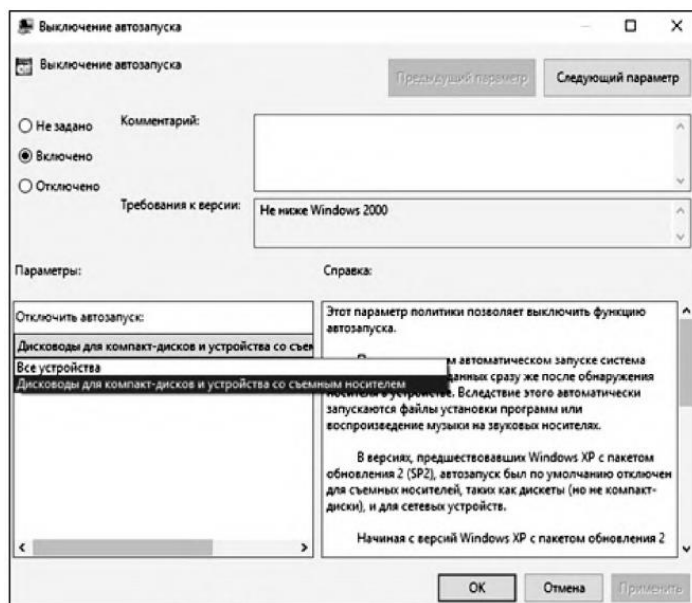


Рисунок 37 – Выключение автозапуска носителя

В разделе «Система» откройте подраздел «Вход в систему» и выберите параметр «Выполнять эти программы при входе в систему». Включите этот параметр и добавьте несколько программ, которые будут запускаться при входе пользователя в систему (рис. 38).



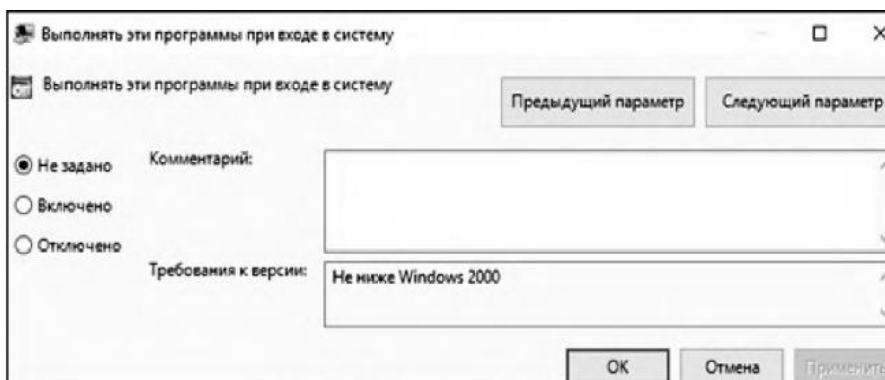


Рисунок 38 – Включение параметра

Добавленные программы (рис. 39) будут запускаться при каждом входе пользователя в систему. Для проверки повторно войдите в систему.

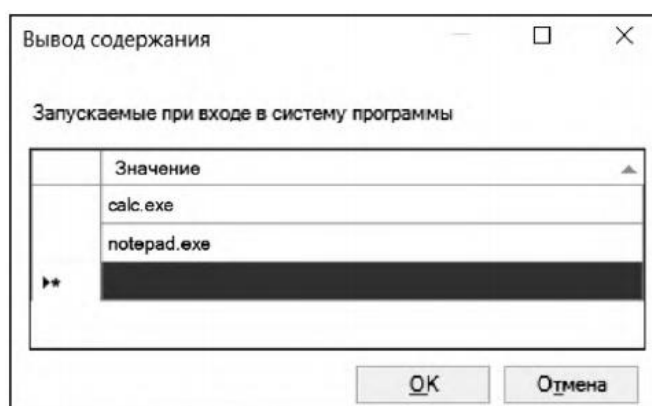


Рисунок 39 – Список запускаемых программ

«Конфигурация пользователя» по умолчанию состоит из тех же разделов, что и «Конфигурация компьютера». При помощи параметров групповой политики существует возможность ограничения доступа пользователя к логическим дискам. Можно скрыть выбранный диск из «Проводника», а также запретить доступ к нему.

Выберите параметр «Запретить доступ к дискам через «Мой компьютер», расположенный в подразделе «Компоненты Windows - Проводник» и запретите доступ к логическому диску C: \ (рис. 40).

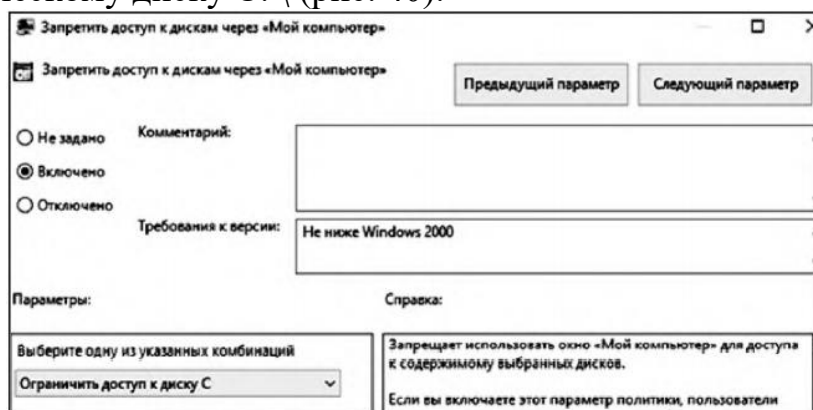


Рисунок 40 – Включение ограничения доступа к диску D

Попытайтесь открыть диск D:\ через «Мой компьютер» (рис. 41) и командную строку (рис. 42). В первом случае система откажет в доступе, а во втором - доступ будет предоставлен (т.к. доступ запрещён только через «Проводник»),

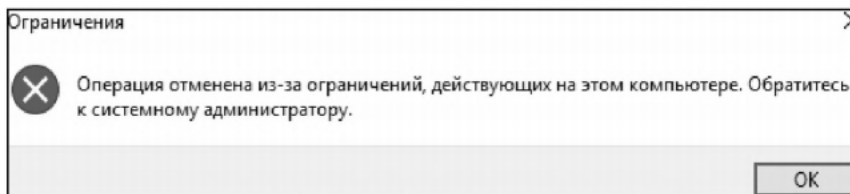


Рисунок 41 – Попытка доступа через проводник

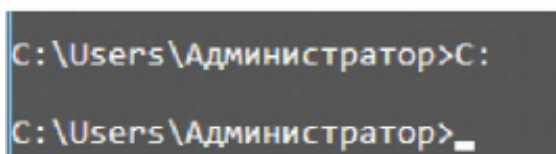


Рисунок 42 – Попытка доступа через командную строку

Ограничение доступа к средствам администрирования возможно за счёт запрета доступа к «Панели управления». Включите параметр «Запретить доступ к панели управления», находящийся в подразделе «Панель управления» (рис. 43). Попытайтесь открыть «Панель управления».

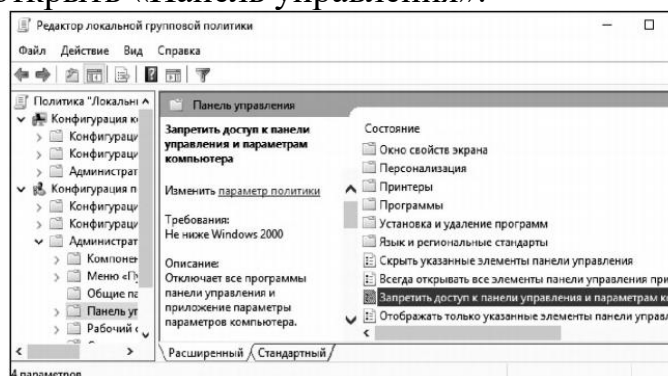


Рисунок 43 – Ошибка при открытии панели управления

Для полного запрета использования командной строки включите параметр «Запретить использование командной строки» в подразделе «Система». Попытайтесь запустить cmd.exe (рис. 44).

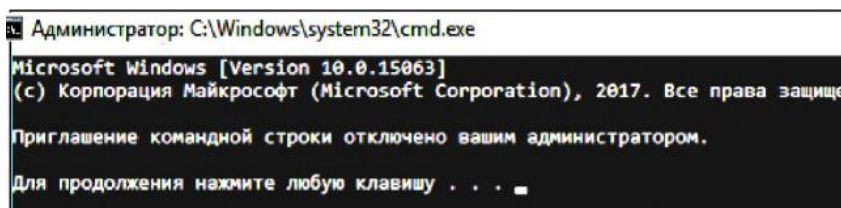


Рисунок 44 – Попытка запуска командной строки

Кроме того, в подразделе «Система» можно запретить использование редактора реестра. Для этого нужно включить параметр «Сделать недоступными средства редактирования реестра». Включите данный параметр и попытайтесь запустить редактор реестра C:\Windows\regedit.exe.

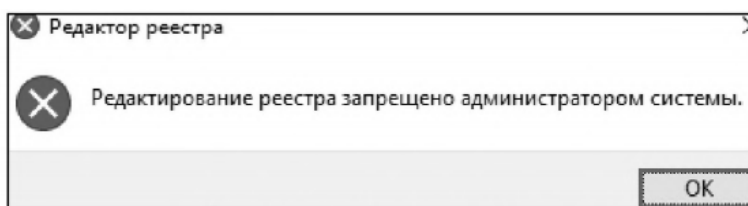


Рисунок 45 – Попытка запуска реестра

Добавление и удаление шаблонов может производиться через контекстное меню раздела «Административные шаблоны» (рис. 46). В появившемся контекстном меню выберите «Добавление и удаление шаблонов». В появившемся окне можно удалить любой шаблон, а также добавить новый шаблон политики.

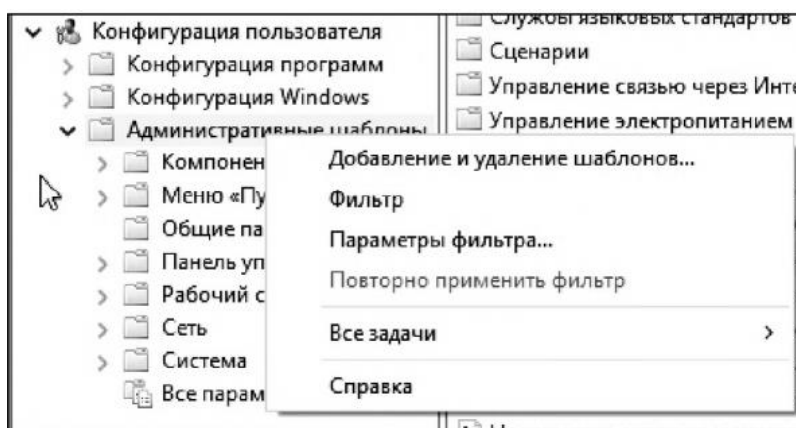


Рисунок 46 – Контекстное меню административных шаблонов

#### 4.Задание на лабораторную работу

1. Ознакомьтесь с теорией.
2. Выполните представленные задания и составьте по проделанной работе отчет.
3. В оснастке «Локальные пользователи и группы» создайте новую группу пользователей. В качестве имени группы пользователей используйте номер Вашей учебной группы.
4. Создайте учётную запись с именем Вашей учётной записи в университетской сети и включите её в созданную группу.
5. Примените к созданной учётной записи настройки, указанные в Вашем варианте (табл. 1).
6. Создайте новую консоль. Добавьте в корень консоли оснастки «Редактор объекта групповой политики» и «Результирующая политика». Сохраните консоль в режиме, указанном в Вашем варианте (табл. 2.).

Таблица 1 – Варианты заданий работы с пользователями

Параметр \ Вариант	1	2	3	4	5	6	7	8	9	10
Максимальный срок действия пароля	30	90	60	30	90	60	30	90	60	30
Минимальная длина пароля	6	7	8	9	10	6	7	8	9	10
Требовать неповторяемости паролей	6	5	4	3	2	6	5	4	3	2
Отвечать требованиям сложности	+	-	-	+	-	-	+	-	+	+
Пороговое значение блокировки	3	4	5	6	7	3	4	5	6	7
Блокировка учётной записи на...	10	20	30	45	60	10	20	30	45	60
Сброс счётчика блокировки через...	5	10	15	20	30	10	20	30	45	60
Завершение работы системы	+	+			+		+		+	
Локальный вход в систему	+	+	+	+	+	+	+	+	+	+
Изменение системного времени	+		+		+		+		+	

Таблица 2 - Варианты работы с групповыми политиками

Вар.	Режим работы с консолью	Параметры групповой политики
1	Авторский	Запретить редактирование реестра. Ограничить размер профиля пользователя значением 5 МБ
2	Пользовательский - полный доступ	Запретить использование командной строки. Запретить изменение рисунка рабочего стола
3	Пользовательский - многооконный	Запретить использование сочетаний клавиш, включающих кнопку «Windows». Удалить имя пользователя из меню «Пуск»
4	Пользовательский - однооконный	Запретить использование диспетчера задач. Установить обязательный запрос пароля при выходе из спящего режима
5	Авторский	Запретить доступ к «Панели управления». Запретить запуск «Блокнота»
6	Пользовательский - полный доступ	Установить обязательный запрос пароля при выходе из экранной заставки. Удалить «Завершение сеанса» из меню
7	Пользовательский - многооконный	Скройте диск D: (CD-привод) из окна «Мой компьютер». Удалите значок «Мои документы» с «Рабочего стола»
8	Пользовательский - однооконный	Удалите «Общие документы» из окна «Мой компьютер». Скройте общие группы программ из меню «Пуск»
9	Авторский	Запретите доступ к диску C: из окна «Мой компьютер». Удалите «Сетевые подключения» из меню «Пуск»
10	Пользовательский - полный доступ	Запретить вызов «Свойств» объекта «Мой компьютер». Установить очистку списка последних использовавшихся

7. Установите параметры групповой политики, указанные в Вашем варианте (табл. 2), и продемонстрируйте преподавателю результат применения параметров (например, невозможность запуска редактора реестра).

8. Проясните преподавателю изменённые параметры при помощи «Результирующей политики» для пользователя «user».

### **Отчет**

Отчет должен содержать:

1. наименование работы;
2. цель работы;
3. задание;
4. последовательность выполнения работы;
5. ответы на контрольные вопросы;
6. вывод о проделанной работе.

### **3. Контрольные вопросы**

1. Поясните параметр «Пароль должен отвечать требованиям сложности» и перечислите минимальные требования, которым должны удовлетворять пароли, если параметр включен.

2. Какие параметры входят в политику блокировки учётной записи?

3. Возможно ли, что учётная запись не будет заблокирована при количестве ошибок больше, чем установленное пороговое значение?

4. Что такое и для чего применяется MMC?

5. Что такое оснастка?

6. В чём состоит отличие конфигурации компьютера от конфигурации пользователя в групповой политике?

7. Каким образом можно включить автозапуск программ через групповую политику?

8. При помощи какой команды можно получить список пользователей операционной системы?

9. При помощи какой команды можно получить список групп пользователей операционной системы?

10. При помощи какой команды можно создать нового пользователя?

### ***Лабораторная работа № 2. Резервное копирование в системе Windows Server 2012 R2***

**Цель данной лабораторной работы** – познакомиться со средствами организации резервного копирования в операционной системе Microsoft Server 2012 R2мы в очередной раз разбираем одну необходимую тему. Многие системные администраторы задаются вопросом сохранения рабочей версии Server 2012 R2, причем бэкапирование должно быть настроено циклично.

С точки зрения управления рисками, важность процедуры резервного копирования очень высока. В тех случаях, когда реализация угрозы приводит к изменению или удалению данных, повреждению программных компонент системы, резервное копирование позволяет снизить причиненный ущерб и значительно ускорить восстановление системы.

При разработке политики резервного копирования нужно определить, как минимум, следующие параметры:

1. частоту выполнения резервных копий;
2. порядок восстановления данных из резервных копий;
3. объем носителей информации, выделяемых для хранения резервных копий;
4. количество хранимых копий;
5. вопросы обеспечения безопасности носителей резервных копий.

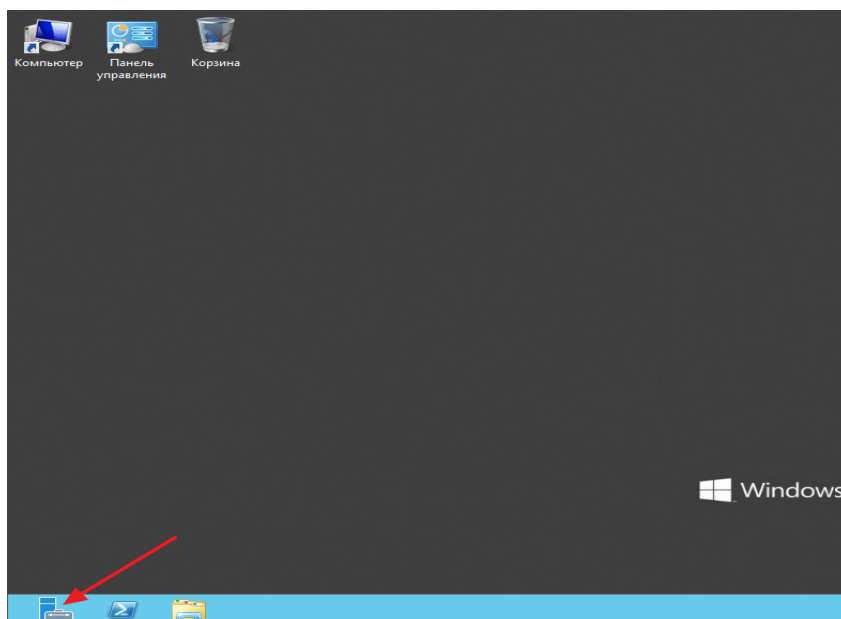
С выходом операционной системы Server 2012 R2 настройку резервных копий можно создать с помощью стандартных компонентов, и никаких дополнительных дорогостоящих лицензий на стороннее программное обеспечение закупать не нужно.

Если кто не знает, что такое бэкапы системы, то я постараюсь вкратце вам об этом рассказать.

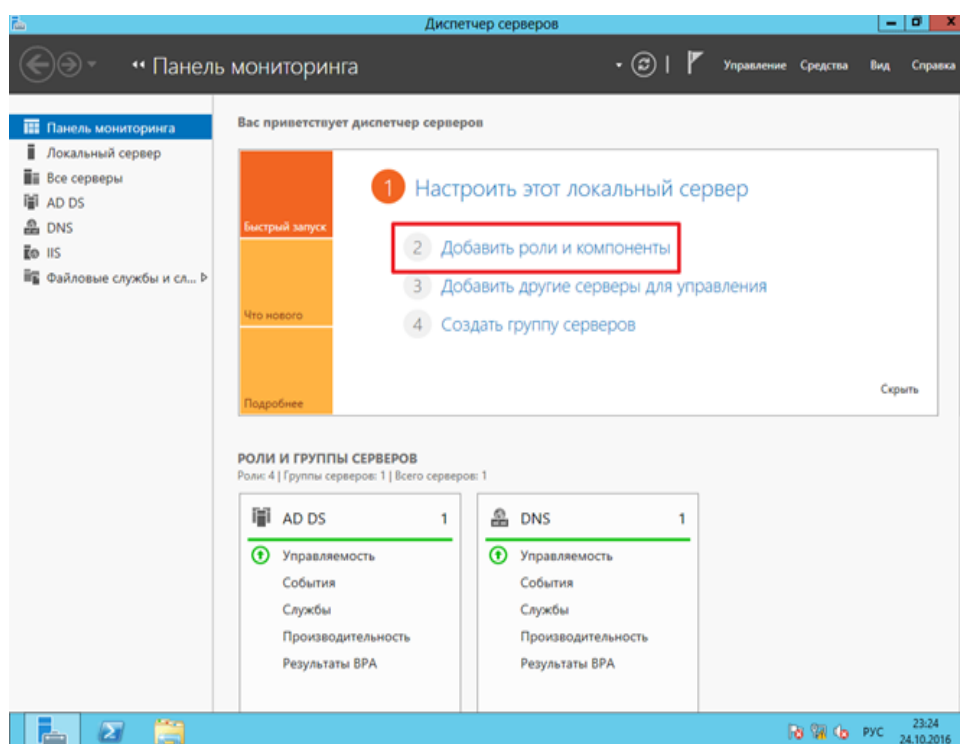
Бэкап системы – это резервное копирование системы с целью ее восстановления в рабочую версию! Если вдруг произошел сбой в системе или потеря какой-либо важной информации, которая хранится на сервере, вы сможете восстановить в рабочую версию выполнив несколько простых действий. Поэтому важно всегда на всякий случай иметь рабочие бэкапы вашей системы!

## **Создание бэкапов системы на Windows Server 2012 R2**

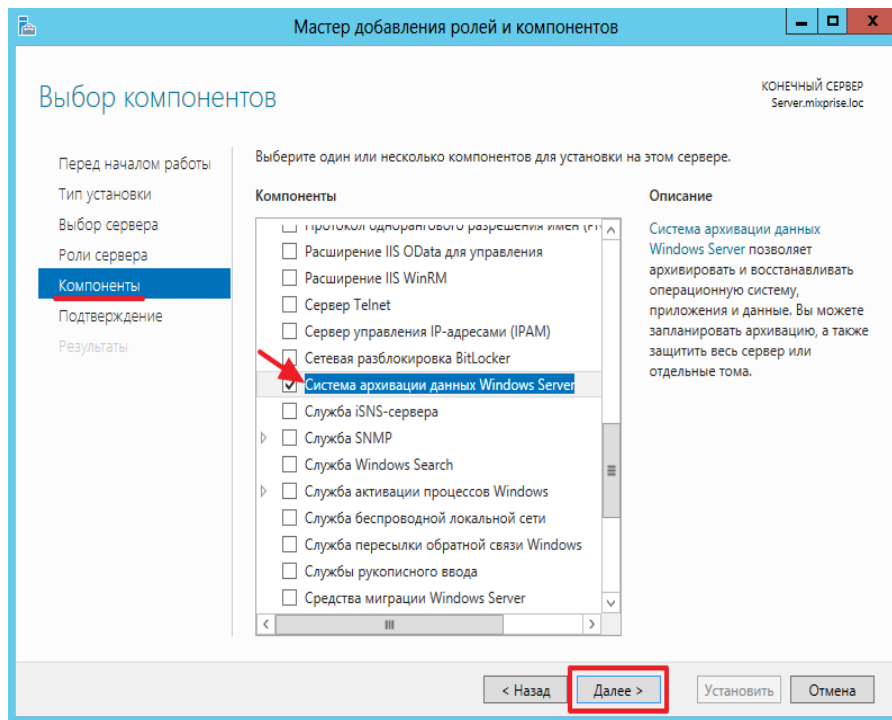
Для включения бэкапирования системы на серверах под управлением Microsoft Server 2012 необходимо установить дополнительные функции. Запустите «Диспетчер серверов»



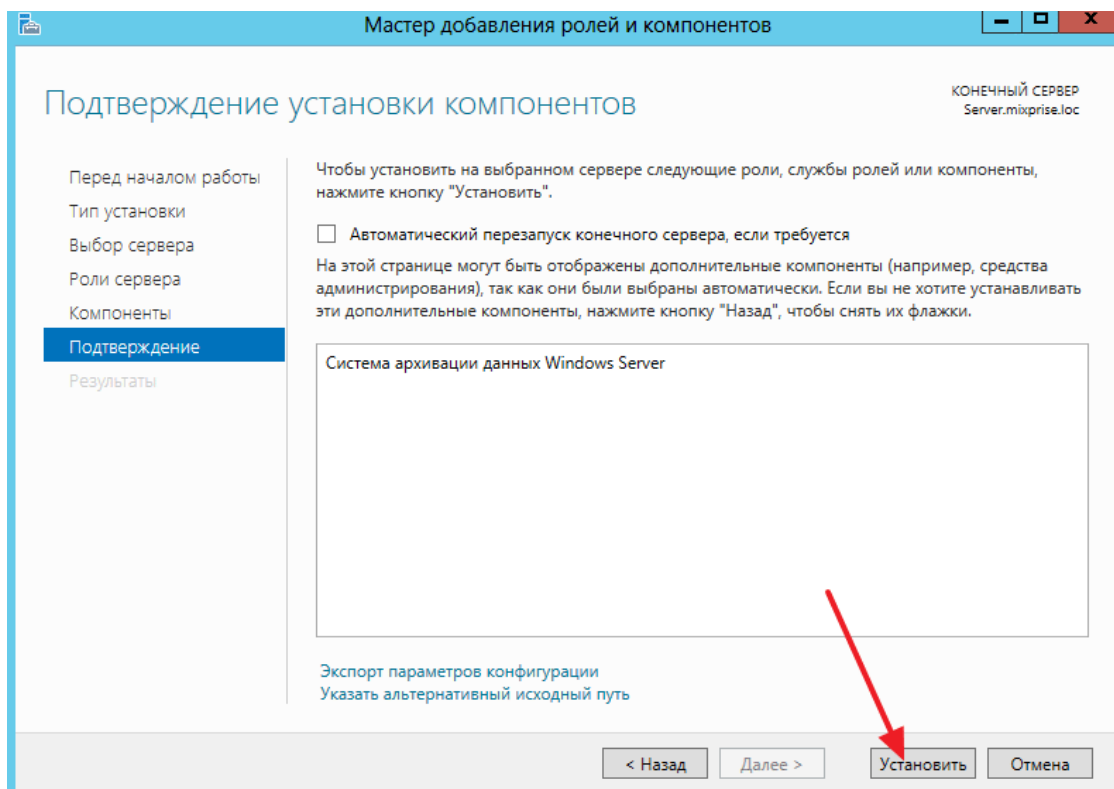
После чего нажимаем на вкладку «Добавить роли и компоненты»»



В появившемся окне перейдите во вкладку «Компоненты» затем ставим галочку напротив надписи: «Система архивации данных с Windows Server» ну и жмем «Далее»



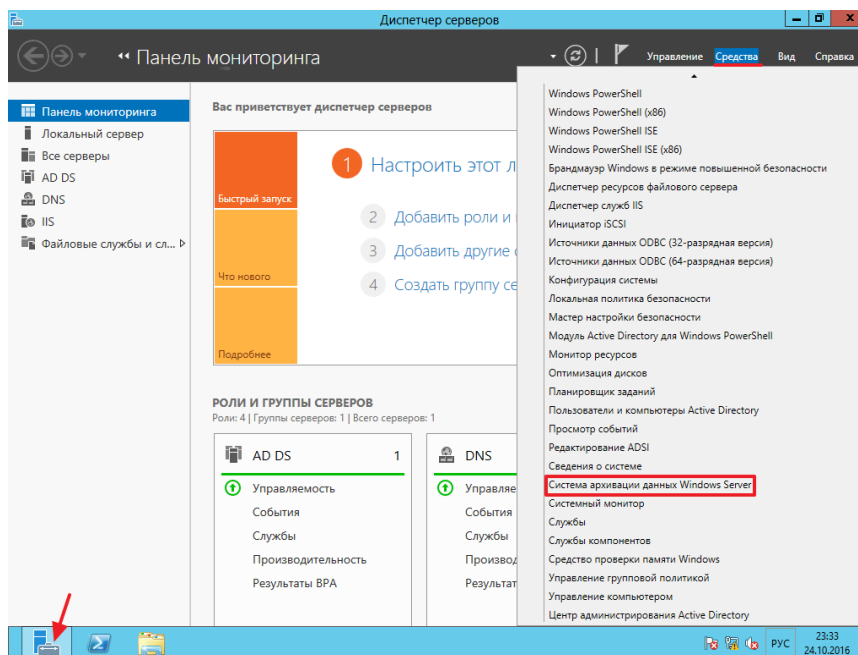
В заключительном этапе установки жмем «Установить»



После того как функционал резервного копирования был добавлен, давайте запустим оснастку, снова откройте «Диспетчер серверов» далее в верхнем

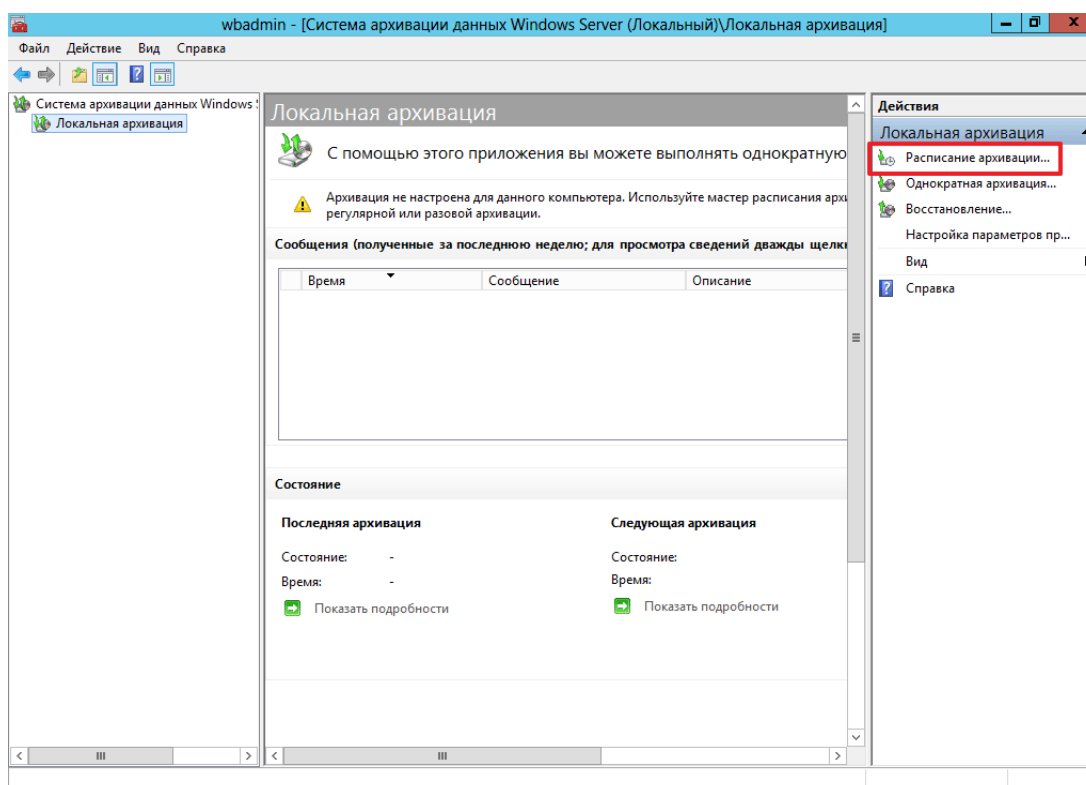


меню жмите по вкладке «Средства» и откройте пункт «Система архивации данных Windows Server»

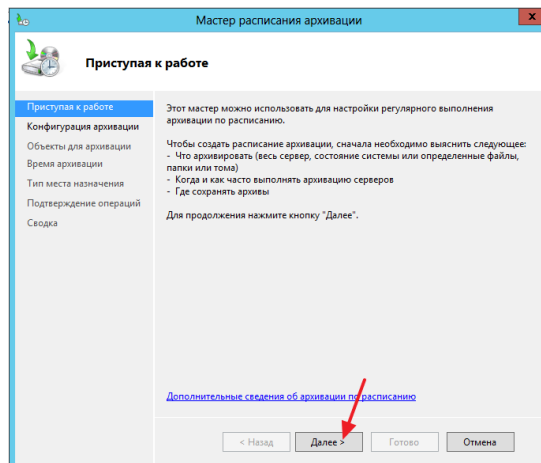


Перед вами должна запуститься графическая оболочка, в правом меню вы можете увидеть возможности, которая она предоставляет.

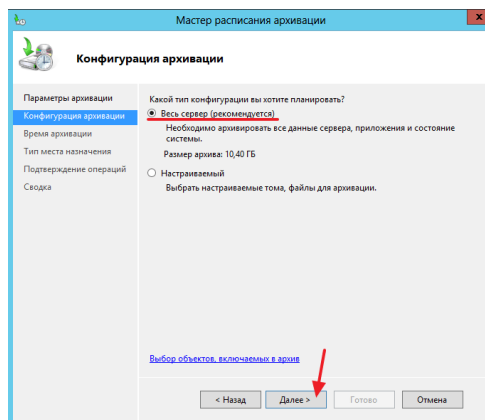
Самым главным этапом, по моему мнению, будет бэкап по расписанию, поэтому выбираем пункт «Расписание архивации»



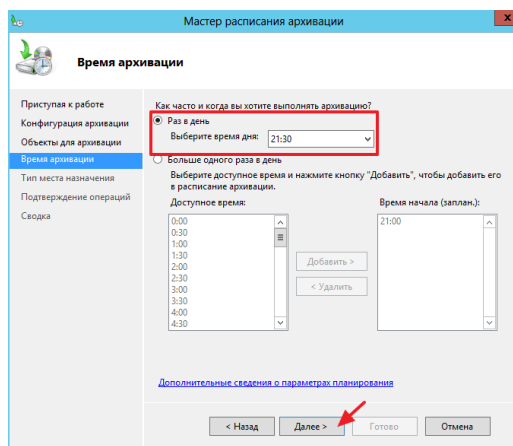
Во вкладке приступая к работе, ждем «Далее»



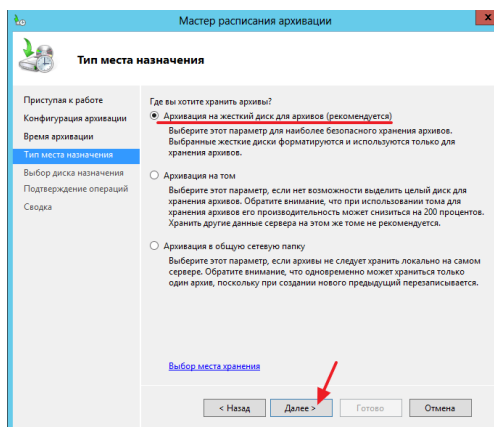
В разделе конфигурации ставим чекбокс напротив пункта «Весь сервер» - с помощью него вы сможете восстановить конфигурацию и настройки сервера полностью!



В разделе время архивации указываем время, когда нам необходимо выполнять архивацию, после того как все параметры указаны нажмите «Далее»

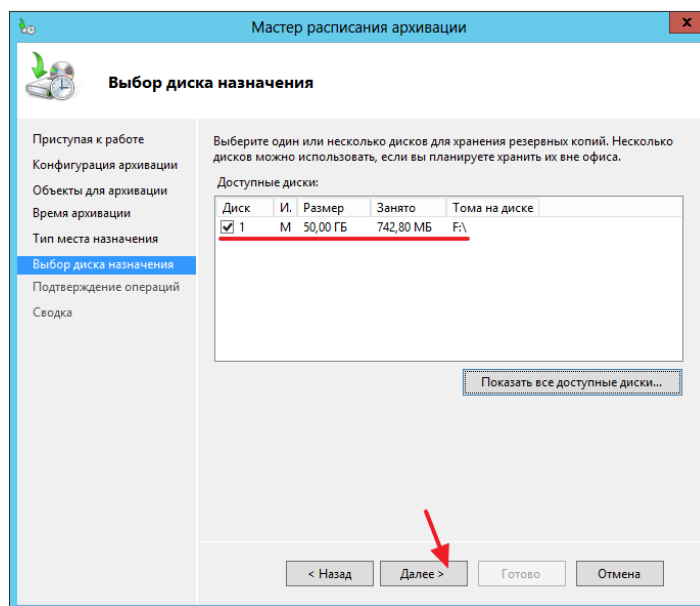


В открывшемся окне необходимо указать место, где будут храниться архивы для восстановления системы, я обычно выбираю «Архивация на жесткий диск для архивов» и жмите «Далее».

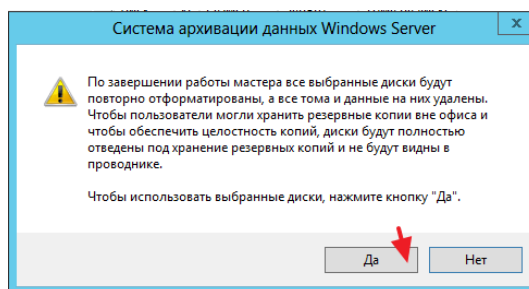


Следующим шагом в появившемся окне необходимо выбрать диск для архивации в моем случае у меня только один диск поэтому я и выбираю его, если вы хотите указать другие диски допустим которые подключены по USB нажмите на вкладку «Показать все доступные диски» и выберите тот который считаете нужным.

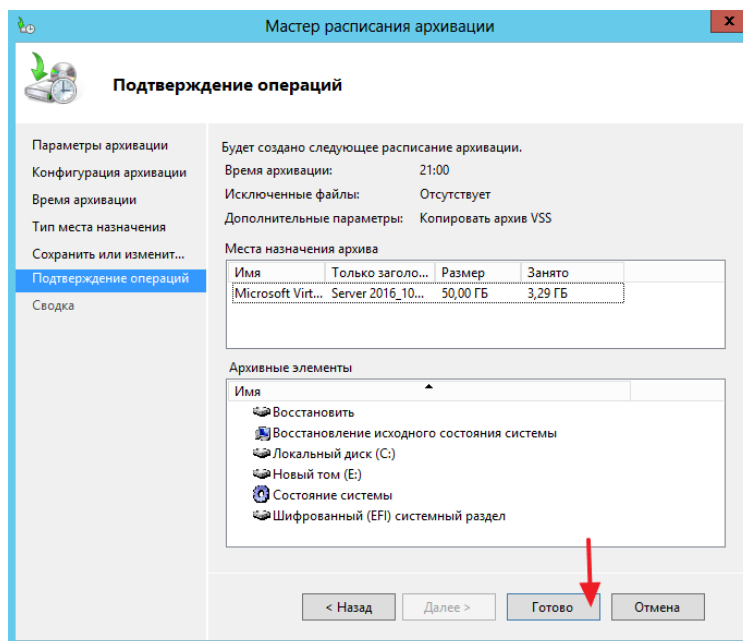
Итак, ставим галочку на уже выбранном жестком диске и кликаем «Далее»



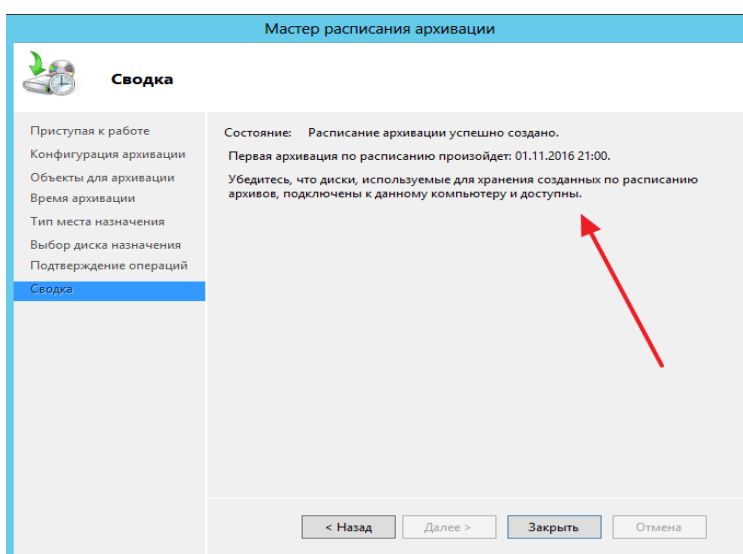
**Важно:** после того как вы укажете жесткий диск для бэкапов, он будет полностью отформатирован, для дальнейшей настройки ждем «Да»



Для завершения операции нажмите «Готово»



После того как вы произвели вышеуказанные настройки и если вы произвели правильные настройки резервного копирования в Server 2012 R2, то вы должны увидеть это информационное окно:



Сегодня мы рассмотрели тему, которая посвящена резервному копированию в операционной системе MS Windows Server 2012 R2.

### **Задание 1.**

1. На учебном сервере (или виртуальной машине) выберите раздел для резервного копирования.

2. С учетом рассмотренных ограничений и объема копируемого раздела, выберите место для размещения копии. Определите, от имени какой учетной записи будет проводиться эта операция.

3. Выполните однократное резервное копирование выбранного раздела.

### Задание 2.

Выберите из архива, созданного в предыдущей части работы, группу файлов для восстановления. Восстановите их в первый раз по исходному пути с сохранением копий, во второй раз - по альтернативному пути. Опишите, в чем разница в полученных результатах.

### Задание 3.

Разработайте и реализуйте план ежедневного резервного копирования раздела с операционной системой.

При выполнении лабораторной работы на виртуальной машине для хранения резервных копий можно подключить дополнительный виртуальный диск (настройка делается в свойствах виртуальной машины, когда она не запущена). При выполнении работы на учебном сервере, заранее определите физический диск, на который можно сохранить копии (диск не должен содержать полезных данных, т.к. он будет отформатирован!).

Выберите такое время создания копии, чтобы результат можно было увидеть в ходе выполнения лабораторной.

После создания копии, восстановите какой-либо из файлов.

Используя опцию Backup Schedule оснастки Windows Server Backup, удалите запланированное задание на резервное копирование.

### **Отчет**

Отчет должен содержать:

1. наименование работы;
2. цель работы;
3. задание;
4. последовательность выполнения работы;
5. ответы на контрольные вопросы;
6. вывод о проделанной работе.

## Литература

1. Об информации, информационных технологиях и о защите информации: федер. закон РФ № 149-ФЗ от 27.07.2006 г.
2. Доктрина информационной безопасности РФ № Пр-1895 от 06.09.2000 г.
3. О персональных данных: федер. закон РФ № 152 от 27.07.2006 г.
4. Об электронной цифровой подписи: федер. закон РФ № 1-ФЗ от 26.12.2001 г.
5. Бабаш А.В., Баранова Е.К., Мельников Ю.Н. Информационная безопасность. Лабораторный практикум: учеб. пособие М.: КноРус, 2016. 136 с.
6. Гафнер В.В. Информационная безопасность: учеб. пособие. Рн/Д: Феникс, 2017. 324 с.
7. Громов Ю.Ю., Драчев В.О., Иванова О.Г. Информационная безопасность и защита информации: учеб. пособие. Ст. Оскол: ТНТ, 2017. 384 с.
8. Ефимова Л.Л., Кочерга С.А. Информационная безопасность детей. Российский и зарубежный опыт: монография. М.: ЮНИТИ-ДАНА, 2016. 239 с.
9. Ефимова Л.Л., Кочерга С.А. Информационная безопасность детей. Российский и зарубежный опыт: монография. М.: ЮНИТИ, 2016. 239 с.
10. Запечников С.В., Милославская Н.Г. Информационная безопасность открытых систем. В 2 т. Т. 1. Угрозы, уязвимости, атаки и подходы к защите. М.: ГЛТ, 2017. 536 с.
11. Информационная безопасность открытых систем. В 2 т. Т. 2. Средства защиты в сетях / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. М.: ГЛТ, 2018. 558 с.
12. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. М.: ГЛТ, 2016. 280 с.
13. Семененко В.А. Информационная безопасность: учеб. пособие. М.: МГИУ, 2017. 277 с.
14. Чипига А.Ф. Информационная безопасность автоматизированных систем М.: Гелиос АРВ, 2017. 336 с.
15. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие. М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2017. 416 с.
16. Шаньгин В.Ф. Информационная безопасность и защита информации. М.: ДМК, 2017. 702 с.
17. Ярочкин В.И. Информационная безопасность: учеб. для вузов. М.: Акад. Проект, 2018. 544 с.
18. Организационное и правовое обеспечение информационной безопасности: учебник и практикум / под ред. Т.А. Поляковой, А.А. Стрельцова. М.: Юрайт, 2017. 325 с.
33. Кузнецов П.У. Информационное право [Электронный ресурс]: учеб. для бакалавров. М.: Изд-во Юстиция, 2017. 335 с. // URL: [http://нэб.рф/catalog/000199\\_000009\\_009476417](http://нэб.рф/catalog/000199_000009_009476417) / - ЭБС «НЭБ».
34. Никулин В.В. Безопасность и защита информации [Электронный ресурс]: учеб.-метод. пособие. Брянск, 2019. // URL: <http://moodle.bgsha.com/course/view.php?id=25340>.

35. Никулин В.В. Безопасность и защита информации [Электронный ресурс] // URL: <http://moodle.bgsha.com/course/view.php?id=25340#section-7>
36. Основные понятия в области информационной безопасности [Электронный ресурс] / А. Пролетарский, Н. Руденков, Е. Смирнова, А. Суоров // Национальный Открытый Университет "ИНТУИТ" // URL: [http://www.intuit.ru/studies/courses/16655/1300/print\\_lecture/25504](http://www.intuit.ru/studies/courses/16655/1300/print_lecture/25504)
37. Атака через Internet [Электронный ресурс] // URL: <http://citforum.ru/internet/attack/c32.shtml>
38. [www.intuit.ru/department/security/antiviruskasp/](http://www.intuit.ru/department/security/antiviruskasp/)
39. Вирусы и средства борьбы с ними: курс лекций для Интернет университета информационных технологий от лаборатории Касперского [Электронный ресурс]. М.: Интернет-университет информационных технологий - [www.INTUIT.ru](http://www.INTUIT.ru), 2007. // URL: [www.intuit.ru/department/security/viruskasper/](http://www.intuit.ru/department/security/viruskasper/)

Учебное издание

Никулин Валерий Владимирович

## **Безопасность и защита информации**

**учебно-методическое пособие**

**Безопасность и защита информации. Лабораторный практикум для  
подготовки для студентов направления подготовки 09.04.03 «Прикладная  
информатика**

Редактор Павлютина И.П.

---

Подписано к печати 18.11.2021. Формат А5. Бумага печатная.  
Усл. п. л. 7,44. Тираж 100 экз. Изд. № 7062.

---

Издательство Брянского государственного аграрного университета  
243365 Брянская область, Выгоничский район, с. Кокино, Брянский ГАУ