ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 1 (3.3)
(краткие теоретические сведения)

Тема: 3.3 Каналы утечки информации и безопасность информационных систем.

Учебные вопросы:

1. Настройка параметров доверенной загрузки операционной системы.
2. Аутентификация, авторизация и управление доступом в ОС Windows.
3. Политики безопасности ОС.
4. Регистрация и оперативное оповещение о событиях безопасности.

1. Настройка базовой системы ввода-вывода (BIOS) компьютера

BIOS (*Basic Input / Output System* – базовая система ввода-вывода) – это программа для первоначального запуска компьютера, настройки оборудования и обеспечения функций ввода-вывода. В современных компьютерах BIOS выполняет несколько функций:

запуск компьютера и процедуру самотестирования (Power-On Self Test, POST). Программа, расположенная в микросхеме BIOS, загружается первой после включения питания компьютера. Она детектирует и проверяет установленное оборудование, настраивает его и готовит к работе. Если обнаруживается неисправность оборудования, процедура POST останавливается с выводом соответствующего сообщения или звукового сигнала;

настройку параметров системы. Во время процедуры POST оборудование настраивается в соответствии с параметрами, хранящимися в специальной CMOS-памяти. Изменяя эти параметры, пользователи могут конфигурировать отдельные устройства и систему в целом по своему усмотрению. Редактируются они в специальной программе, которую называют BIOS Setup или CMOS Setup.

Во всех современных компьютерах BIOS хранится в микросхеме на основе flash-памяти (Flash Memory). Такая микросхема может быть перезаписана с помощью специальных программ прямо на компьютере. Запись новой версии BIOS обычно называется перепрошивкой.

В большинстве случаев flash-память устанавливается на специальную панель (рис. 1), что позволяет легко заменить микросхему при необходимости. В старых компьютерах встречались микросхемы BIOS в прямоугольном корпусе DIP32 (рис. 1, слева); в большинстве плат используются микросхемы BIOS в квадратном корпусе (рис. 1, в центре), а в новых платах можно встретить маленькие чипы с последовательным интерфейсом (рис. 1, справа). Обычно на них есть наклейка с обозначением версии BIOS, а если ее нет – маркировка чипа flash-памяти.

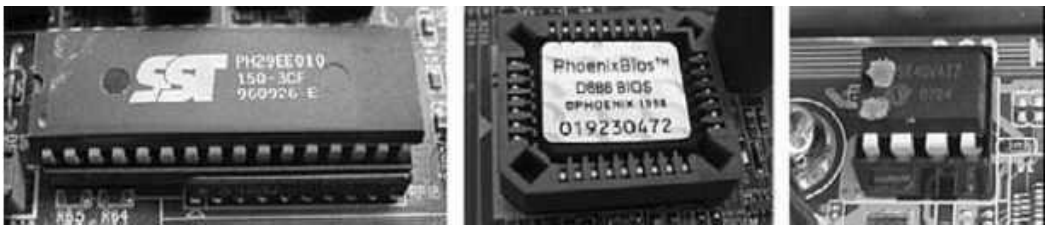


Рис.1. Примеры установки микросхемы BIOS на панель системной платы

BIOS использует параметры конфигурации, которые хранятся в специальной CMOS-памяти. CMOS-память питается от специальной батарейки на системной плате, которая также используется для питания часов реального времени (рис. 2).

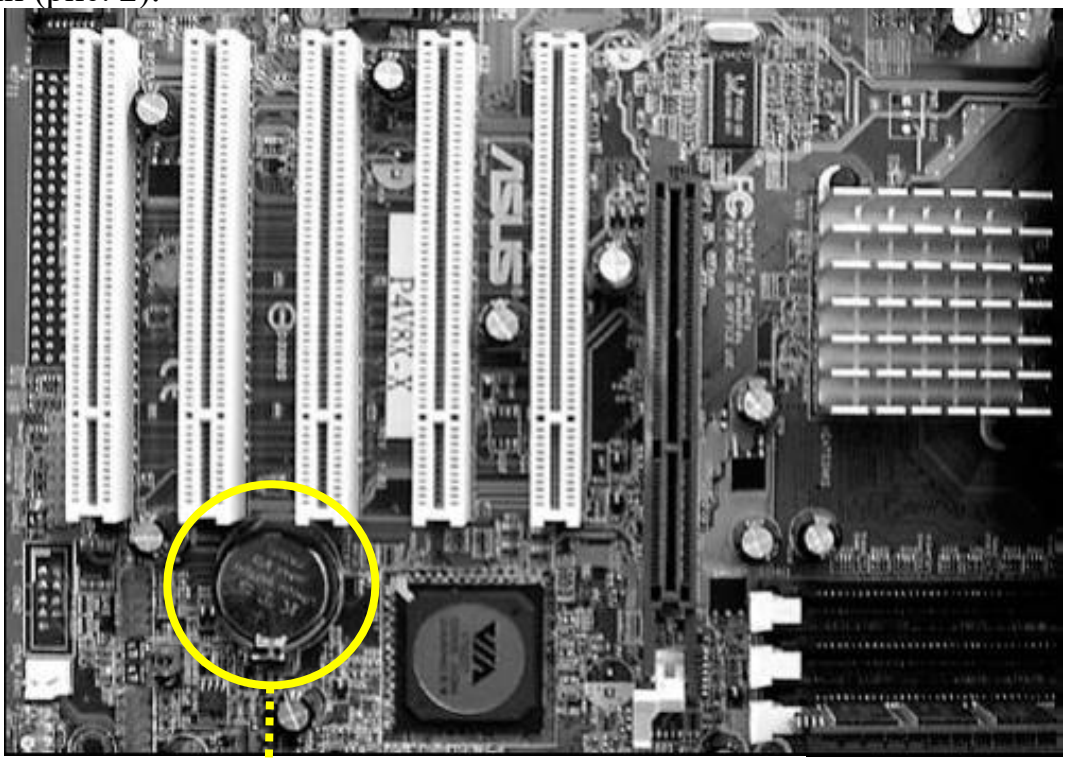


Рис.2. Пример размещения специальной батарейки на системной плате, которая также используется для питания часов реального времени

Все начальные загрузчики операционных систем обращаются к базовой системе ввода-вывода (BIOS) с тем, чтобы провести первоначальную инициализацию установленного оборудования и контрольное тестирование его работоспособности, а также получить сведения о том, каким образом выполнять дальнейшую загрузку ОС. Поскольку BIOS – это самый нижний уровень программного обеспечения, предназначенного для конфигурирования и управления оборудованием компьютера, в нем содержится код для взаимодействия со средствами ввода-вывода, дисковыми накопителями, коммуникационными портами и другими устройствами, что с точки зрения информационной безопасности можно рассматривать как серьезную уязвимость системы.

Учитывая, что BIOS запускается с высоким уровнем привилегий на ранней стадии загрузки системы, вредоносный код, исполняемый на уровне

BIOS, достаточно трудно обнаружить. Кроме того, он может использоваться для повторного «инфицирования» системы даже после того, как была произведена переустановка ОС или даже замена жесткого диска компьютера. В этих условиях BIOS и загрузчик воспринимаются нарушителем как привлекательные объекты атак:

атаки на BIOS, заключающиеся в подмене исходного кода BIOS вредоносным кодом BIOS, внедренным нарушителем;

атаки на загрузчик, заключающиеся в установке подконтрольного нарушителю так называемого «буткита» (bootkit, разновидность «руткита» (rootkit), который исполняется в режиме ядра), «инфицирующего» загрузчик. При этом «буткит» может использоваться для организации утечки чувствительной информации, обрабатываемой в процессе загрузки, такой как пароли шифрования информации на жестком диске.

Кроме того, изменив в BIOS приоритет носителя для первоочередной загрузки ОС, злоумышленник может загрузить ее со своего USB-носителя и с помощью специального вредоносного обеспечения осуществить сброс (обнуление) пароля от учетной записи, получив тем самым несанкционированный доступ к ПК.

В соответствии с Инструкцией об организации технической защиты информации, не отнесенной к государственным секретам, в государственных информационных системах органов внутренних дел и внутренних войск Министерства внутренних дел Республики Беларусь, утвержденной приказом МВД Республики Беларусь от 08 июля 2016 г. № 187 (далее – Инструкция), во избежание возможности изменения настроек автоматизированного рабочего места (далее – АРМ), на котором обрабатывается информация ограниченного распространения, вход в настройку BIOS должен быть защищен паролем. При этом подразделение по технической защите информации ведет журнал регистрации паролей для входа в BIOS Setup АРМ подразделения, зарегистрированный в установленном порядке, который хранится в подразделении по режиму секретности ОВД.

Для минимизации вышеобозначенных угроз в BIOS предусмотрены следующие опции безопасности (таблица 1)[1]:

Таблица 1

Наименование опции безопасности BIOS	**Описание**
BIOS Flash Protect (Firmware Write Protect)	Данная опция предназначена для защиты BIOS от случайного повреждения (обновления) пользователями или компьютерными вирусами. Когда она включена, данные, содержащиеся в BIOS, не смогут быть изменены.
BIOS Features Setup Virus Warning (Anti-Virus Protection)	Когда данная опция включена, BIOS выдаст предупреждение при попытке обращения к загрузочному сектору или к таблице разделов (область в главной загрузочной записи (MBR), которая используется

[1] В зависимости от версии программного обеспечения наименование опций безопасности и их количество может отличаться.

Наименование опции безопасности BIOS	Описание
	компьютером для определения доступа к диску).
Hard Disk Access Control	Опция позволяет включить режим защиты от записи для жесткого диска. Может принимать следующие значения: *Read-Write* (по умолчанию) – запись на жесткий диск разрешена; *Read Only* – запись на жесткий диск запрещена.
Hardware Reset Protection	Опция позволяет запретить возможность использования кнопки RESET, которая расположена на системном блоке. Крайне полезна для компьютеров, выполняющих функции файл-сервера, или в случаях, когда неудобно расположена кнопка или системный блок, что постоянно приводит к случайной перезагрузке.
Change Supervisor Password	Опция позволяет вам изменить пароль администратора, который используется для запуска программы настройки BIOS или для запуска компьютера. Для изменения пароля необходимо зайти в систему с паролем администратора.
Change User Password	Опция позволяет изменить пароль пользователя, который используется для запуска программы настройки BIOS или для запуска компьютера. Для изменения пароля необходимо зайти в систему с паролем администратора.
Password Checking Option	Опция позволяет определить, в каких ситуациях будет запрашиваться пароль. Может принимать следующие значения: *Disabled* (по умолчанию) – парольная защита не используется; *Setup* – пароль запрашивается при запуске программы настройки BIOS; *Always* – пароль запрашивается еще и при запуске компьютера. В случае, когда доступ внутрь системного блока ограничен, данную опцию можно использовать в качестве одного из способов ограничения несанкционированного доступа к персональному компьютеру.
Clear User Password	Опция позволяет отключить использование пароля пользователя. Для изменения следует зайти в систему с паролем администратора.
User Access Level	Опция позволяет устанавливать уровень безопасности. Может принимать следующие значения: *No Access* – контроль отключен; *View Only* – разрешен только просмотр настроек; *Limited* – полный доступ разрешен только к ограниченному количеству опций; *Full Access* (по умолчанию) – разрешен полный доступ абсолютно ко всем настройкам.
First Boot Device (1st Boot Device)	Параметр определяет носитель для первоочередной загрузки системы. Если с данного устройства загрузиться невозможно, компьютер обратится к тем, которые указаны в параметрах *Second Boot Device* и *Third Boot Device*. С помощью этих параметров можно настроить любую

Наименование опции безопасности BIOS	Описание
	желаемую последовательность поиска операционной системы для загрузки. В качестве значений параметров могут использоваться: ***имена накопителей, которые могут быть подключены к плате***. Наиболее часто встречаются следующие обозначения: *Floppy* – дисковод; *HDD-0/1/2/3 (IDE-0/1/2/3)* – жесткий диск, подключенный к одному из IDE-каналов; *CDROM (CD/DVD)* – привод компакт-дисков и DVD; *USB FDD, USB CDROM, USB HDD, USB-ZIP* – одно из устройств с интерфейсом USB; *SCSI* – устройство с интерфейсом SCSI; *LAN (Network)* – загрузка через локальную сеть; *Disabled (None)* – устройства для загрузки нет; *имена фактически обнаруженных накопителей*. В этом случае значение параметра будет соответствовать названию устройства; ***названия категорий устройств***: *Removable* – загрузка со сменного носителя. Если их несколько, используется параметр *Removable Device Priority (Removable Drives*); *Hard Disk* – загрузка с жесткого диска. Если в системе не один жесткий диск, нужный накопитель следует выбирать с помощью параметра *Hard Disk Boot Priority (Hard Disk Drives);* *CDROM (CD/DVD)* – загрузка с компакт-диска. Нужное устройство из нескольких выбирается с помощью параметра *CDROM Boot Priority (CDROM Drives);* *Disabled* – устройство для загрузки не выбрано
Second Boot Device (2nd Boot Device), Third Boot Device (3rd Boot Device)	Параметры определяют второе и третье устройства для загрузки системы. Значения будут такими же, как и для параметра *First Boot Device*. Иногда можно встретить и четвертое загрузочное устройство (правда, необходимость в нем возникает крайне редко), обозначаемое параметром *4th Boot Device*.
Hard Disk Boot Priority (Hard Disk Drives)	Параметр определяет очередность загрузки с жестких дисков, если их несколько. В качестве значений может использоваться список дисков, подключенных к данной системной плате, а в новых версиях – список фактически обнаруженных дисков. Для перемещения устройства вверх или вниз в данном списке используйте клавиши +/ - на дополнительном цифровом блоке клавиатуры.
Removable Device Priority (Removable Drives)	Для загрузки компьютера с помощью этого параметра выбирается устройство со сменными носителями. Порядок использования аналогичен параметру *Hard Disk Boot Priority*.
Boot Other Device (Try Other Boot Device)	Параметр разрешает загрузиться с других устройств, которые не указаны явно в параметрах First/ Second/Third

Наименование опции безопасности BIOS	Описание
	Boot Device. Возможные значения: *Enabled* – загрузка с не указанных явно устройств разрешена; *Disabled* – для загрузки могут использоваться только те устройства, которые явно выбраны в параметрах First/Second/Third Boot Device.
Boot From Network (Boot From LAN)	Параметр разрешает загрузить компьютер с помощью локальной сети, для чего в ней должен быть сервер, обеспечивающий удаленную загрузку
Case Open Warning (Chassis Intrusion)	С помощью данного параметра можно включить контроль открытия корпуса компьютера, если он оборудован специальным датчиком. Возможные значения: *Enabled* - контроль открытия корпуса компьютера включен. Поведение системы после открытия корпуса и последующей перезагрузки зависит от модели платы (например, могут выдаваться предупреждения на экране, звуковые сигналы или выполняться блокировка загрузки с приглашением войти в Setup); *Disabled* - контроль вскрытия корпуса отключен; *Reset* – выбрав это значение, можно очистить сообщение об ошибке, после чего параметру снова будет присвоено значение *Enabled*. В некоторых платах для этого имеется отдельный параметр *Reset Case Open Status*.
USB Controller (OnChip USB Controller, OnChip EHCI Controller)	Параметр включает (значение Enabled (On)) или отключает (Disabled (Off)) встроенный USB-контроллер.
HDD S.M.A.R.T. Capability (HDD SMART Monitoring)	Параметр управляет утилитой S.M.A.R.T. (Self Monitoring Analysis and Reporting Technology), которая контролирует состояние жесткого диска, выявляет повреждения и по возможности устраняет их. Возможные значения: *Enabled* – утилита S.M.A.R.T. включена, что позволит заблаговременно выявлять дефекты диска; *Disabled* – утилита S.M.A.R.T. отключена. Хотя утилита S.M.A.R.T. повышает надежность хранения информации, она далеко не всегда может предупредить о приближающейся поломке диска. Поэтому, работая с важными данными, не забывайте о регулярном резервном копировании на сменные носители.
Load Fail-Safe Defaults (Load BIOS Setup Defaults)	Команда сбрасывает все настройки BIOS до значений по умолчанию. При этом устанавливаются наиболее безопасные значения всех параметров, обеспечивающие высокую стабильность работы системы.

Чтобы войти в настройку BIOS (BIOS Setup), следует во время первоначального тестирования компьютера (при его запуске) нажать определенную клавишу или их комбинацию. Наиболее часто используется клавиши **Delete**, **F9**, реже **F1** или **F2**; существуют и другие варианты (зависит от

версии BIOS). Узнать, за какой клавишей закреплен вход в BIOS Setup, можно из инструкции к системной плате или из подсказки, которая появляется во время прохождения процедуры инициализации системной платы и имеет, например, такой вид: *Press DEL to enter SETUP*.

Если инструкции к плате нет, а экранная подсказка отсутствует, рекомендуется последовательно попробовать наиболее известные варианты: **Delete**; одну из функциональных клавиш: **Fl**, **F2**, **F3**, **F10**, **F11**, **F12**; **Esc**; **Ctrl+Shift+S**, **Ctrl+Alt+S** или **Ctrl+Alt+Esc**.

В большинстве версий используется классический интерфейс главного окна программы BIOS Setup, в котором разделы размещены в два столбца (рис.3). Хотя у каждой модели системной платы свой уникальный набор параметров, названия основных разделов BIOS Setup, как правило, не меняются.

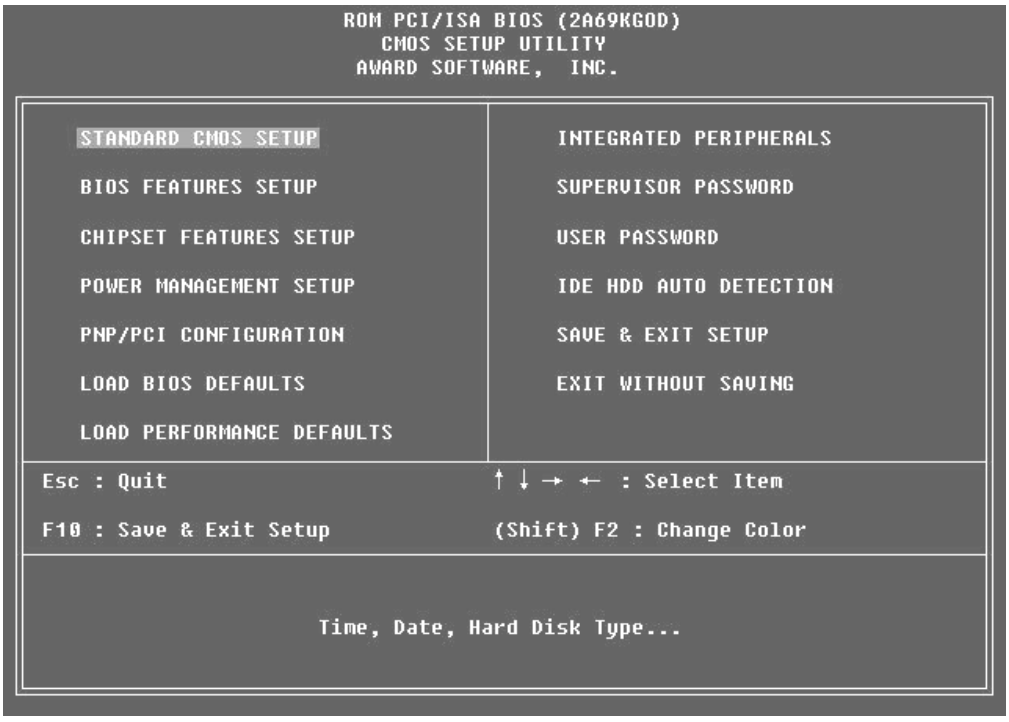


Рис. 3. Пример интерфейса главного окна программы BIOS Setup

Все разделы BIOS Setup имеют одинаковую структуру (рис. 4).

В верхней части окна выводится название текущего раздела или подраздела.

В левой части находится список доступных параметров выбранного раздела. Кроме отдельных параметров, могут присутствовать названия подразделов, обозначенные треугольными стрелками.

Справа от названий параметров выводятся их текущие значения. Если параметр и его значения отображаются бледным цветом, значит, либо он предназначен только для чтения, либо для его редактирования нужно изменить другой связанный параметр.

Рис. 4. Пример структуры раздела BIOS

В правой части окна обычно выводится краткая справка по выбранному параметру, а в нижней части – подсказка по использованию функциональных клавиш.

Для выхода из BIOS Setup существуют два способа:

с отменой всех внесенных изменений;

с сохранением всех внесенных изменений.

Для выхода с отменой внесенных изменений выберите в главном окне команду *Exit Without Saving*, после чего обычно появляется окно с сообщением *Quit Without Saving (Y/N)*?, в котором нужно нажать клавиши **Y** и **Enter**. Вы выйдете из BIOS Setup, а компьютер продолжит загрузку.

Выход с отменой изменений следует использовать в следующих случаях:

когда вы не планировали вносить каких-либо изменений, а только просматривали текущие значения параметров;

если вы не уверены в правильности действий либо случайно изменили один или несколько параметров.

Для выхода с сохранением всех внесенных изменений выберите в главном окне команду *Save & Exit Setup* – появится окно с сообщением *SAVE to CMOS and EXIT (Y/N)*? Нажмите клавиши **Y** и **Enter**, при этом все настройки будут сохранены, а компьютер продолжит загрузку. Если вы передумали вносить изменения в CMOS, нажмите **N** и **Enter** или же воспользуйтесь клавишей **Esc**.

Выход с сохранением изменений используйте только в том случае, если вы уверены в правильности своих действий и не допустили ошибок или оплошностей, редактируя параметры.

Последовательность сброса (обнуления) настроек BIOS обычно выглядит следующим образом:

1. Выключите компьютер и отсоедините питание от системного блока.

2. Откройте крышку системного блока и установите на несколько секунд перемычку в положение Clear CMOS.

3. Верните перемычку в прежнее положение, соберите и включите компьютер.

ВНИМАНИЕ: не переставляйте перемычку при включенном питании, а также не включайте компьютер, если перемычка находится в состоянии Clear CMOS.

В большинстве системных плат для очистки CMOS необходимо переставить перемычку из положения 1-2 в положение 2-3 (рис. 5, слева). Иногда присутствуют только два контакта, которые нужно замкнуть на несколько секунд (рис. 5, справа). В некоторых платах может быть установлен микропереключатель или кнопка для очистки CMOS.

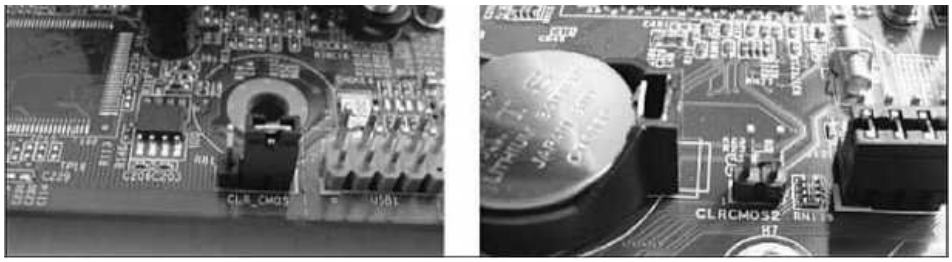


Рис. 5. Трех- и двухконтактная перемычка для очистки CMOS

Если перемычки или переключателя для очистки CMOS нет, можно попробовать такой способ.

1. Отключите питание, откройте системный блок и извлеките батарейку из гнезда (если она припаяна к системной плате, этот способ не подойдет).

2. Через 10-20 минут вставьте батарейку обратно и запустите компьютер.

Если данные действия не привели к очистке CMOS, можно попробовать оставить системную плату без батарейки на сутки.

2. Аутентификация, авторизация и управление доступом в ОС Windows. Управление квотами дискового пространства

Требования, предъявляемые Инструкцией к техническим (программным) средствам защиты информации на АРМ, взаимодействующем с автоматизированной информационной системой, предполагают обязательную реализацию механизмов аутентификации и авторизации.

Аутентификация (установление подлинности) – проверка принадлежности субъекту доступа предъявленного им идентификатора (в качестве идентификатора обычно используется имя пользователя) и подтверждение его подлинности. Другими словами, аутентификация заключается в проверке: является ли подключающийся субъект тем, за кого он себя выдает.

Аутентификация применяется для ограничения доступа случайных и незаконных субъектов (пользователи, процессы) информационных систем к ее объектам (аппаратные, программные и информационные ресурсы). Каждый

пользователь должен проходить аутентификацию перед началом работы на АРМ. Для этого он должен иметь учетную запись, определяющую его как пользователя АРМ.

Учётная запись пользователя – это запись, которая содержит сведения, необходимые для идентификации пользователя при подключении к системе, а также информацию для авторизации и учёта. Это имя пользователя и пароль (или другое аналогичное средство аутентификации – например, биометрические характеристики).

Авторизация – предоставление определённому лицу или группе лиц прав на выполнение определенных действий, а также процесс проверки (подтверждения) данных прав при попытке выполнения этих действий. Часто можно услышать выражение, что пользователь «авторизован» для выполнения данной операции – это значит, что он имеет на неё право. Авторизация позволяет системе определить, может ли заверенный пользователь получить доступ и возможность обновить защищенные системные ресурсы.

Управление доступом в ОС Windows заключается в предоставлении пользователям, группам и компьютерам определенных *прав на доступ* к данным объектам, а также *управлении квотами дискового пространства*.

Указанная функция доступна только в файловой системе NTFS.

В таблице 1 приведены уровни разрешений, которые обычно доступны для файлов и папок.

Рассмотрим в качестве примера настройку прав доступа (например: *только чтение и выполнение, просмотр содержимого*) к файловой папке «D\Документы (приказы)» для пользователя **Гость 1** (тип учетной записи – *стандартная*). В системе имеется также учетная запись **User**, обладающая правами *администратора* (рис 6).

Таблица 1

Уровень разрешений	**Описание**
Полный доступ	Пользователи могут просматривать содержимое файла или папки, изменять существующие файлы или папки, создавать новые файлы и папки и запускать программы, расположенные в папке.
Изменение	Пользователи могут изменять существующие файлы и папки, но не могут их создавать.
Чтение и выполнение	Пользователи могут просматривать содержимое существующих файлов и папок, а также запускать программы, расположенные в папке.
Чтение	Пользователи могут просматривать содержимое папки и открывать файлы и папки.
Запись	Пользователи могут создавать новые файлы и папки, а также изменять существующие файлы и папки.

Рис. 6. Учетные записи, доступные для настройки в Панели управления.

Решение данной задачи предполагает выполнение следующих действий:

1. Нажимаем правой кнопкой мыши на папку «Документы (приказы)». В контекстном меню выбираем пункт «Свойства». В открывшемся окне «Свойства: Документы (приказы)» открываем вкладку «Безопасность». Обращаем внимание, что какие-то группы и пользователи уже имеют доступ к данной папке. Эти права были унаследованы от своего «родителя» – диска D (рис. 7).

2. Теперь удаляем лишние права, оставляя *Полный доступ* только для субъектов *«Администратор»* и «*Система»*. Для этого нажимаем на кнопку «Дополнительно». Откроется диалоговое окно «Дополнительные параметры безопасности для “Документы (приказы)”». Выделяем по очереди субъекты (например, «Прошедшие проверку» и «Пользователи») и удаляем кнопкой «Удалить» (рис. 8).

3. Прерываем наследование прав от «родителя». Для этого в диалоговом окно «Дополнительные параметры безопасности для “Документы (приказы)”». включаем параметр «Заменить все разрешения дочернего объекта на разрешения, наследуемые от этого объекта» и нажимаем кнопку «Отключить наследования». Подтверждаем замену явно заданных разрешений для всех потомков объекта на наследуемые разрешения (рис. 8).

4. Нажимаем кнопку «Ок» в диалоговом окне «Дополнительные параметры безопасности для “Документы (приказы)”» и возвращаемся к простому виду окна «Свойства: Документы (приказы)» (рис. 9).

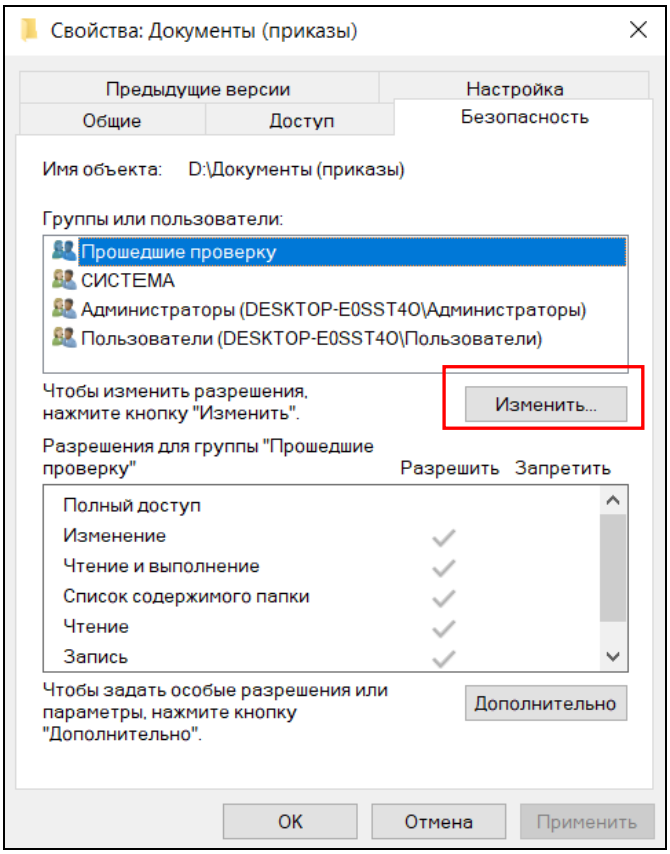


Рис. 7. Диалоговое окно «Свойства» объекта, вкладка «Безопасность».

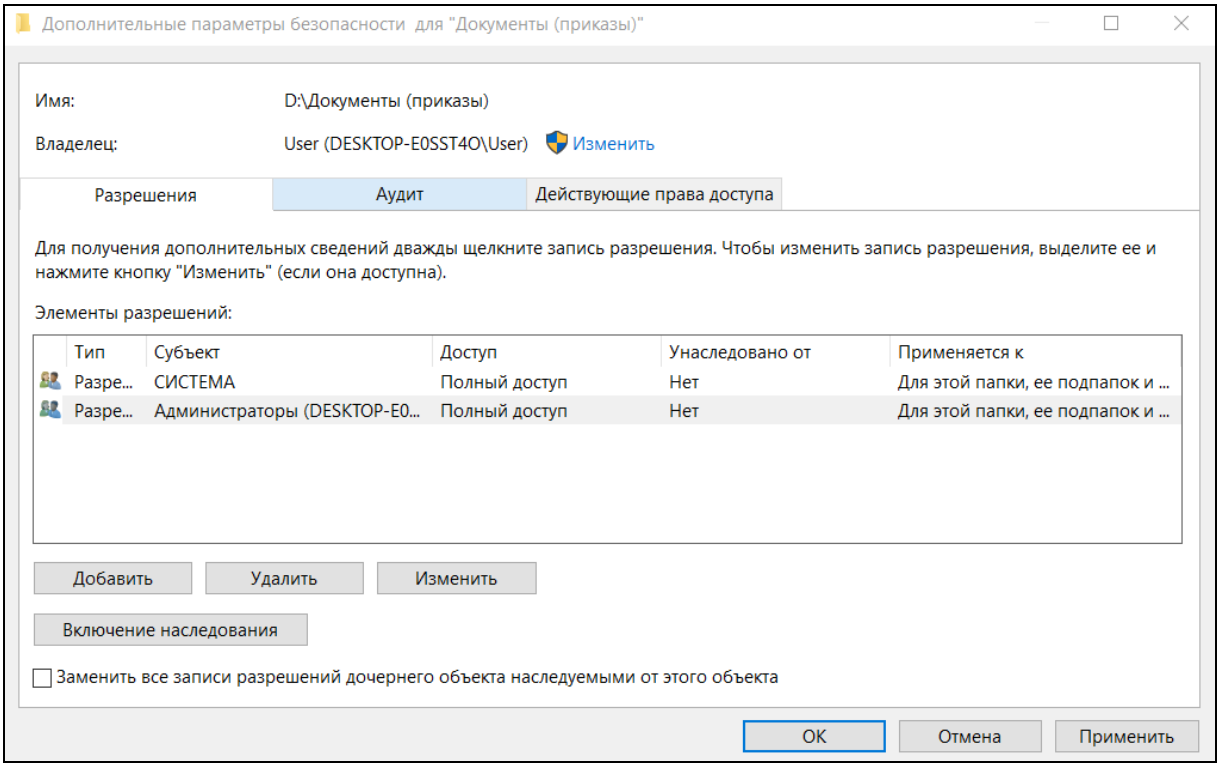


Рис. 8. Диалоговое окно «Дополнительные параметры безопасности»

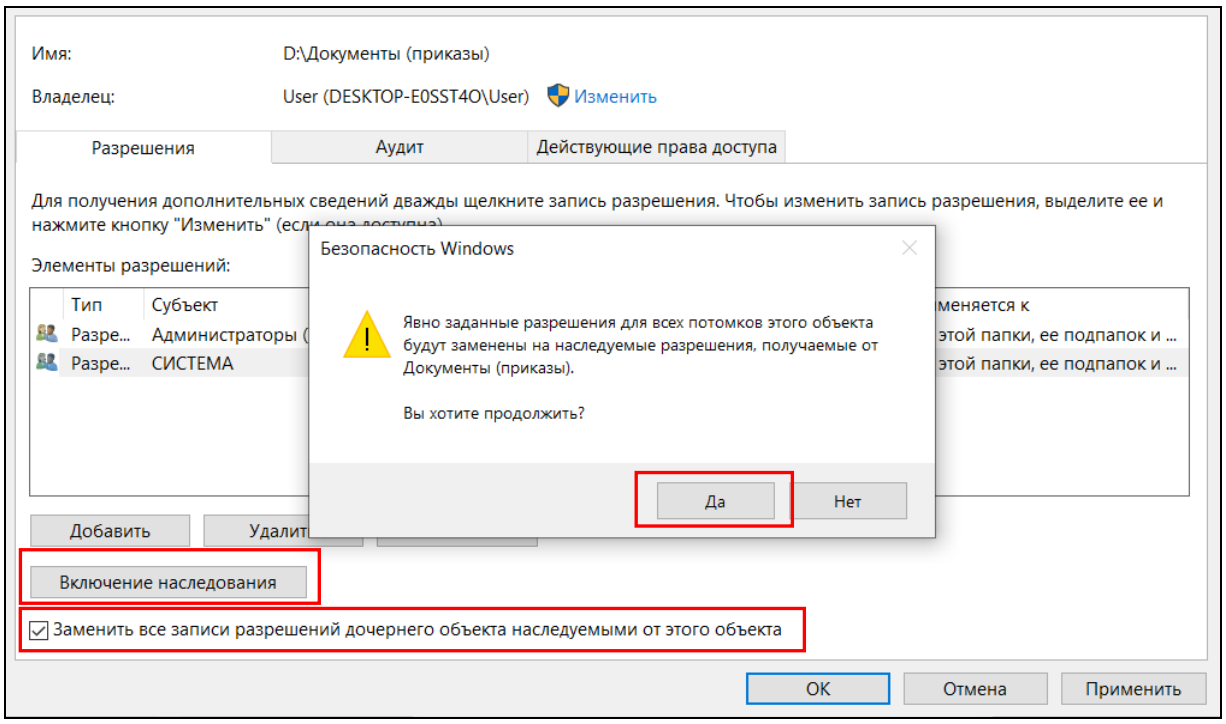


Рис. 8. Учетные записи, доступные для настройки в Панели управления.

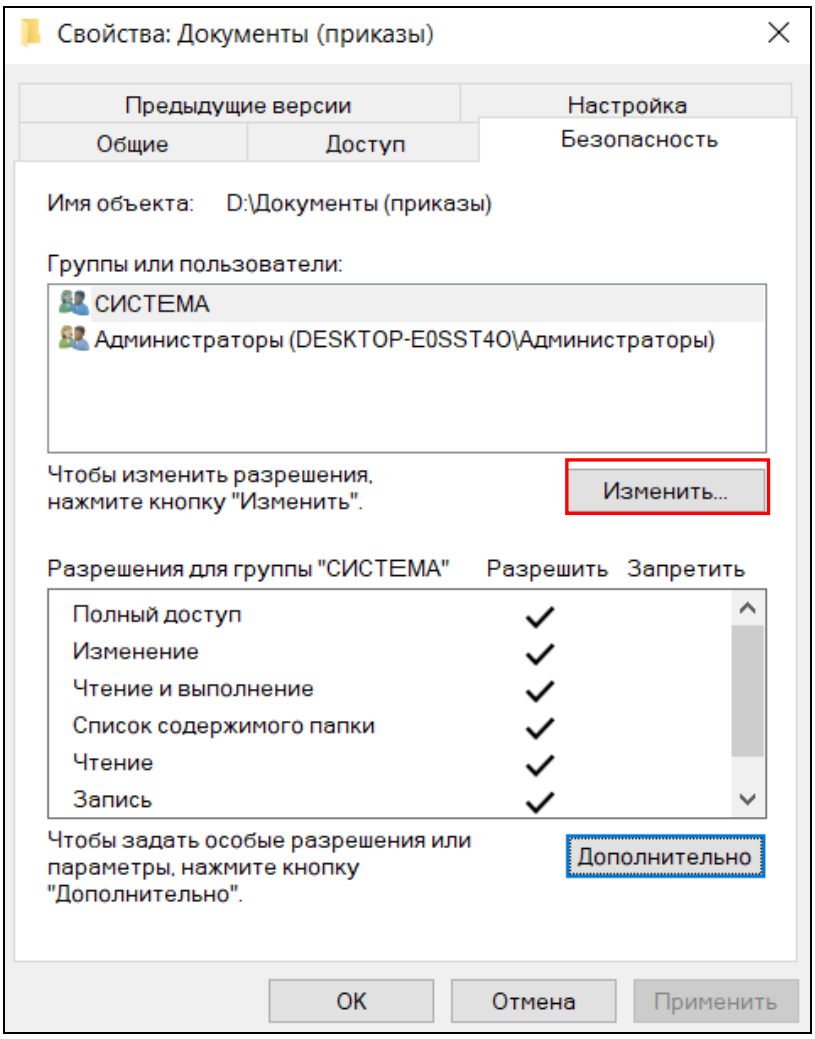


Рис. 9. Диалоговое окно «Свойства» объекта, вкладка «Безопасность».

5. Нажимаем кнопку «Изменить», а затем «Добавить». В поле «Введите имена выбираемых объектов» открывшегося диалогового окна «Выбор: Пользователи” или “Группы”» вводим наименование учетной записи **Гость1** и нажимаем на кнопку «Проверить имена» (рис. 10). Для завершения выбора нажимаем «Ок».

Аналогично добавляем наименование учетной записи **User**.

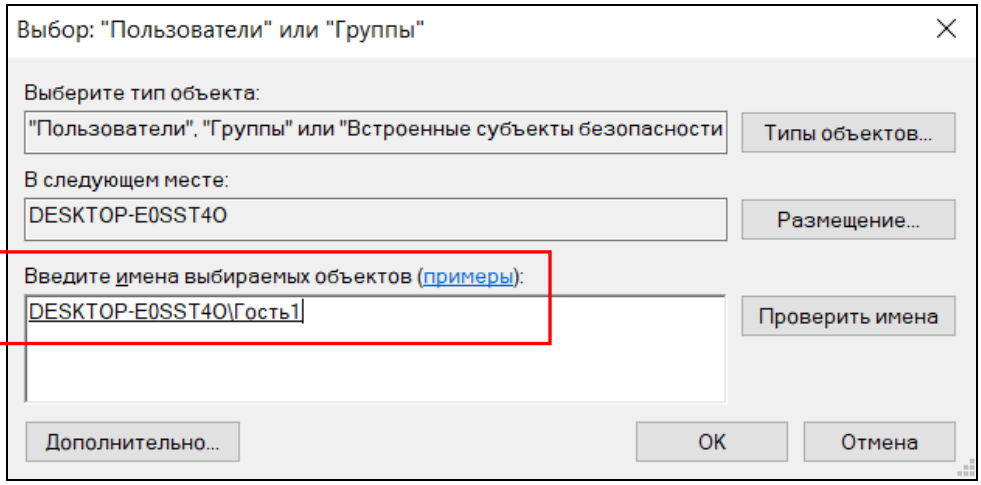


Рис. 10. Диалоговое окно «Выбор: Пользователи” или “Группы”»

6. Для установления прав доступа нажимаем кнопку «Изменить», в области «Группы или пользователи» выделяем нужный субъект, устанавливаем соответствующие параметры разрешения и запрета (рис. 11). Затем нажимаем «Ок».

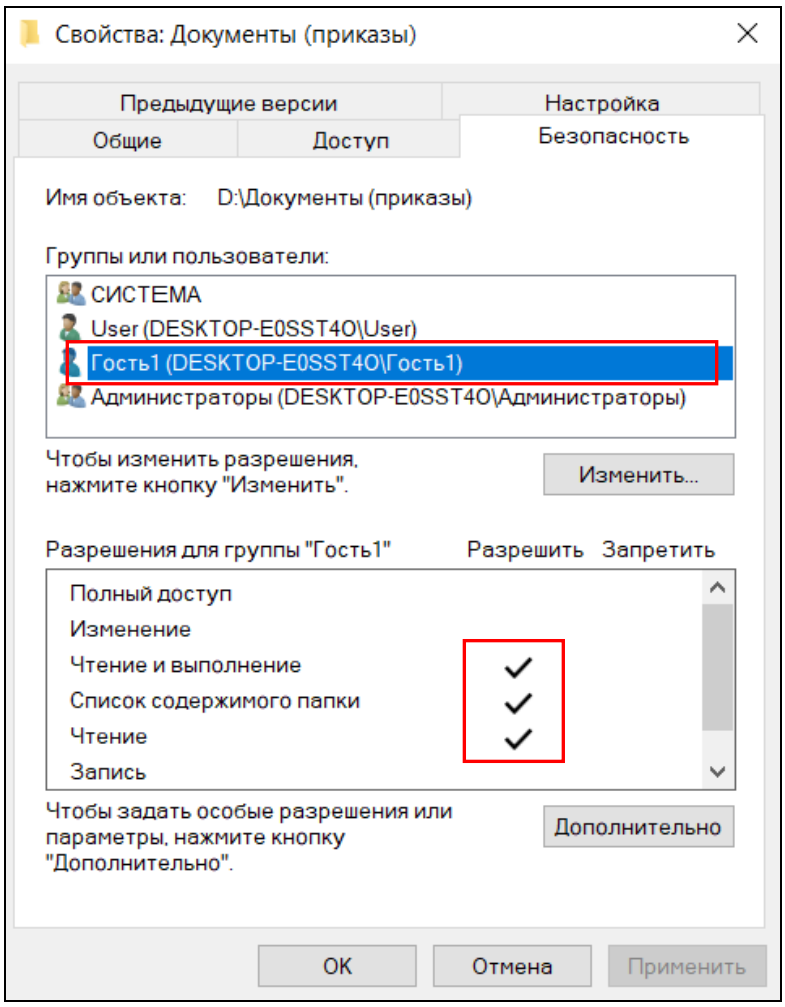


Рис. 11. Учетные записи, доступные для настройки в Панели управления.

Для каждого пользователя администратор может задать также квоты дискового пространства, после чего пользователь сможет хранить на томе ограниченный объем данных. Управление квотами дискового пространства локального компьютера осуществляется путем изменения определенных параметров на вкладке «Квота» диалогового окна «Свойства» соответствующего объекта (рис. 11).

Если пользователь превышает выданную ему квоту, в журнал событий вносится соответствующая запись (рис. 12). Затем, в зависимости от конфигурации системы, пользователь либо сможет записать информацию на том (более «мягкий» режим ограничений), либо ему будет отказано в записи из-за отсутствия свободного пространства («жесткий» режим).

Квоты можно использовать на локальных и общих дисках (в этом случае общий доступ должен быть разрешен на уровне корневого каталога тома).

Сжатие файлов не имеет значения при вычислении занятого пространства – всегда учитывается размер исходного несжатого файла.

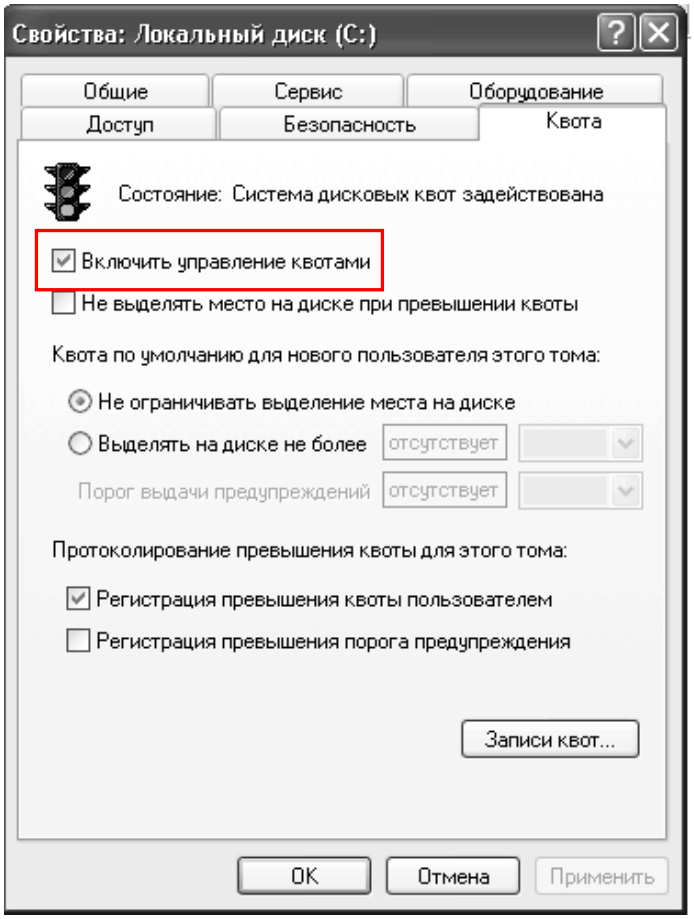


Рис.11. Управление квотами дискового пространства.

Устанавливать и просматривать квоты на диске можно только в разделе с NTFS и при наличии необходимых полномочий (задаваемых с помощью локальных или доменных групповых политик) у пользователя, устанавливающего квоты. По умолчанию для работы с квотами нужно быть членом группы Администраторов.

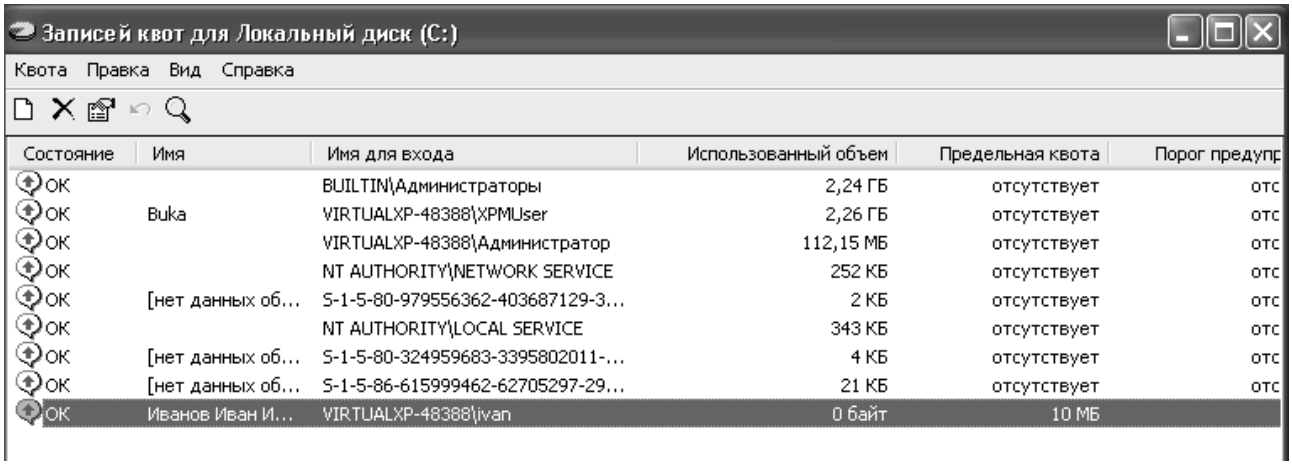


Рис.12. Управление квотами дискового пространства.

3. Политики безопасности ОС

Краткие теоретические сведения:

Политики безопасности ОС Windows: общие сведения

Безопасность операционной системы основана на определенных правилах, регулирующих различные аспекты ее функционирования. Совокупность этих правил составляют единую политику безопасности. В Windows 2000 и более поздних NT-образных операционных системах политика безопасности представляет собой две группы правил:

локальная политика безопасности, применяемая только к локальному компьютеру или пользователям (группе локальных пользователей). При этом, локальная политика является частью групповой политики безопасности;

локальная групповая политика безопасности, применяется в сетях, в которых присутствует контроллер домена – сервер, распространяющий политики на группу ПК в сети. Локальная групповая политика предоставляет сетевым администраторам возможность назначать определенные параметры рабочей среды для групп пользователей или компьютеров. Эти настройки применяются, когда пользователь из группы входит в систему на сетевом компьютере, или всякий раз, когда запускается ПК в группе.

Локальные и групповые политики безопасности позволяют управлять различными штатными средствами системы:

политики для настройки встроенного брандмауэра Windows;
политики для управления электропитанием;
политики для настройки панели управления, панели задач и др.
политики для настройки антивирусной защиты;
политики для управления подключаемых устройств;
политики для настройки штатных средств шифрования
политики для настройки штатного браузера;
политики для настройки беспроводных сетей и др.

Локальные групповые политики безопасности ОС Windows.

Для настройки параметров локальной групповой политики безопасности в операционной системе MS Windows 10 используется оснастка[2] «Редактор локальной групповой политики». Данная оснастка служит для просмотра и редактирования объектов групповой политики (GPO), в которых хранятся параметры локальных политик безопасности для ПК и пользователей.

Оснастка «Редактор локальной групповой политики» запускается командой *gpedit.msc* в окне «Выполнить» (Win+R). Для удобства можно добавить ярлык оснастки на рабочий стол. Для этого необходимо открыть *C:\Windows\System32*, выбрать правой клавишей мыши *gpedit* и отправить ярлык на *Рабочий стол*.

[2]Оснастка в Windows – программа, позволяющая настроить разные параметры операционной системы.

Оснастка «Редактор локальной групповой политики позволяет изменять политики, распространяющиеся как на компьютеры, так и на пользователей (учетные записи).

В панели пространства имен оснастки «Редактор локальной групповой политики» представлено два узла: *Конфигурация компьютера* и *Конфигурация пользователя* (рис. 1).

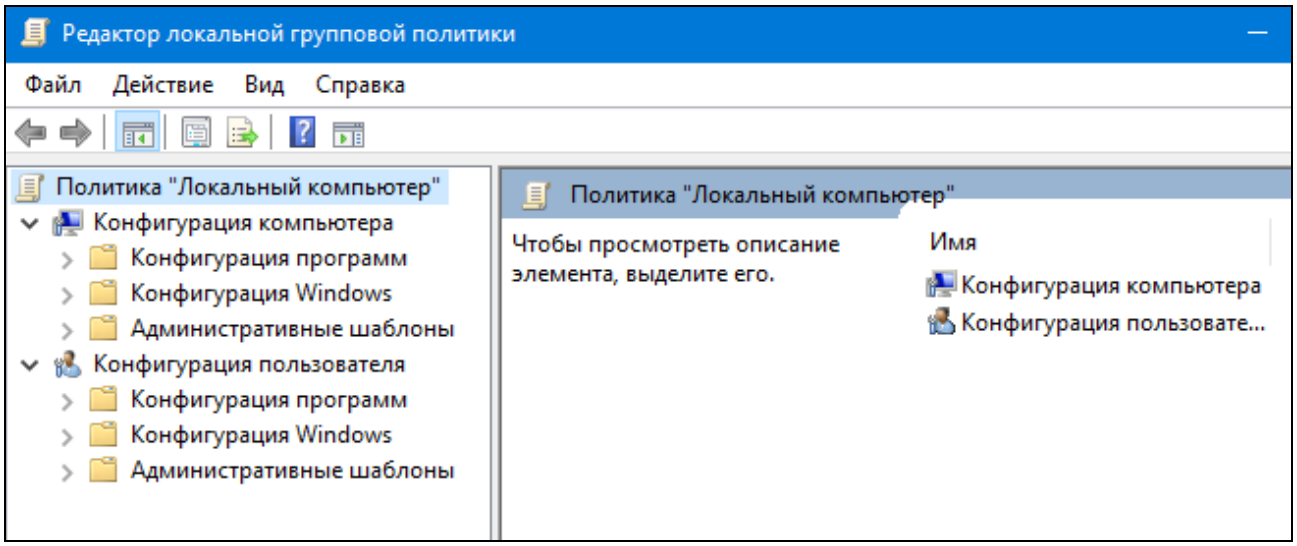


Рис. 1. Редактор локальной групповой политики

Узел *Конфигурация компьютера* содержит общесистемные настройки, определяющие работу ПК. Эти политики регулируют функционирование операционной системы, определяют права пользователей в системе, работу системных служб и средств безопасности и т. д.

Узел *Конфигурация пользователя* содержит пользовательские настройки, определяющие работу пользователей ПК (вид рабочего стола, параметры выполняющихся приложений, средств обеспечения безопасности и пользовательских сценариев входа и выхода и пр.).

В вышеприведенных узлах находятся по три дочерних узла (*конфигурация программ*, *конфигурация Windows*, *административные шаблоны)*, при помощи которых настраиваются все параметры локальных объектов групповых политик.

Примечание: локальная групповая политика в Windows 10 с определенным интервалом времени автоматически совершает обновление реестра. Это делается для сохранения его рабочего состояния. Как правило, интервал времени находится в диапазоне от 30 до 90 минут. Однако, при желании, его всегда можно изменить. Для некоторых политик, чтобы изменения вступили в силу сразу, необходимо в окне «Выполнить» ввести следующую команду: *gpupdate /force.*

Если необходимо чтобы изменения локальных групповых политик вступили в силу немедленно, можно принудительно применить измененные параметры, которые были внесены в редакторе локальной групповой политики несколькими способами:

а) осуществить перезагрузку операционной системы;

б) использовать утилиту *gpupdate.exe* для принудительного обновления групповой политики. Для этого необходимо либо в окне «Выполнить» (Win+R), либо в командной строке ввести *gpupdate /force* и нажать «Ок».

С использованием параметра */target* можно указать, будет ли это обновление параметров применяться только для конкретного пользователя или только для компьютера. Если не указано, обновляются параметры обеих политик.

Так, для выполнения обновления политик для конкретного пользователя, необходимо ввести команду *gpupdate /target:user*.

В качестве примера настройки локальных групповых политик безопасности рассмотрим механизм включения параметра «*Предупреждение и предотвращение обхода*» для встроенной функции Windows SmartScreen.

Функция SmartScreen помогает защищать компьютеры, предупреждая пользователей перед запуском нераспознанного или заведомо вредоносного приложения. Для этого она использует облачную систему рейтинга сайтов и файлов, по которой проводится проверка исполняемых файлов при первом запуске.

При включении соответствующей политики с параметром «*Предупреждение и предотвращение обхода*», диалоговое окно SmartScreen не будет предоставлять пользователю возможность игнорировать предупреждение и запустить опасное приложение.

Механизм выполнения данной задачи будет состоять из следующих действий:

1. Войти в систему под учетной записью администратора.

2. Запустить оснастку «Редактор локальной групповой политики» (Win+R > *gpedit.msc* > Enter).

3. Последовательно развернуть элементы оснастки *Конфигурация компьютера* > *Административные шаблоны* > *Компоненты Windows* > *Проводник* в окне Редактора локальной групповой политики.

4. В правой части Редактора откройте параметр *Настроить Windows SmartScreen*. Установите состояние параметра в положение *Включено*. В блоке *Параметры* выберите подходящий вариант работы фильтра: *Предупреждение и предотвращение обхода* (рис. 2).

Для завершения нажать кнопку «Ок»

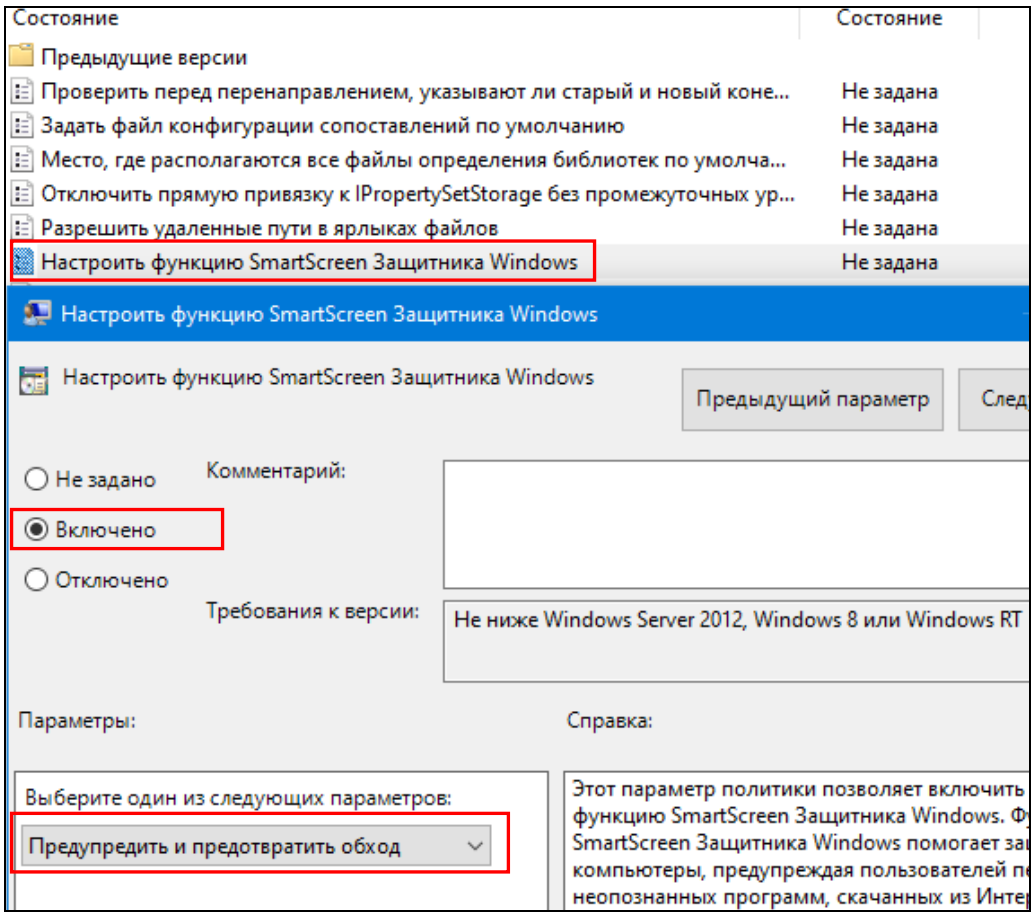


Рис. 2. Настройка функции Windows SmartScreen
с помощью Редактора локальной групповой политики

7. Закрыть Редактор локальной групповой политики. Чтобы изменения вступили в силу сразу, необходимо в окне «Выполнить» ввести следующую команду: *gpupdate /force*. Проверить результат.

Примечание: изменения, которые вносятся через редактор локальной групповой политики, будут применены для всех учетных записей, зарегистрированных в системе, включая учетную запись администратора, который инициировал изменения.

Локальные политики безопасности ОС Windows.

Оснастка *локальной политики безопасности* запускается командой *secpol.msc* и ограничивает настройку объектов локальной политики следующими параметрами и политиками (рис. 3):

Политики учетных записей. Определяют работу с паролями, а также условия блокировки учетных записей.

Локальные политики. Включают правила аудита событий, назначения привилегий пользователям и группам, а также некоторые возможности защиты.

Брандмауэр Windows в режиме повышенной безопасности. Определяют правила блокировки либо разрешения для программ, портов или предопределенных соединений.

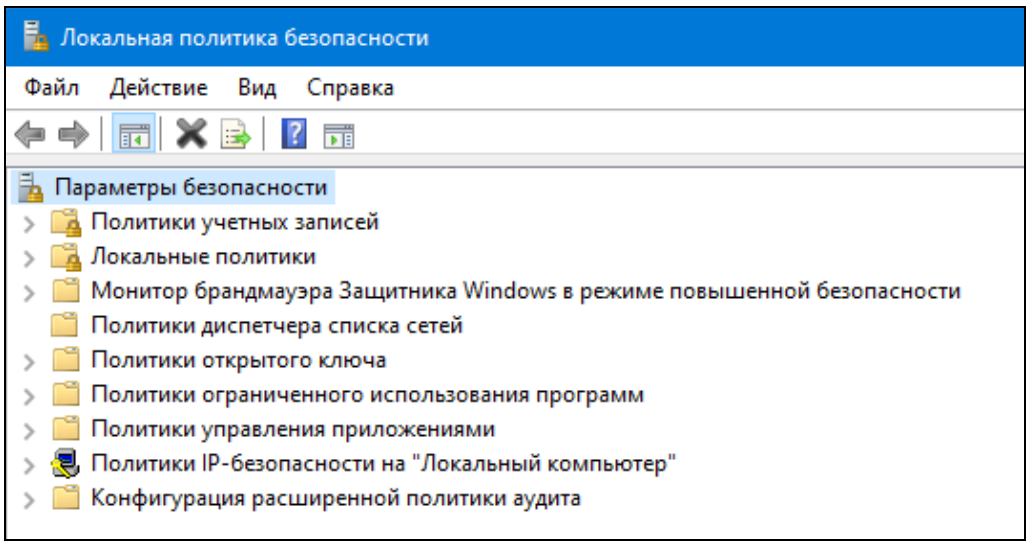


Рис. 3. Локальные политики безопасности Windows

Политики диспетчера списков сетей. Параметры безопасности, которые можно использовать для настройки различных аспектов того, как сети перечислены и отображаются на одном устройстве или на нескольких устройствах

Политики открытого ключа. Позволяют настроить, в частности, правила использования файловой системы с шифрованием EFS (Encrypted File System).

Политики ограниченного использования программ. Основанная на групповых политиках функция, которая выявляет программы, работающие на компьютерах в домене (сети), и управляет возможностью выполнения этих программ.

Политики управления приложениями. Определяет настройки инструмента «AppLocker», который включает в себя множество самых разнообразных функций и настроек, позволяющих регулировать работу с программами. Например, он позволяет создать правило, ограничивающее запуск всех приложений, кроме указанных, либо установить ограничение на изменение файлов программами, задав отдельные аргументы и исключения.

Политики безопасности IP на локальном компьютере. Определяют возможности самостоятельной настройки неограниченного количества правил безопасности (методы шифрования, ограничения на передачу и прием трафика, фильтрация по IP-адресам, разрешение или запрет на подключение к сети и пр.)

Настройка политики расширенной проверки. Включают правила аудита событий, назначения привилегий пользователям и группам и некоторые возможности защиты.

В качестве примера настройки локальной политики безопасности рассмотрим реализацию защиты пользователей ПК от атак с попыткой перехвата паролей. Для этого осуществим настройку параметра «*Интерактивный вход в систему: не требовать нажатия CTRL+ALT+DEL*». Этот параметр безопасности определяет, требуется ли нажатие клавиш CTRL+ALT+DEL перед входом в систему. Если эта политика включена либо не настроена, нажатие клавиш CTRL+ALT+DEL перед входом в систему не

требуется. Обязательное же нажатие клавиш CTRL+ALT+DEL перед входом в систему гарантирует передачу данных по доверенному каналу при вводе паролей пользователями.

Кроме того, в целях безопасности следует также отключить отображение учетных данных последнего пользователя, выполнившего вход на этом компьютере, а также на экране входа в Windows. За соответствующие настройки отвечают параметры «*Интерактивный вход в систему: не отображать имя пользователя при входе в систему*» и «*Интерактивный вход в систему: не отображать учетные данные последнего пользователя*».

Алгоритм реализации поставленной задачи состоит из следующих действий:

1. Войти в систему под учетной записью администратора.
2. Запустить оснастку «Редактор локальной политики безопасности» (Win+R > *secpol.msc* > Enter).
3. Последовательно развернуть элементы оснастки *Локальные политики* > *Параметры безопасности* в окне Редактора.
4. В правой части Редактора откройте параметр *Интерактивный вход в систему: не требовать нажатия CTRL+ALT+DEL*. Установите состояние параметра в положение *Отключен*. (рис. 4).
5. В правой части Редактора откройте параметр *Интерактивный вход в систему: не отображать учетные данные последнего пользователя*. Установите состояние параметра в положение *Включен*.
6. В правой части Редактора откройте параметр *Интерактивный вход в систему: не отображать имя пользователя при входе в систему*. Установите состояние параметра в положение *Включен*. Для завершения нажмите кнопку «Ок». Закройте Редактор локальной политики безопасности.

Примечание: внесение любых изменений непосредственно в окне редактора будет иметь силу для всех учётных записей: и для администратора, и для стандартных пользователей.

Таким образом, редакторы групповой и локальной политик безопасности Windows реализуют *стандартную локальную групповую политику* (первый уровень), позволяющую изменять системные и пользовательские настройки, которые будут применены для всех пользователей операционной системы, а также домена (сети).

Для того, чтобы настроить политики безопасности для конкретных пользователей, в операционной системе Windows предусмотрена дополнительная многоуровневая локальная групповая политика:

групповая политика для администраторов и не администраторов (второй уровень). Эта групповая политика содержит только конфигурационные параметры пользователя и применяется в зависимости от того, является ли используемая учетная запись пользователя членом локальной группы *Администраторы* или нет;

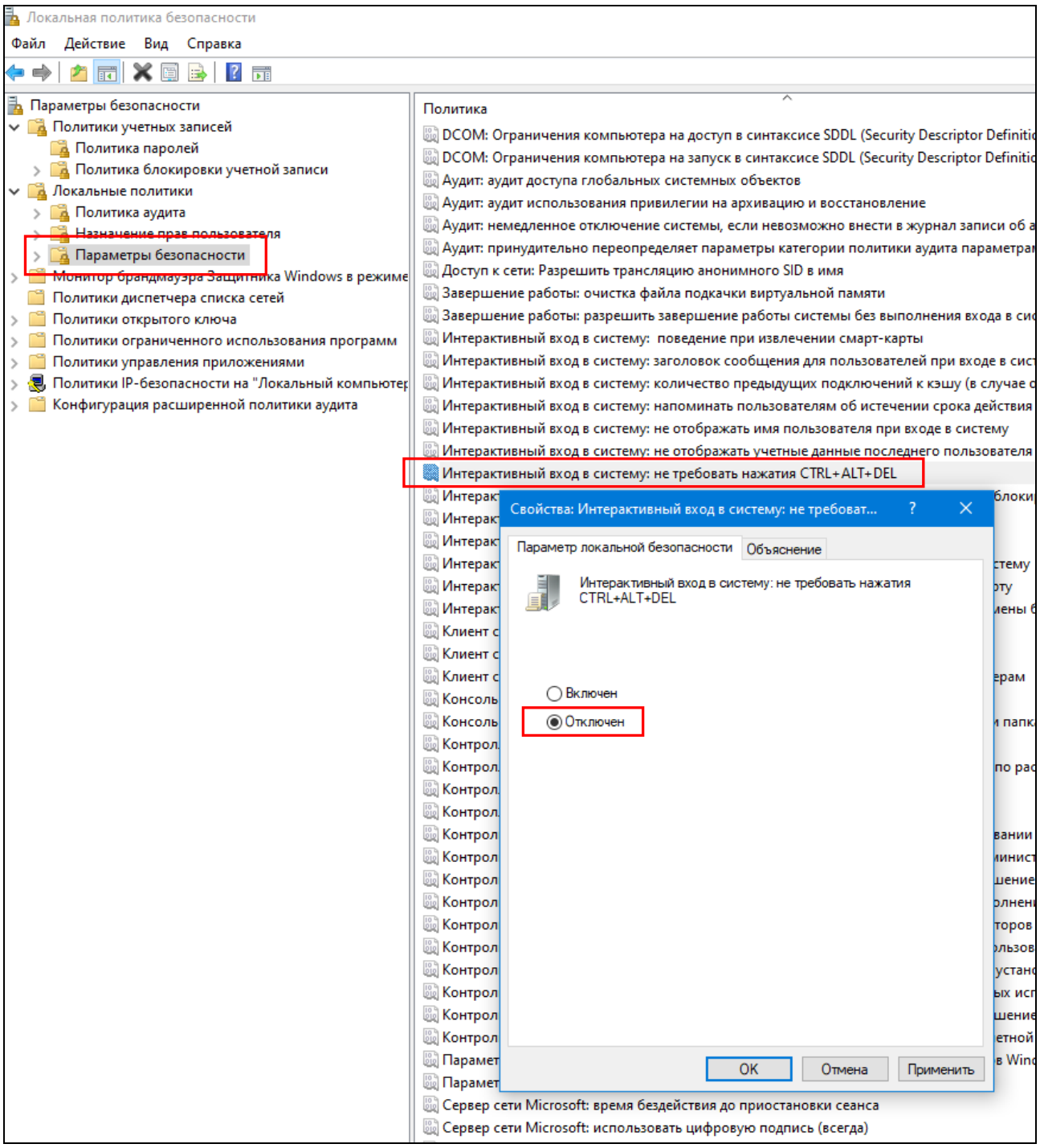


Рис. 4. Пример настройки одного из параметров локальной политики безопасности

групповая политика для конкретного пользователя (третий уровень). Эта групповая политика содержит только конфигурационные параметры конкретного пользователя.

Возможность управления политиками безопасности в части применения изменений не для всех, а лишь для выбранных пользователей, может быть реализована с помощью консоли MMC.

Консоль MMC в Windows – это специальная панель (пульт) управления различными оснастками Windows. С помощью консоли MMC можно

самостоятельно создать свою собственную панель управления, в которой будут собраны необходимые инструменты администрирования (оснастки), например:

Брандмауэр Windows;

Локальные пользователи и группы;

Диспетчер устройств;

Общие папки;

Просмотр событий;

Редактор групповых политик;

Сертификаты;

Службы;

Управление дисками;

и др.

Для разных задач и проектов можно создать отдельную консоль управления и сохранить ее под определенным именем.

Рассмотрим последовательность действий, позволяющих настроить политики безопасности для конкретных пользователей с помощью консоли управления MMC.

Добавление объекта групповой политики второго уровня:

1. Войти в систему под учетной записью администратора.

2. Запустить консоль управления MMC (Win+R > *mmc* > Enter).

3. В окне «Добавление и удаление оснасток» добавить новую оснастку «Редактор объектов групповой политики».

2. В мастере групповой политики в поле *Объект групповой политики* нажать кнопку «Обзор».

3. На вкладке *Пользователи* выбрать значение «*Администраторы»* и нажать кнопку «Ок» и «Готово» (рис. 5).

Добавление объекта групповой политики третьего уровня:

1. Войти в систему под учетной записью администратора.

2. Запустить консоль управления MMC (Win+R > *mmc* > Enter).

3. В окне «Добавление и удаление оснасток» добавить новую оснастку «Редактор объектов групповой политики».

4. В мастере групповой политики в поле *Объект групповой политики* нажать кнопку «Обзор».

5. На вкладке *Пользователи* выбрать нужную учетную запись.

6. Нажать кнопку «Ок», чтобы закрыть диалоговое окно «Добавление и удаление оснасток».

Для удобства, используя команды в главном меню *Файл > Сохранить как,* можно сохранить файл консоли управления на рабочем столе под определенным именем для последующего редактирования заданных политик.

Таким образом, используя данную консоль, можно настраивать политики для определенных пользователей ПК либо домена (сети).

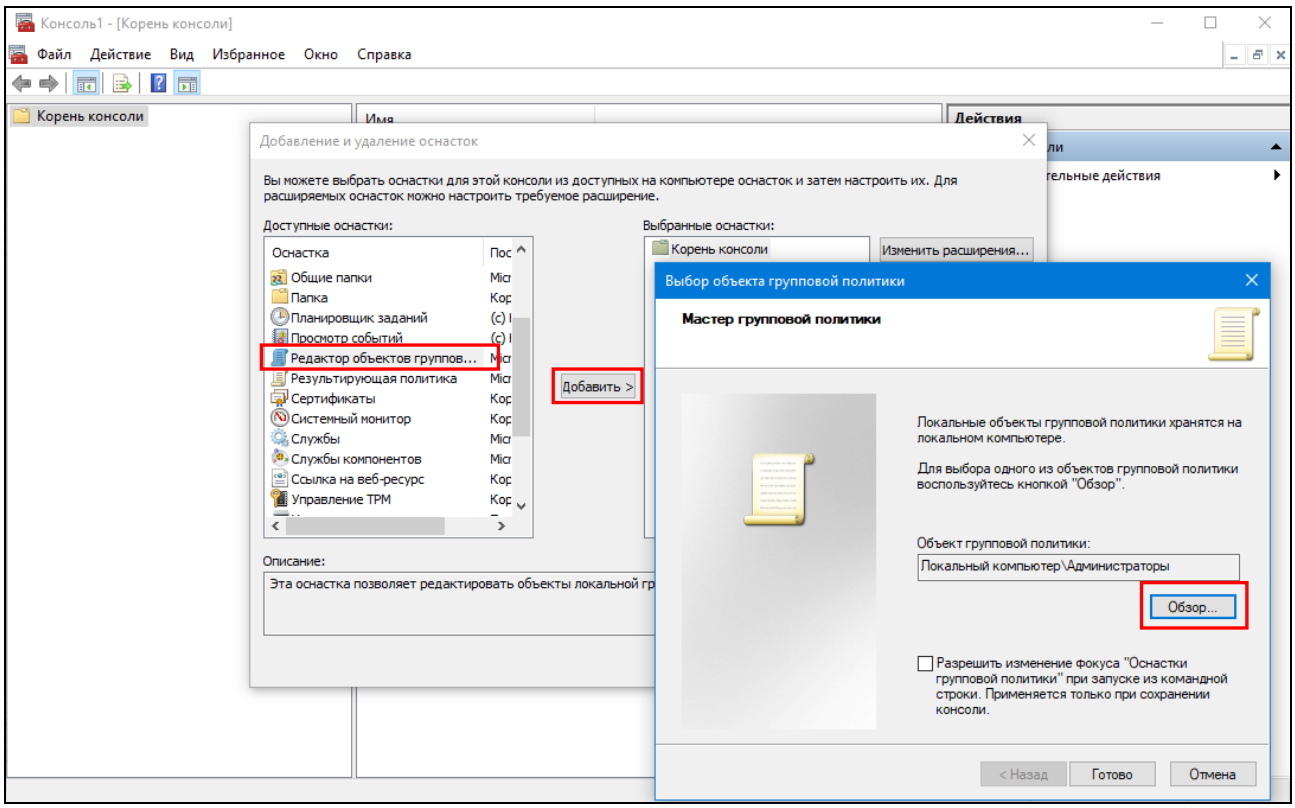


Рис. 5. Пример настройки одного из параметров локальной политики безопасности

Сервис AppLocker: общие сведения и сценарии использования

В условиях, когда информационные ресурсы являются одним из наиболее ценных активов, крайне важно обеспечить доступ к ним только авторизованным пользователям. Имеющиеся в ОС Windows технологии управления доступом позволяют достаточно эффективно контролировать, к чему пользователи могут получить доступ. Однако если пользователь запускает процесс, этот процесс имеет тот же уровень доступа к данным, что и у пользователя. В результате конфиденциальные либо критически важные сведения могут быть без труда удалены или переданы за пределы контролируемой зоны, если пользователь намеренно или случайно запускает вредоносное программное обеспечение. Разнообразие форм вредоносного программного обеспечения значительно усложняет понимание пользователями того, что безопасно запускать, а что нет. Активированное вредоносное ПО может повредить содержимое жесткого диска, заполнить сеть запросами, вызвав атаку по типу «отказ в обслуживании» (DoS), передать конфиденциальные сведения в Интернет или нарушить безопасность компьютера.

Кроме того, разработчики программного обеспечения создают все больше приложений, которые могут быть установлены пользователями, не являющимися администраторами. Это может нарушить политику безопасности организации либо подразделения и позволит обойти традиционные решения по управлению приложениями, которые полагаются на невозможность установки приложений пользователями.

Устранить подобные уязвимости системы безопасности можно с помощью интегрированного сервиса AppLocker, который позволяет ограничить возможности запуска нежелательного (и потенциально злонамеренного) ПО пользователями или группами.

Сервис AppLocker идеально подходит для организаций либо подразделений, которые используют групповую политику для управления своими компьютерами.

Ниже приведены примеры сценариев, при которых может использоваться AppLocker:

политика безопасности вашей организации определяет использование только лицензионного программного обеспечения, поэтому нужно запретить пользователям запускать нелицензионное программное обеспечение, а также ограничить использование лицензионного программного обеспечения только авторизованными пользователями;

приложение больше не поддерживается вашей организацией, поэтому вам необходимо предотвратить его использование всеми пользователями;

возможность того, что нежелательное программное обеспечение может появиться в среде, достаточно высока, поэтому необходимо снизить эту угрозу;

лицензия на приложение была отозвана или истек срок ее действия в вашей организации, поэтому вам необходимо предотвратить возможность ее использования всеми пользователями;

развернуто новое приложение или новая версия приложения, и вам необходимо запретить пользователям запускать старую версию;

отдельные программные средства не разрешены в организации, или только определенные пользователи имеют доступ к этим средствам;

отдельный пользователь или небольшие группы пользователей должны использовать определенное приложение, в доступе к которому отказано всем прочим пользователям;

некоторые компьютеры в организации совместно используются пользователями, которые имеют различные потребности в плане программного обеспечения, а вам необходимо защитить определенные приложения;

помимо других мер вам необходимо управлять доступом к конфиденциальным данным через использование приложений.

Таким образом, сервис AppLocker поможет вам защитить цифровые активы вашей организации, снизить угрозы, связанные с использованием вредоносного ПО в вашей среде, и улучшить управление приложениями и поддержку политик управления приложениями.

Примечание: сервис AppLocker включен в версии Windows корпоративного уровня. Вы можете создать правила AppLocker для одного компьютера или для группы компьютеров. Для одного компьютера можно создать правила с помощью редактора локальной политики безопасности (*secpol.msc*). Для группы компьютеров можно создать правила в объекте групповой политики с помощью консоли управления групповыми политиками (GPMC). Консоль GPMC доступна на клиентских компьютерах под

управлением Windows только после установки средств удаленного администрирования сервера.

В качестве примера рассмотрим алгоритм действий по блокировке с помощью AppLocker установки (запуска) приложений, которые ставятся в папку с профилем пользователя (такие как Yandex-браузер, Амиго, спутник Mail и т. п.) и не требуют прав администратора. Данные приложения содержат потенциальные каналы утечки информации и при определенных условиях могут нанести существенный вред информационной безопасности системы.

Механизм выполнения данной задачи состоит из следующих действий:

1. Водите в систему под учетной записью администратора.

2. Из сетевой папки, указанной преподавателем, скопируйте на диск D подписанный файл-установщик Yandex.

3. Откройте вкладку «Администрирование» Панели управления (*Пуск > Служебные – Windows > Панель управления > Все элементы панели управления > Администрирование*). Запустите сервис «Службы».

Откроется окно с перечнем служб ОС Windows (рис. 8).

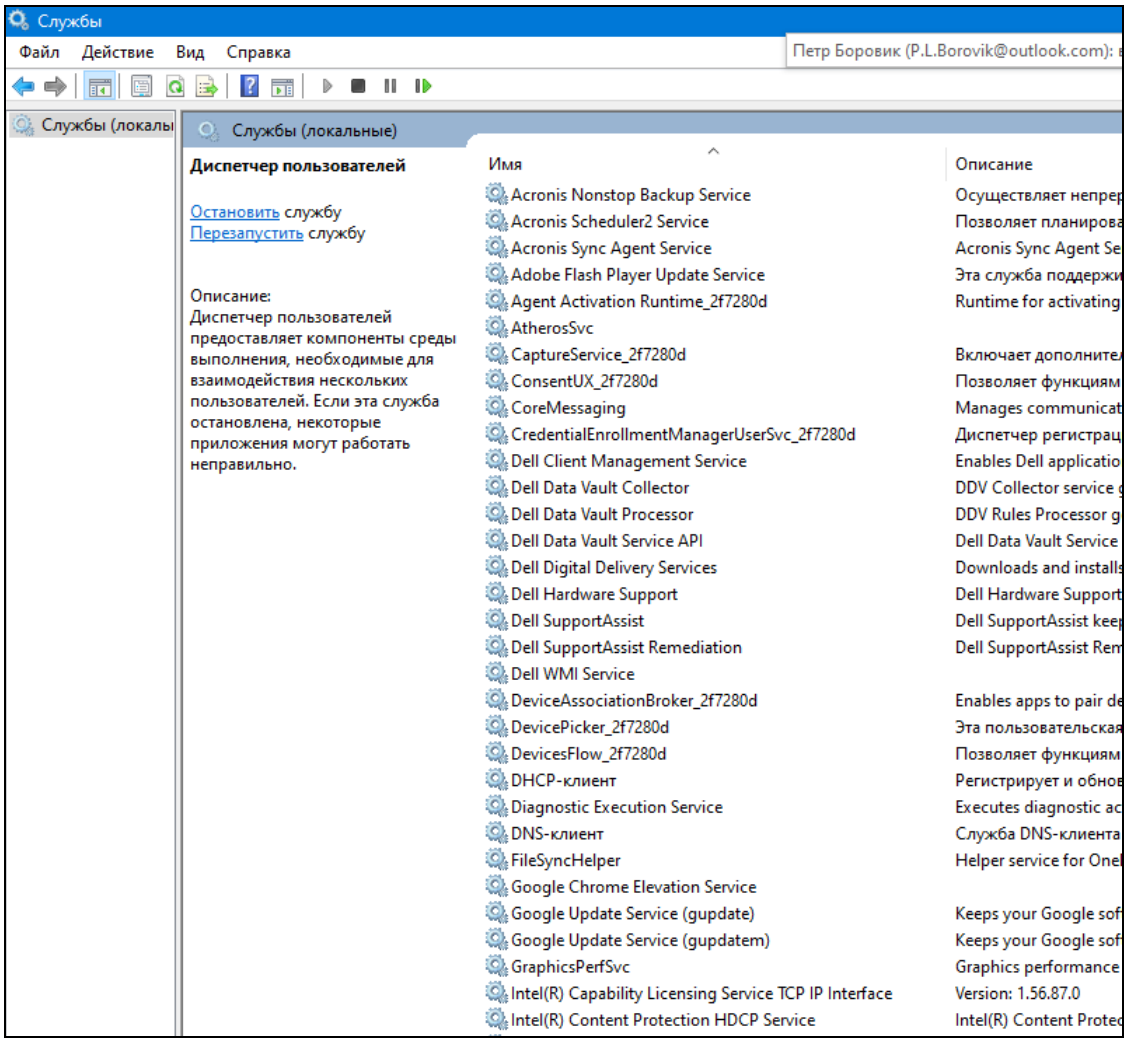


Рис. 8. Фрагмент окна с перечнем служб ОС Windows

4. Найдите службу «Удостоверение приложения» и откройте ее свойства. Установите тип запуска: *автоматически*. Нажмите на кнопку «Запустить», а затем «Ок» (рис. 9).

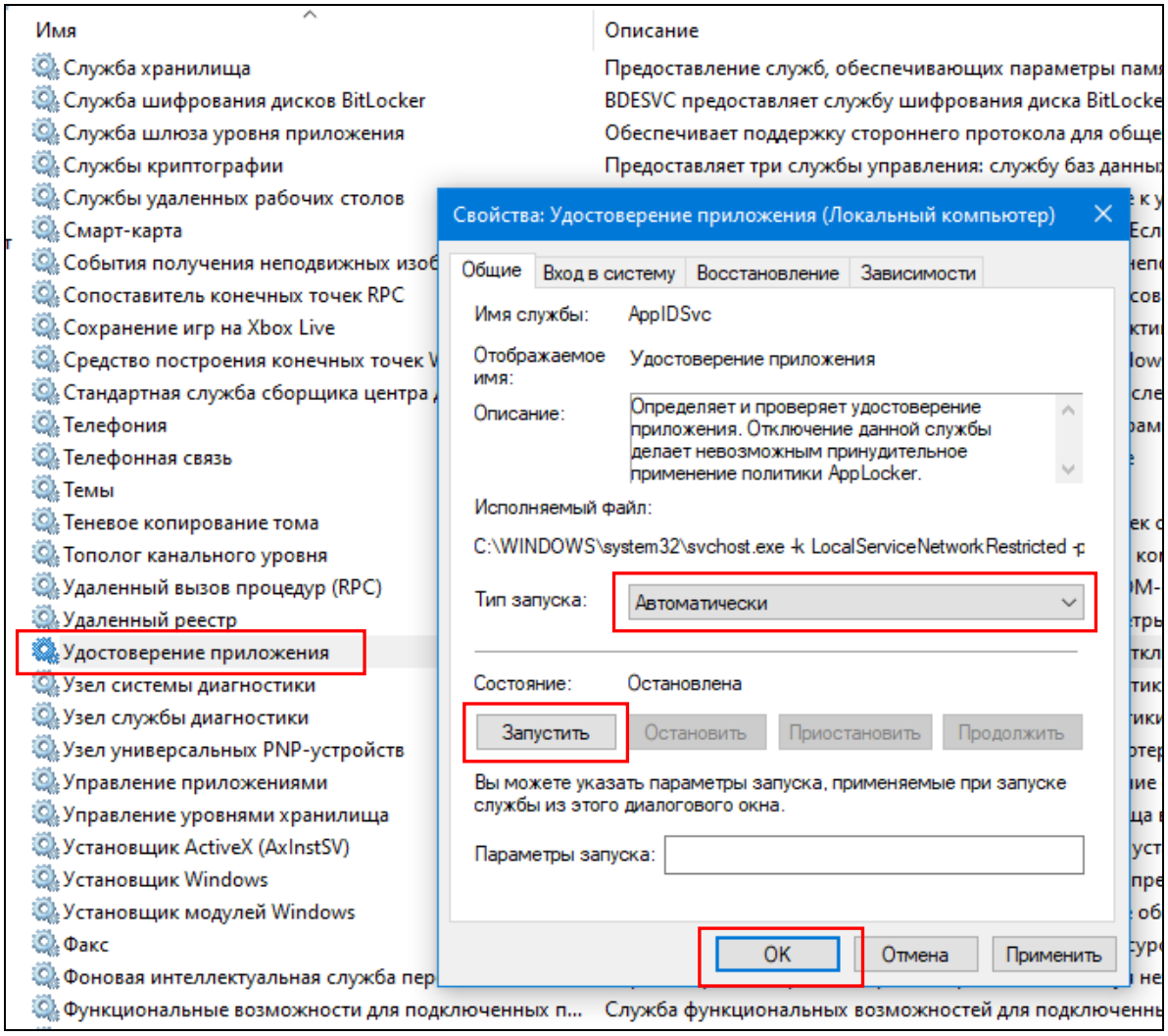


Рис. 9. Запуск службы «Удостоверение приложения»

5. В окне «Администрирование» откройте оснастку «Локальная политика безопасности». В открывшемся окне запустите настройку параметров «Исполняемые правила» (*Параметры безопасности* > *Политики управления приложениями* > *AppLocker* > *Исполняемые правила*).

Правой клавишей мыши нажмите на параметр «Исполняемые правила» и в контекстном меню выберите пункт «Создать новое правило» (рис. 10).

Откроется «Мастер создания новых правил». Нажмите «Далее» (рис. 11).

6. На шаге «Разрешения» выберите используемые действие: *разрешить* (рис. 12). Нажмите «Далее».

7. На шаге «Условия» выберите тип основного условия, которое следует создать: *Издатель* (рис. 13). Нажмите «Далее».

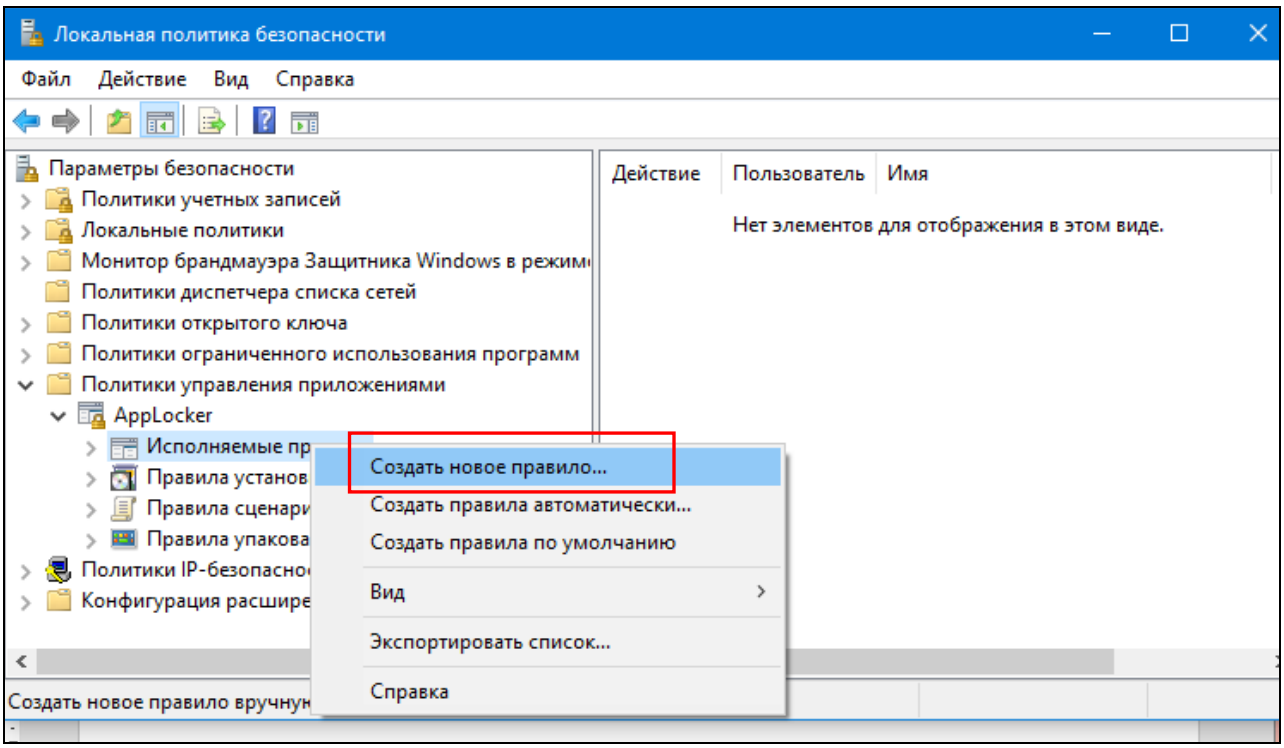


Рис. 10. Создание исполняемого правила с помощью сервиса AppLocker

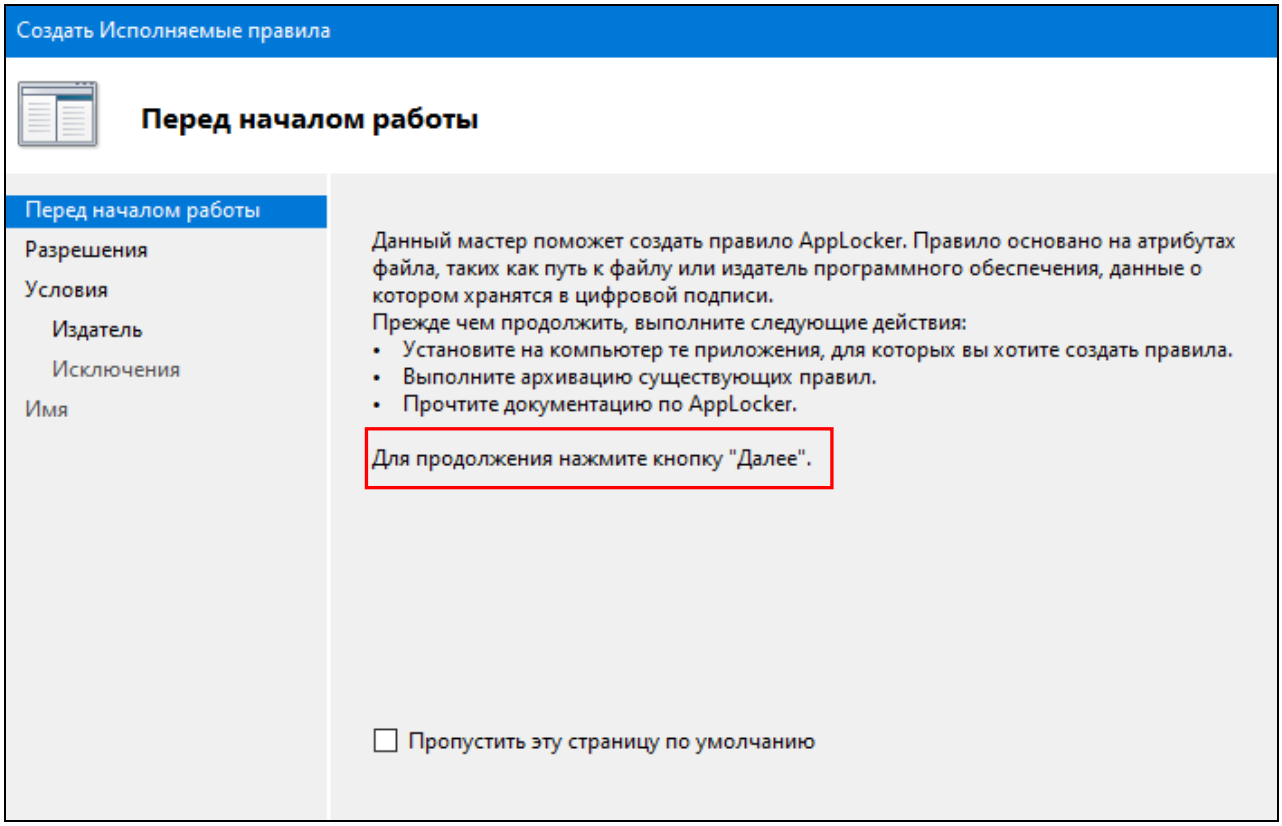


Рис. 11. Мастер создания исполняемого правила с помощью сервиса AppLocker (шаг 1)

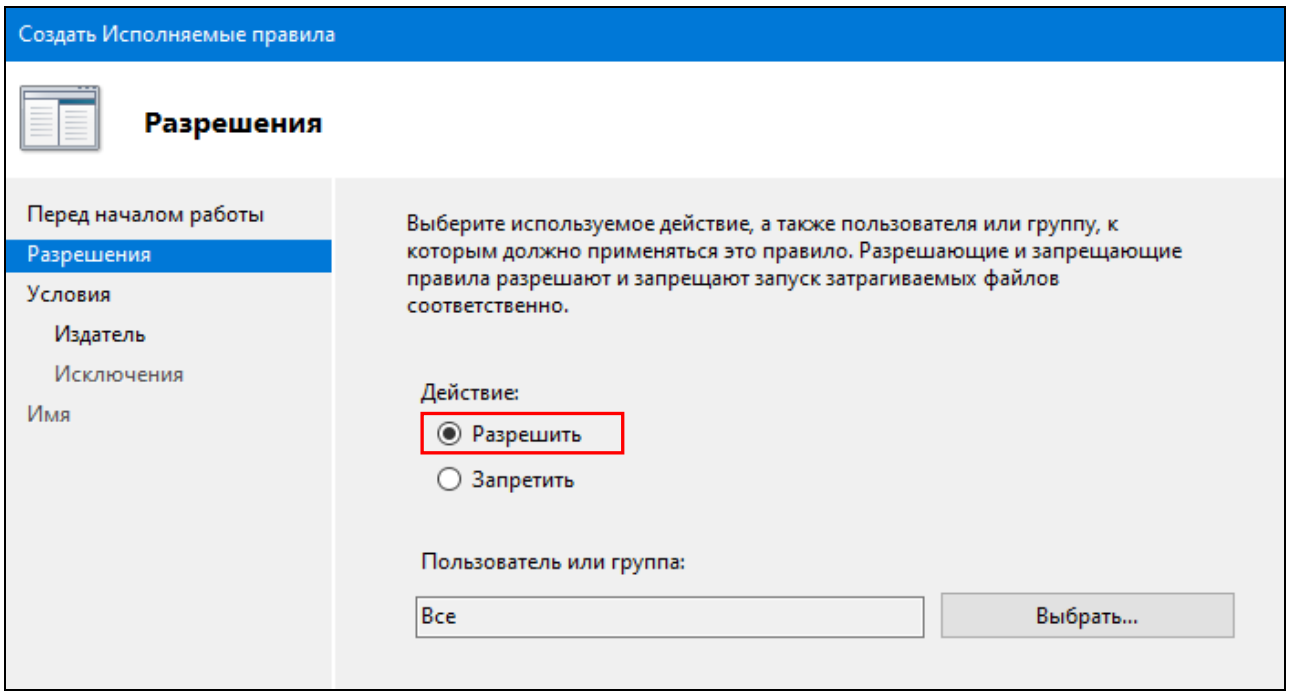


Рис. 12. Мастер создания исполняемого правила с помощью сервиса AppLocker (шаг 2)

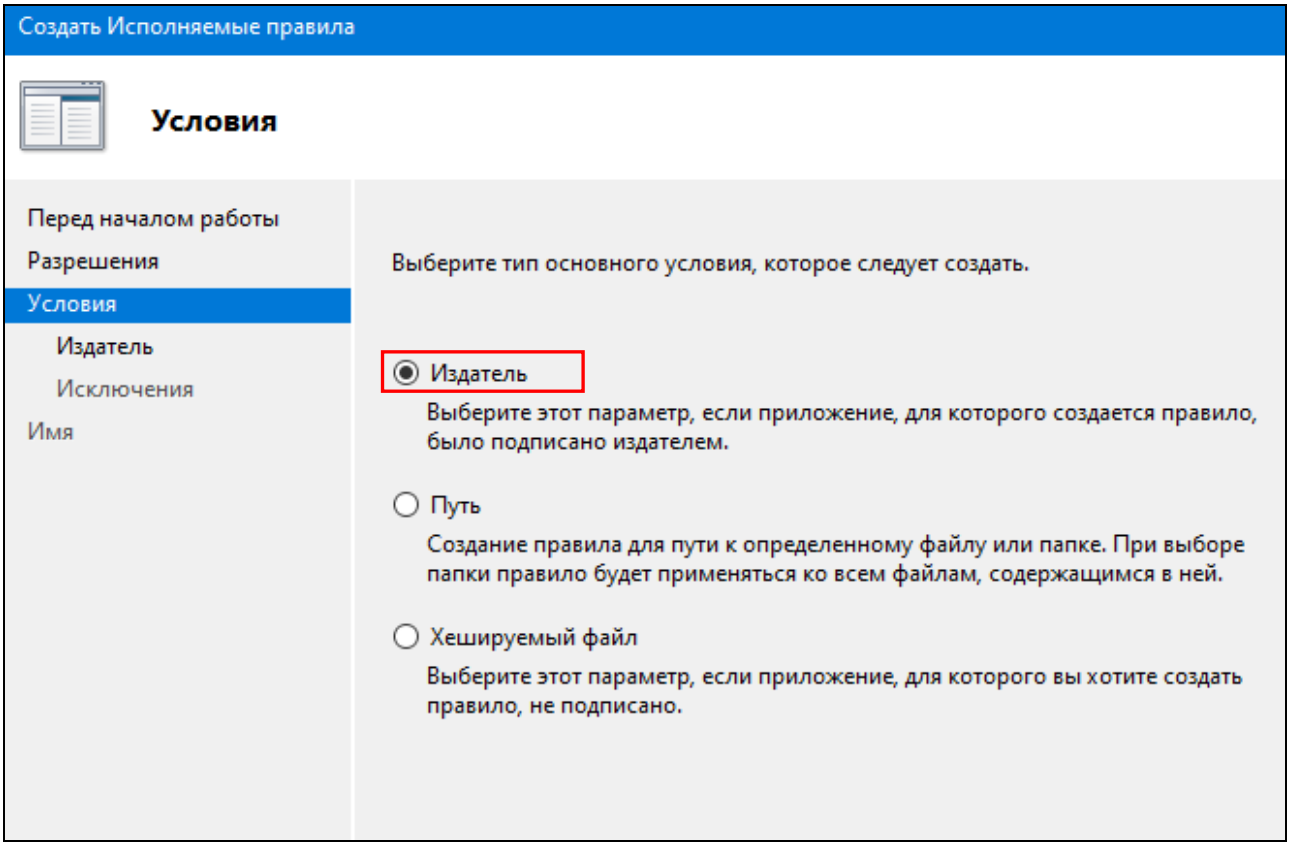


Рис. 13. Мастер создания исполняемого правила с помощью сервиса AppLocker (шаг 3)

Примечание: выбрав способ привязки к правилу «*Издатель*», вы указываете правило доступа для приложения на основе его издателя. Такой способ гарантирует, что даже после выхода обновлений для приложения, правило AppLocker продолжит действовать. Но данный способ не подойдет для тех приложений, которые не подписаны.

Используя способ «*Путь*», вы указываете путь к файлу, к которому нужно применить данное правило. Достоинством такого способа является простота создания. Кроме того, указав путь к папке, вы примените политику для папки, ее подпапок и файлов. Недостатком этого способа привязки является возможность обхода запрета правила AppLocker путем переименования или перемещения файлов и папок.

Привязка «*Правило хэша*» происходит через двоичное кодирование файла. Вне зависимости от того, где находится файл, на него все равно будет действовать политика AppLocker. Но стоит обновить файл или любым другим способом изменить его код, правило перестанет действовать, так как файл будет изменен.

8. На шаге «Издатель» найдите подписанный файл для использования в качестве образца для правила. С помощью ползунка выберите свойства, определяющее правило: *Версия файла* (рис. 14). Нажмите «Далее».

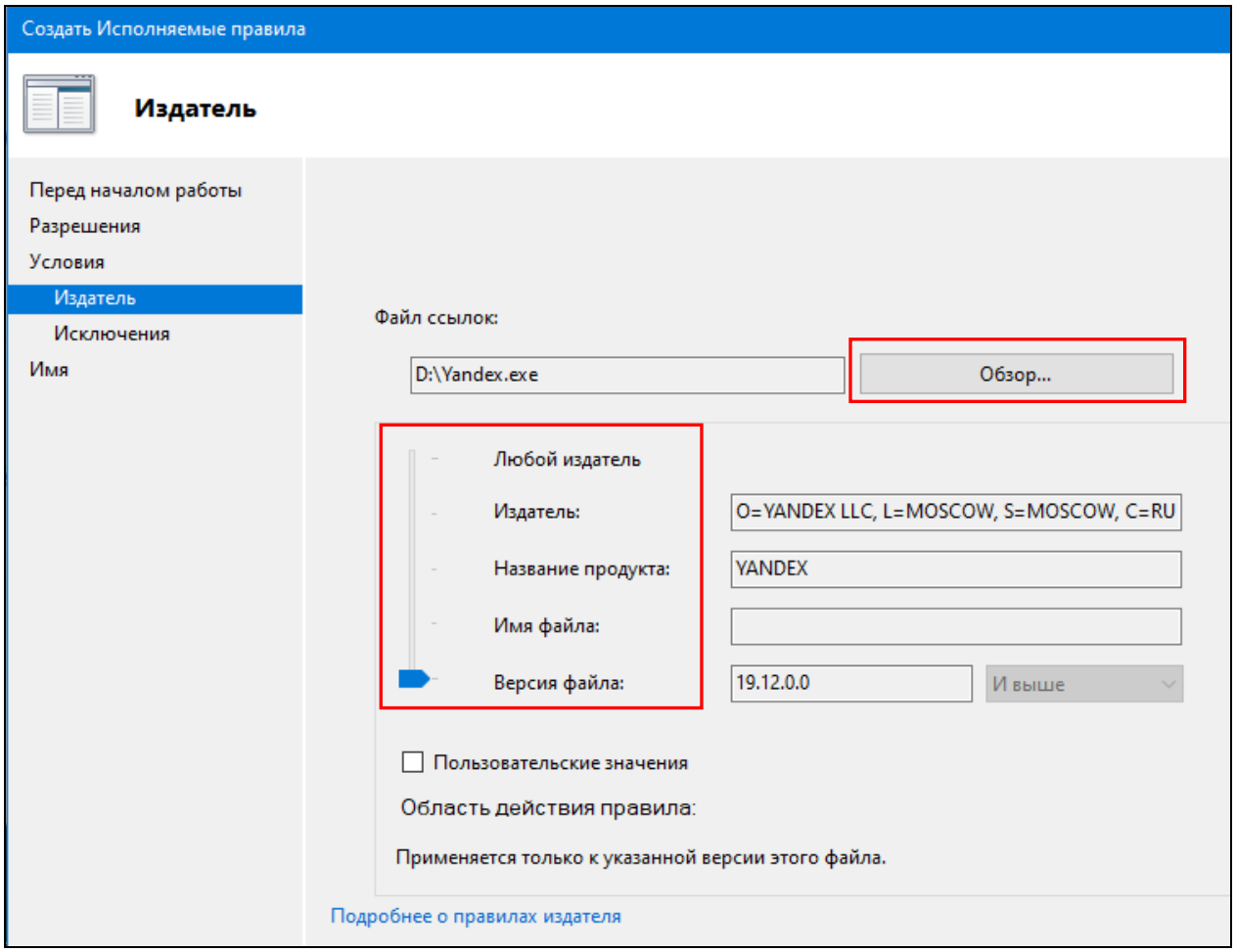


Рис. 14. Мастер создания исполняемого правила с помощью сервиса AppLocker (шаг 4)

9. На шаге «Исключения» можно задать исключения из правил. Например, запрещая установку любого ПО от производителя «Яндекс», можно разрешить установку программ «Яндекс.Диск» или «Яндекс.Карты». В этом случае соответствующие файлы-установщики следует добавить в исключения с помощью кнопки «Добавить» (рис. 15).

Для продолжения нажмите «Далее».

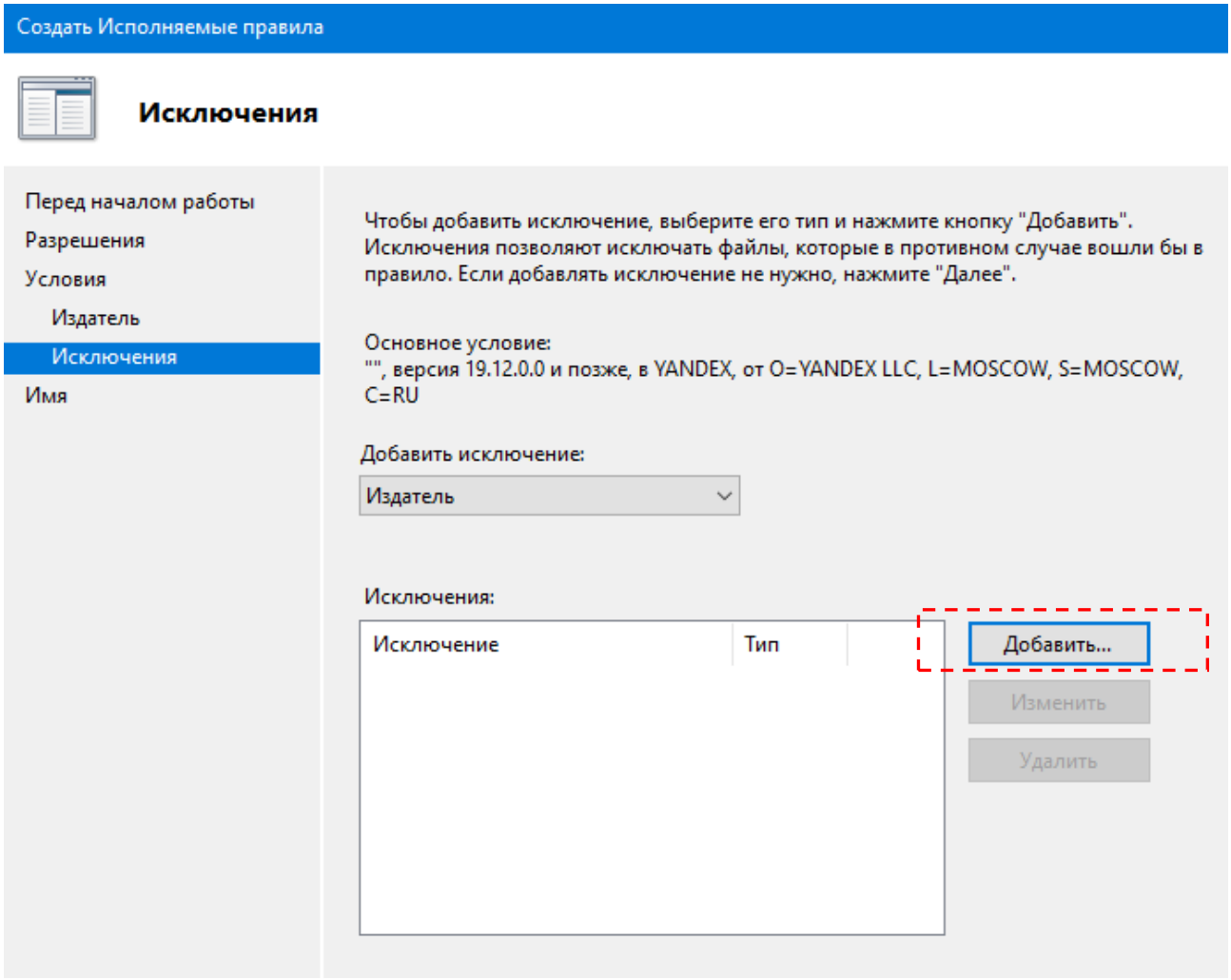


Рис. 15. Мастер создания исполняемого правила с помощью сервиса AppLocker (шаг 5)

10. На шаге «Имя» можно присвоить имя, определяющее созданное правило и ввести описание (необязательно) (рис. 16).

11. Для завершения работы Мастера создания Исполняемого правила AppLocker нажмите кнопку «Создать». Правило готово. Для того, чтобы оно немедленно вступило в силу правила политики для ПК и Пользователя необходимо обновить.

Для этого откройте командную строку (Win+R > *cmd*), в которой вводите и запустите следующую команду: *gpupdate /force* (рис. 17).

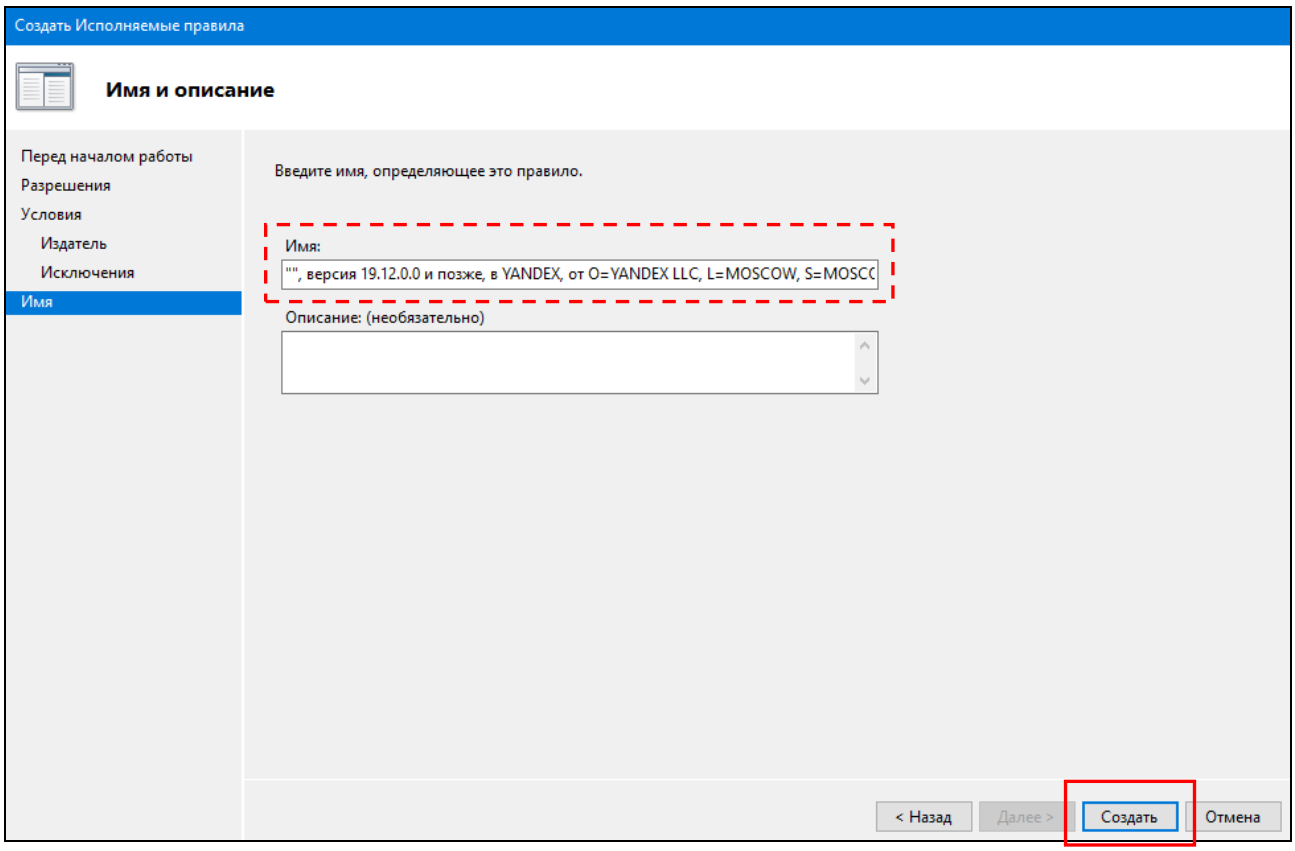


Рис. 16. Мастер создания исполняемого правила с помощью сервиса AppLocker (шаг 6)

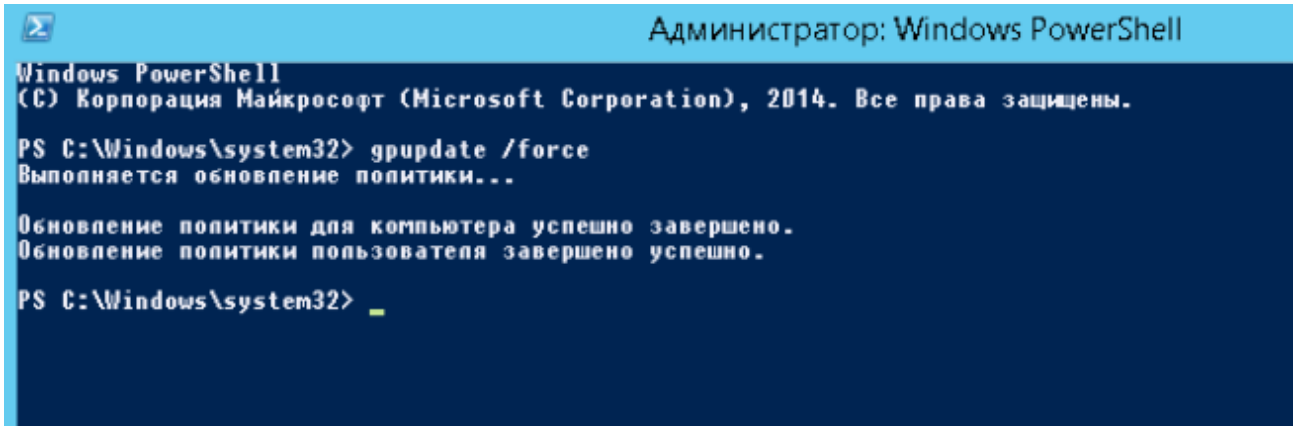


Рис. 17. Обновление правил политики AppLocker для ПК и Пользователя

12. В основном окне политики управления приложениями AppLocker вы можете управлять применением созданных (создаваемых) правил, а также увидите сводную информацию по их количеству (рис. 18).

Чтобы изменить режим применения политики AppLocker, откройте ссылку «Настроить применение правил». Для каждого типа правил можно выбрать один из двух режимов работы (рис. 19):

Принудительное применение правил – правила AppLocker принудительно применяются к пользователям. И любой файл, для которого нет подходящего правила, будет заблокирован для запуска;

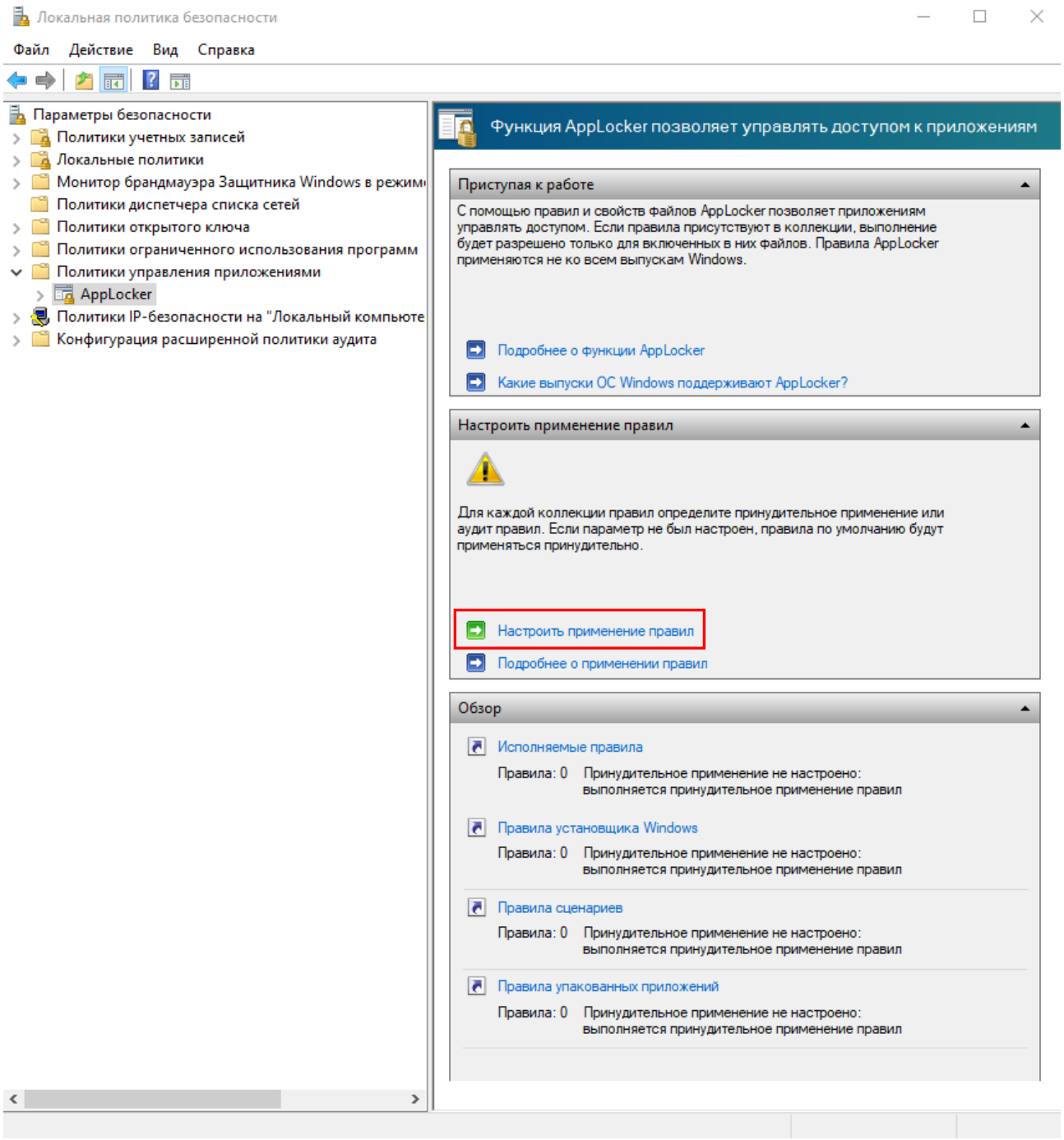


Рис. 18. Основное окно политики управления приложениями AppLocker

Только аудит – режим аудита. Он полезен для определения списка ПО, которое используется пользователями. Когда включен этот режим, политики AppLocker не ограничивают запуск приложений. Но если для запускаемого файла (сценария или приложения) задано правило в политике, в журнал событий AppLocker будет добавлена соответствующая запись. Этот журнал можно просмотреть через оснастку «Управление компьютером» (Win+R > *eventvwr.msc* > Служебные программы > Просмотр событий > Журналы приложений и служб > Microsoft > Windows > AppLocker) (рис. 20).

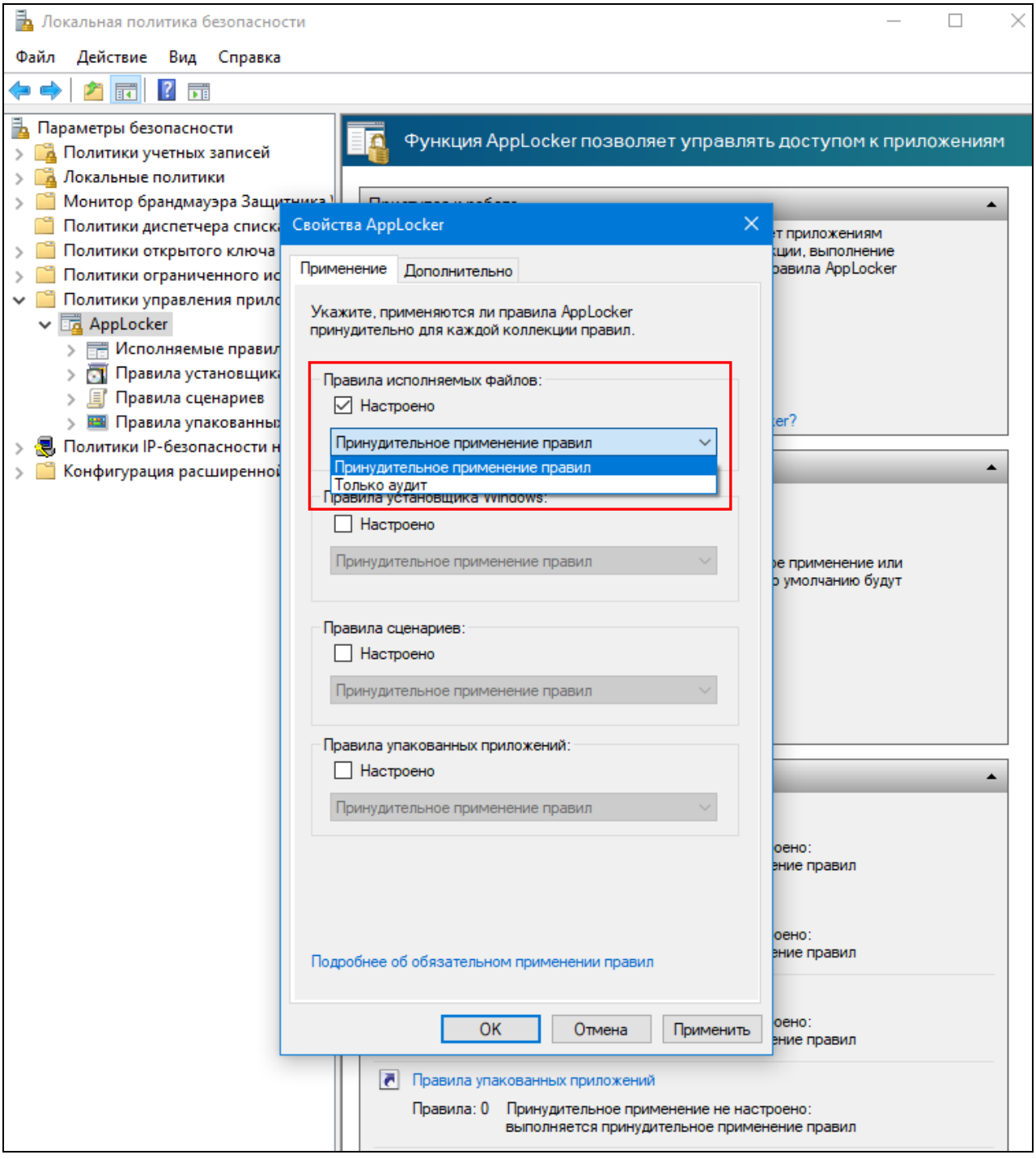


Рис. 19. Основное окно политики управления приложениями AppLocker

Анализируя журнал событий AppLocker, можно обнаружить несколько событий со следующими кодами:

Информационное событие 8001. Свидетельствует о том, что политика AppLocker была успешно применена на этом компьютере;

Информационное событие 8002. Это событие указывает на то, что в данном случае, выполнение определенного EXE- либо DLL-файла разрешены, согласно с распространяемым правилом AppLocker;

Событие-предупреждение 8003. Данное событие указывает на то, что выполнение определенного файла на данный момент разрешается, однако, в

случае применения политики AppLocker, его выполнение будет запрещено. Это означает, что как только будет распространяться данное запрещающее правило не в режиме аудита, пользователь более не сможет использовать такое приложение. В том случае, если бы не использовался режим аудита, мы бы сейчас видели событие уровня «ошибка» под номером 8004.

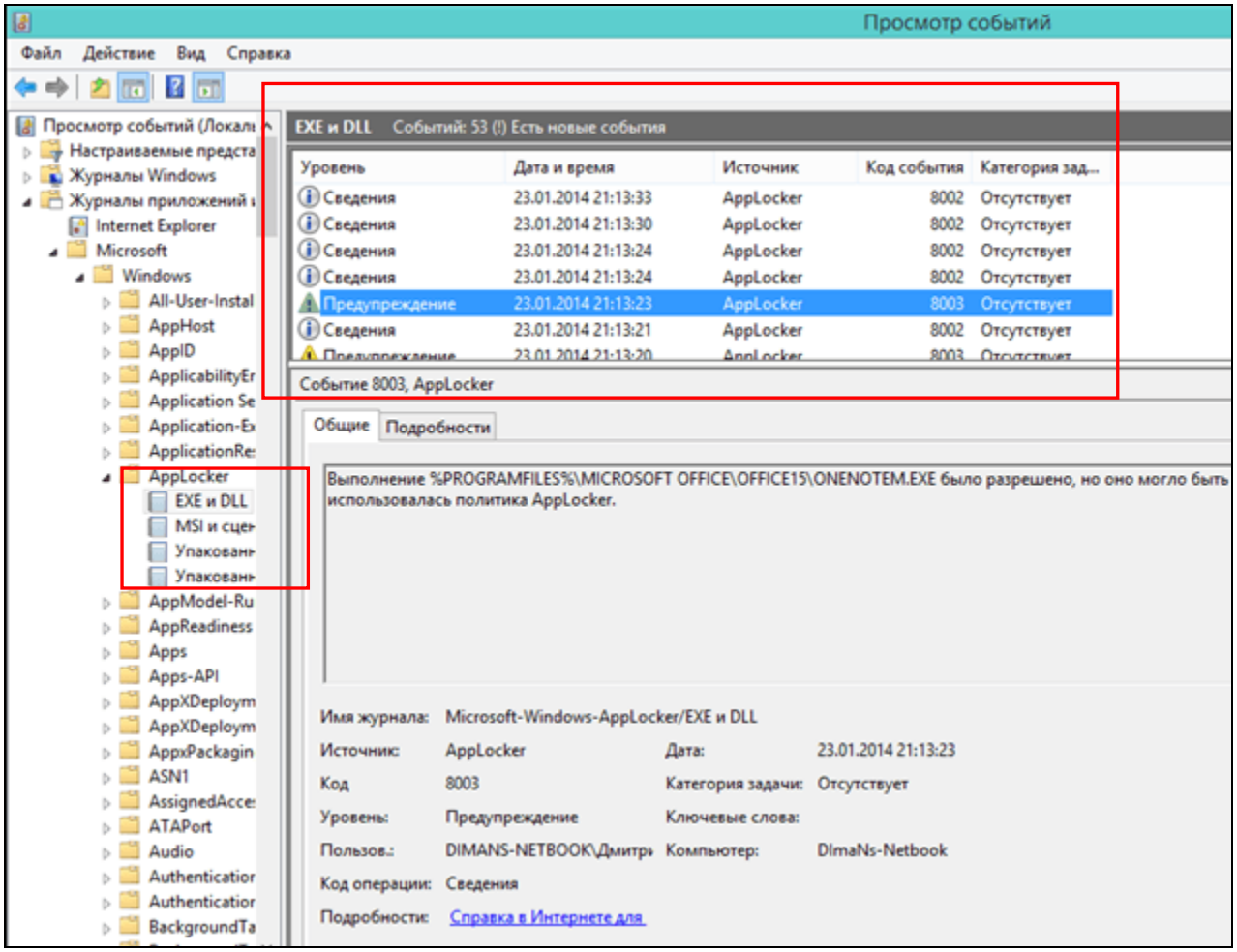


Рис. 20. Фрагмент основного окна политики управления приложениями AppLocker

Проверка целостности системных файлов с помощью интегрированного сервиса «File Signature Verification».

Одна из серьезных уязвимостей безопасности информационной системы связана с установленными системными файлами и драйверами Windows. Так, драйверы режима ядра в ОС могут использоваться не только для управления устройствами, но и как «окно» для доступа в более привилегированный режим. Это позволяет злоумышленнику при проникновении в сеть организации использовать уязвимости системных файлов и драйверов на ПК, осуществлять их изменение (модификацию), отключать антивирусные программные продукты, устанавливать собственное вредоносное программное обеспечение и выполнять несанкционированный доступ в систему.

Своеобразным паспортом, гарантирующим целостность и подлинность (т.е. безопасность) установленного системного файла либо драйвера, является

цифровая подпись. Она содержит в себе информацию не только о производителе данного файла и об аппаратном обеспечении, для которого оно изготовлено, но и сведения о внесенных легальных изменениях. Цифровая подпись подтверждается центром сертификации. Все это дает уверенность в том, что данный файл выпущен указанным производителем и что все изменения были сделаны им.

Наиболее полную информацию о цифровых подписях системных файлов и драйверов можно получить с помощью интегрированного в ОС Windows средства «File Signature Verification». Сервис позволяет осуществлять сканирование системы и выявлять системные файлы и драйвера , не содержащие цифровой подписи.

Механизм работы с ним можно представить в виде следующей последовательности действий:

1. Запустите сервис «File Signature Verification» (Win+R > *sigverif*).
2. Откроется окно сервиса (рис. 21). Для осуществления анализа системных файлов нажмите кнопку «Начать».

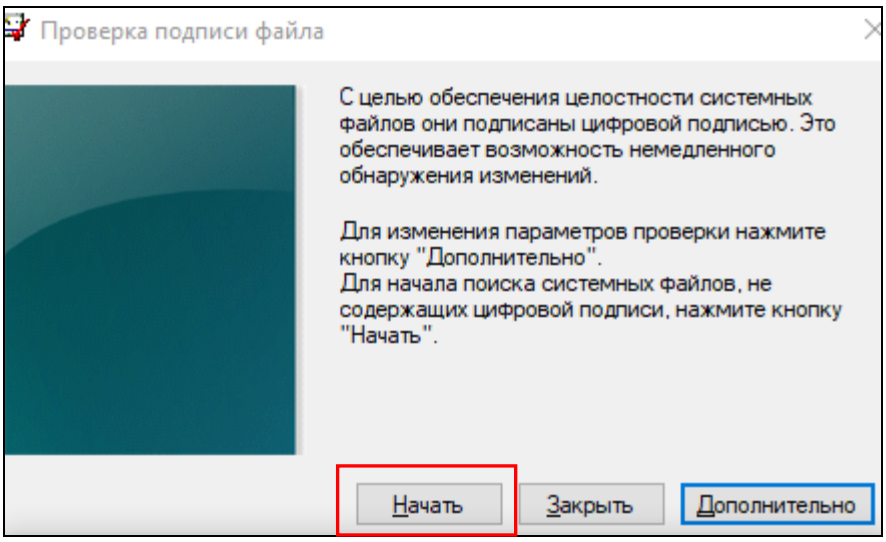


Рис. 21. Сервис «File Signature Verification»

3. После проведения анализа откроется окно «Результаты проверки подписи», в котором отобразится список не подписанных системных файлов и драйверов (рис. 22).
4. Для просмотра более подробной информации о результатах проверки следует закрыть окно «Результаты проверки подписи», и в начальном окне сервиса «File Signature Verification» нажать на кнопку «Дополнительно».
5. В открывшем диалоговом окне «Дополнительные параметры проверки подписи файлов) нажмите на кнопку «Просмотр журнала» (рис. 23)

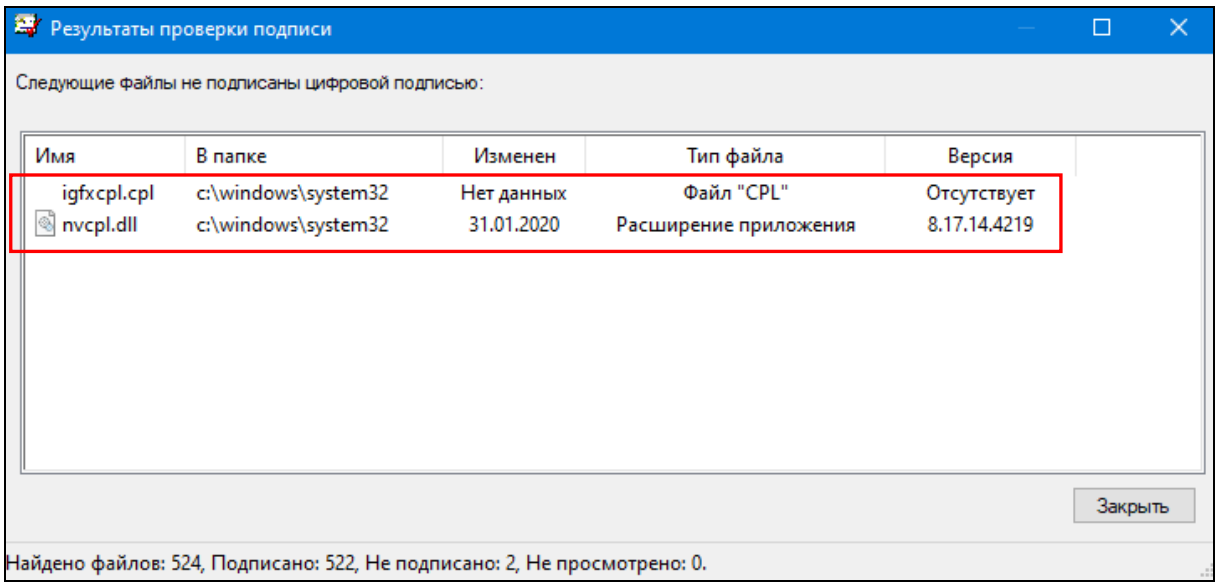


Рис. 22. Результаты проверки файлов на наличие цифровой подписи с помощью сервиса «File Signature Verification»

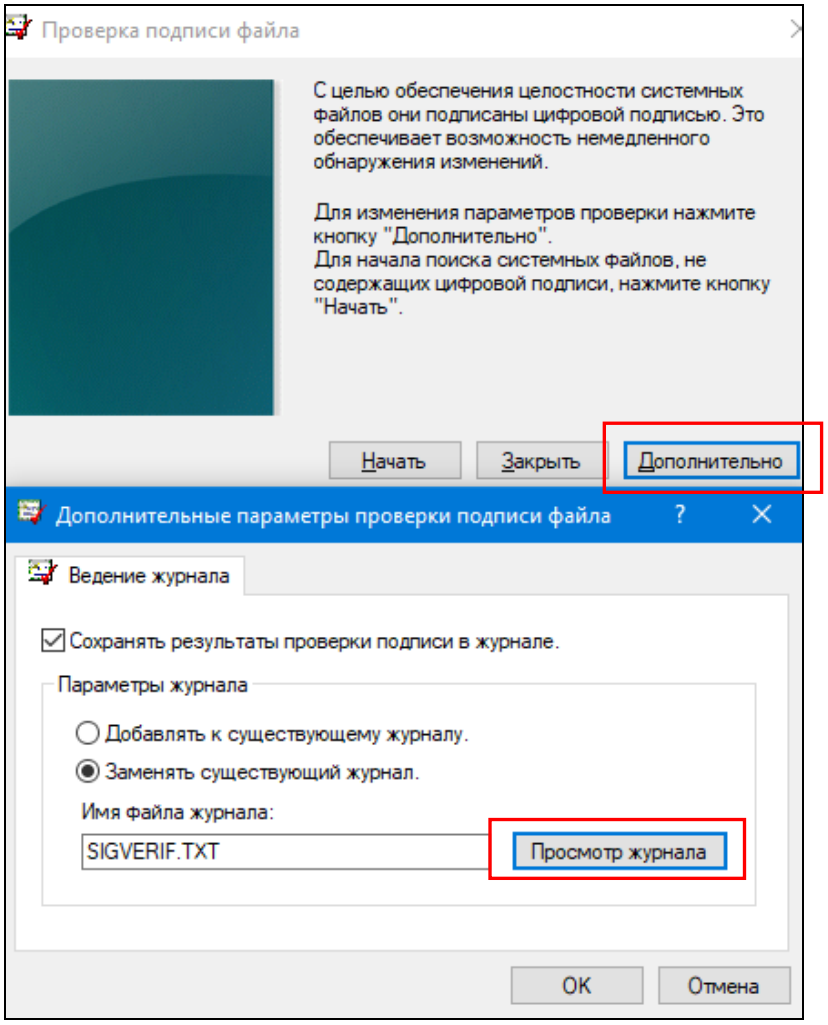
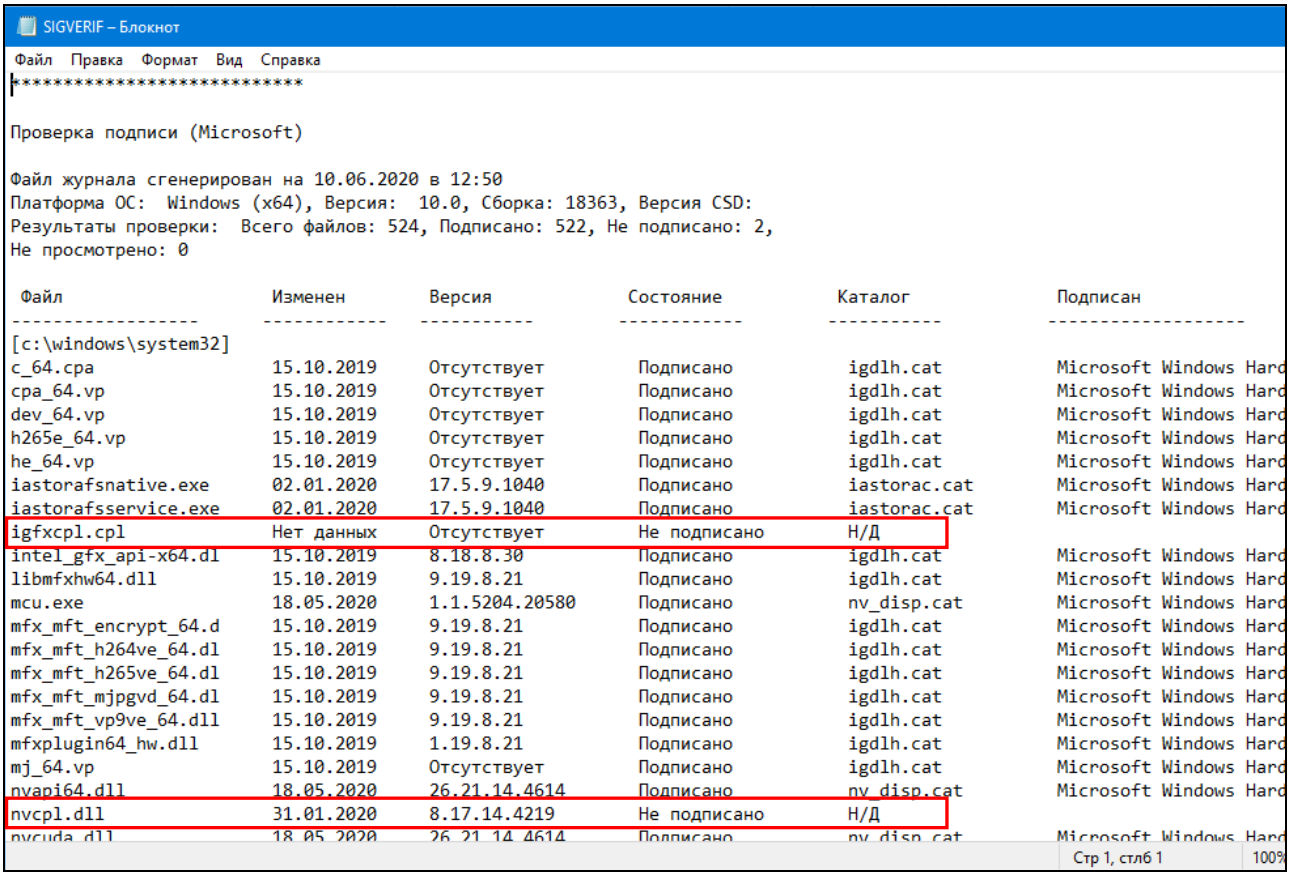


Рис. 23. Открытие журнала проверки файлов на наличие цифровой подписи с помощью сервиса «File Signature Verification»


SIGVERIF – Блокнот

Файл Правка Формат Вид Справка

****

Проверка подписи (Microsoft)

Файл журнала сгенерирован на 10.06.2020 в 12:50
Платформа ОС: Windows (x64), Версия: 10.0, Сборка: 18363, Версия CSD:
Результаты проверки: Всего файлов: 524, Подписано: 522, Не подписано: 2,
Не просмотрено: 0

Файл	Изменен	Версия	Состояние	Каталог	Подписан
[c:\windows\system32]					
c_64.cpa	15.10.2019	Отсутствует	Подписано	igdlh.cat	Microsoft Windows Hard
cpa_64.vp	15.10.2019	Отсутствует	Подписано	igdlh.cat	Microsoft Windows Hard
dev_64.vp	15.10.2019	Отсутствует	Подписано	igdlh.cat	Microsoft Windows Hard
h265e_64.vp	15.10.2019	Отсутствует	Подписано	igdlh.cat	Microsoft Windows Hard
he_64.vp	15.10.2019	Отсутствует	Подписано	igdlh.cat	Microsoft Windows Hard
iastorafsnative.exe	02.01.2020	17.5.9.1040	Подписано	iastorac.cat	Microsoft Windows Hard
iastorafsservice.exe	02.01.2020	17.5.9.1040	Подписано	iastorac.cat	Microsoft Windows Hard
igfxcpl.cpl	Нет данных	Отсутствует	Не подписано	Н/Д	
intel_gfx_api-x64.dl	15.10.2019	8.18.8.30	Подписано	igdlh.cat	Microsoft Windows Hard
libmfxhw64.dll	15.10.2019	9.19.8.21	Подписано	igdlh.cat	Microsoft Windows Hard
mcu.exe	18.05.2020	1.1.5204.20580	Подписано	nv_disp.cat	Microsoft Windows Hard
mfx_mft_encrypt_64.d	15.10.2019	9.19.8.21	Подписано	igdlh.cat	Microsoft Windows Hard
mfx_mft_h264ve_64.dl	15.10.2019	9.19.8.21	Подписано	igdlh.cat	Microsoft Windows Hard
mfx_mft_h265ve_64.dl	15.10.2019	9.19.8.21	Подписано	igdlh.cat	Microsoft Windows Hard
mfx_mft_mjpgvd_64.dl	15.10.2019	9.19.8.21	Подписано	igdlh.cat	Microsoft Windows Hard
mfx_mft_vp9ve_64.dll	15.10.2019	9.19.8.21	Подписано	igdlh.cat	Microsoft Windows Hard
mfxplugin64_hw.dll	15.10.2019	1.19.8.21	Подписано	igdlh.cat	Microsoft Windows Hard
mj_64.vp	15.10.2019	Отсутствует	Подписано	igdlh.cat	Microsoft Windows Hard
nvapi64.dll	18.05.2020	26.21.14.4614	Подписано	nv_disp.cat	Microsoft Windows Hard
nvcpl.dll	31.01.2020	8.17.14.4219	Не подписано	Н/Д	
nvcuda.dll	18.05.2020	26.21.14.4614	Подписано	nv_disp.cat	Microsoft Windows Hard

Стр 1, стлб 1 100%

Рис. 24. Журнал проверки файлов на наличие цифровой подписи с помощью сервиса «File Signature Verification»

Анализируя данный журнал, можно выявить системные файлы или драйвера, являющиеся потенциально вредоносными либо обладающими потенциальной уязвимостью.

4. Регистрация и оперативное оповещение о событиях безопасности

Краткие теоретические сведения:

Регистрация и оперативное оповещение о событиях безопасности информационной системы предназначены для достижения следующих целей:

анализа фактов, свидетельствующих о нарушении политики безопасности компьютерной системы, для выявления его истинных причин и подтверждения вины конкретных пользователей или администраторов;

выявления действий, направленных на подготовку компьютерного правонарушения для его предотвращения;

немедленного реагирования на попытки компьютерного правонарушения для их максимально быстрого предупреждения.

К основным требованиям политики аудита в компьютерной системе относятся:

ассоциирование пользователя с любым событием аудита, что обеспечивает индивидуальную ответственность пользователей за их действия в компьютерной системе;

обязательность аудита стандартного набора событий – идентификации и аутентификации пользователя, создания и завершения процессов доступа к объектам компьютерной системы, действий администратора компьютерной системы (изменений в базе данных учетных записей и политике безопасности);

наличие необходимого набора атрибутов записи журнала аудита – даты и времени события, логического имени инициировавшего событие пользователя, типа события, признака успешного или неудачного завершения вызвавшего событие действия, имени связанного с событием объекта;

возможность фильтрации записей журнала аудита.

При определении политики аудита следует понимать, что адекватной угрозам безопасности компьютерной системы будет не политика, предполагающая регистрацию многих событий, а политика, при которой будут регистрироваться необходимые события. К таким событиям можно отнести следующие:

вход пользователей в компьютерную систему и выход из нее;

доступ к объектам с конфиденциальной информацией со стороны пользователей, в отношении которых имеются обоснованные подозрения о попытках несанкционированного доступа;

изменения в списке зарегистрированных пользователей и политике безопасности компьютерной системы;

запуск и завершение системных и прикладных программ при наличии обоснованных подозрений о внедрении в них вредоносного кода.

При этом некоторые события записываются автоматически, а регистрацию других (в основном, касающихся безопасности системы) необходимо активировать и настраивать.

ОС Windows ведет аудит событий по 9 категориям:

1. Аудит событий входа в систему.
2. Аудит управления учетными записями.
3. Аудит доступа к службе каталогов.
4. Аудит входа в систему.
5. Аудит доступа к объектам.
6. Аудит изменения политики.
7. Аудит использования привилегий.
8. Аудит отслеживания процессов.
9. Аудит системных событий.

Рассмотрим более подробно, какие события отслеживает каждая из категорий.

Аудит событий входа в систему

Аудит попыток пользователя войти в систему с другого компьютера или выйти из нее, при условии, что этот компьютер используется для проверки подлинности учетной записи.

Аудит управления учетными записями

Аудит событий, связанных с управлением учетными записями на компьютере: создание, изменение или удаление учетной записи пользователя или группы; переименование, отключение или включение учетной записи пользователя; задание или изменение пароля.

Аудит доступа к службе каталогов

Аудит событий доступа пользователя к объекту каталога Active Directory, для которого задана собственная системная таблица управления доступом.

Аудит входа в систему

Аудит попыток пользователя войти в систему с компьютера или выйти из нее.

Аудит доступа к объектам

Аудит событий доступа пользователя к объекту – например, к файлу, папке, разделу реестра, принтеру и т. п., – для которого задана собственная системная таблица управления доступом.

Аудит изменения политики

Аудит фактов изменения политик назначения прав пользователей, политик аудита или политик доверительных отношений.

Аудит использования привилегий

Аудит попыток пользователя воспользоваться предоставленным ему правом.

Аудит отслеживания процессов

Аудиту таких событий, как активизация программы, завершение процесса, повторение дескрипторов и косвенный доступ к объекту.

Аудит системных событий

Аудит событий перезагрузки или отключения компьютера, а также событий, влияющих на системную безопасность или на журнал безопасности.

Решения об аудите конкретного типа событий безопасности принимаются в соответствии с политикой аудита локальной системы, называемой локальной политикой безопасности.

В качестве примера рассмотрим настройку протоколирования и аудита наиболее важных событий безопасности ОС локального компьютера. Алгоритм реализации данной задачи состоит из следующих действий:

1. Запустите консоль политик безопасности. Для этого воспользуйтесь комбинацией клавиш +R для открытия диалога «Выполнить». В диалоговом окне «Выполнить», в поле «Открыть» введите команду *secpol.msc* и нажмите на кнопку «Ок».

2. В открывшемся дереве консоли найдите и выберите пункт «Локальные политики». Откройте подпункт «Политика аудита». По умолчанию на обычном компьютере политики аудита отключены (рис. 13).

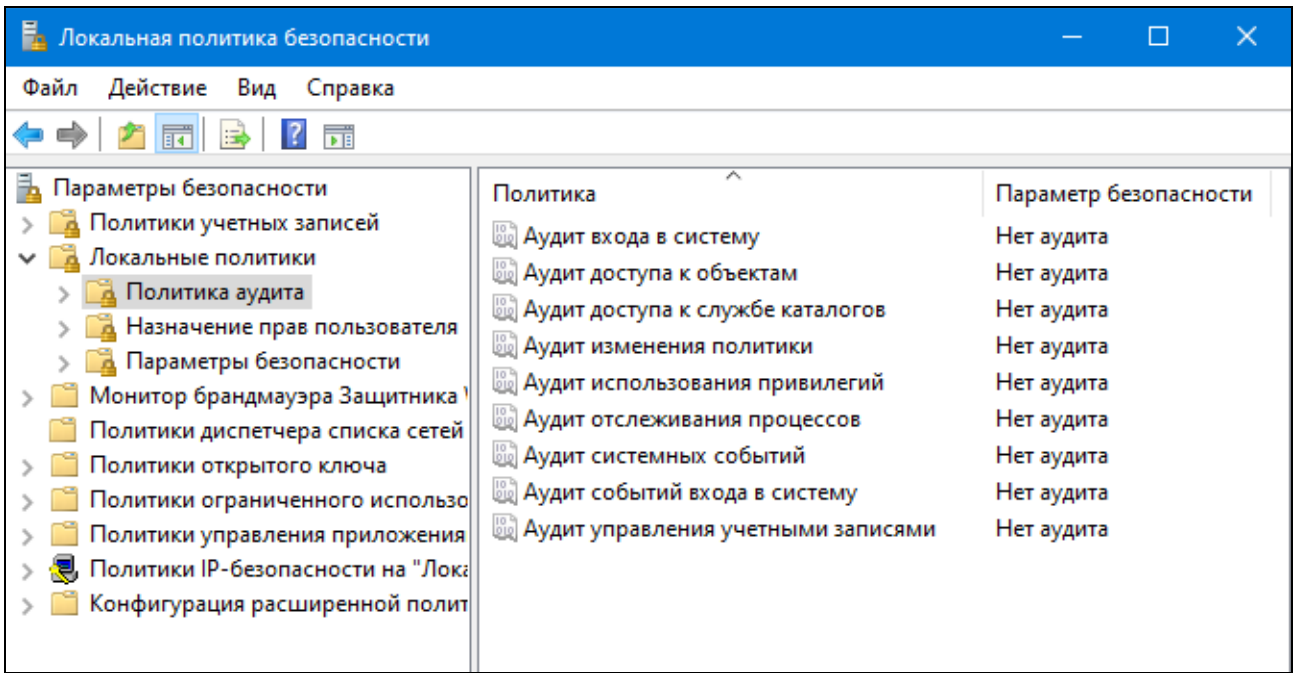


Рис. 13. Настройка политики аудита системы (часть 1)

Для включения или отключения параметров аудита выберите требуемый параметр и дважды щелкните левой клавишей мыши (рис. 14).

Для каждого параметра задайте аудит успехов или отказов, либо вообще отключите аудит событий данного типа (рис. 15).

Общий механизм протоколирования наиболее важных событий безопасности ОС активизирован.

В качестве частного случая реализации механизма протоколирования и аудита событий безопасности ОС рассмотрим особенности регистрации доступа к объектам файловой системы. Например, необходимо установить контроль доступа, в том числе удаления файлов и папок из папки «D:\Документы (общее)» (*см. п. 2 предыдущего задания для самостоятельной работы*) пользователями локального ПК.

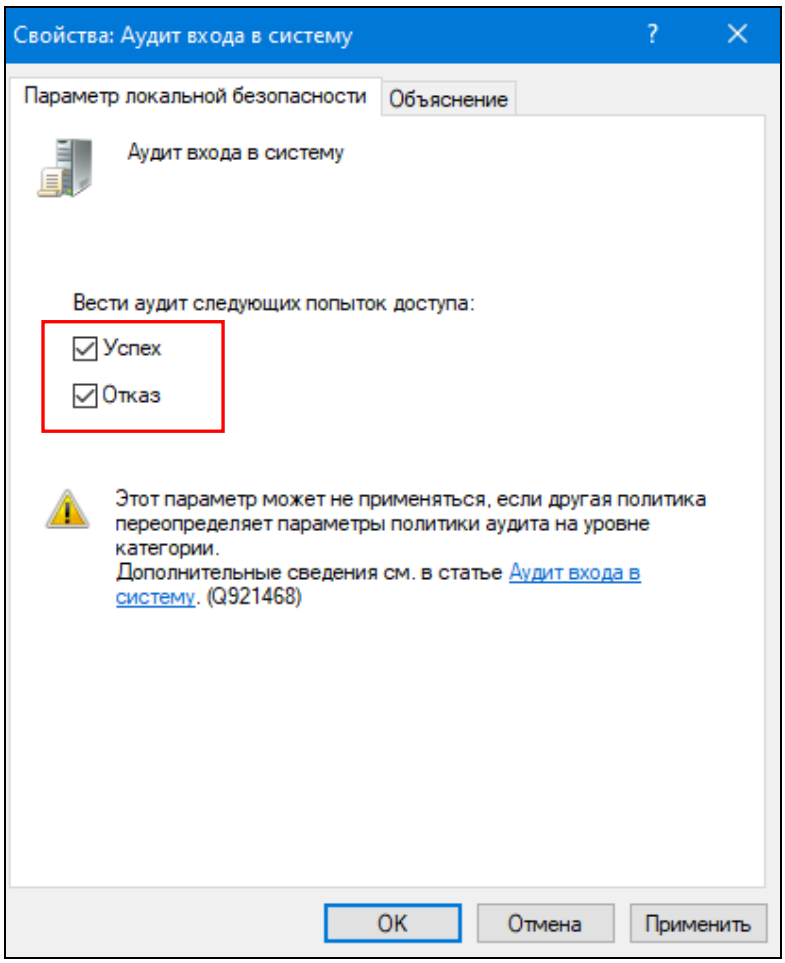


Рис. 14. Настройка политики аудита системы (часть 2)

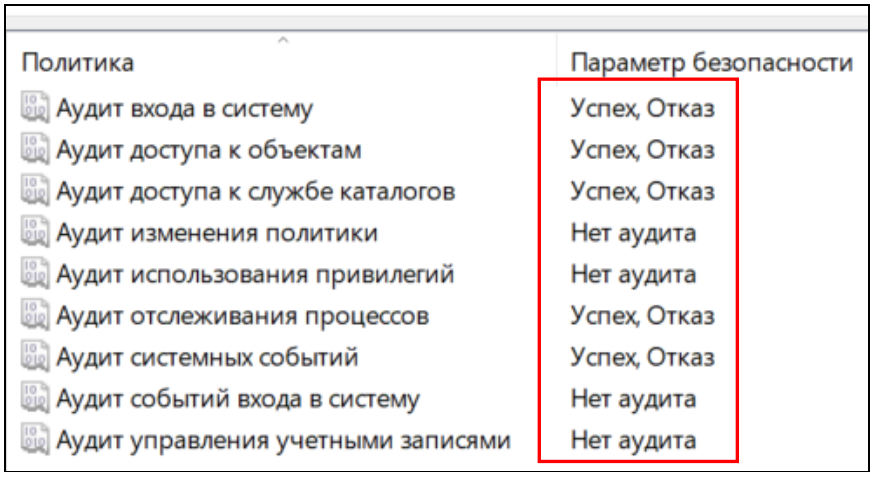


Рис. 15. Настройка политики аудита системы (часть 3)

Для решения поставленной задачи следует задать собственную системную таблица управления доступом, создав список пользователей, для которых будут отслеживаться попытки доступа к искомой папке и установив, какие именно попытки будут регистрироваться в журнале событий (например, попытки удаления папок и файлов, успешные и неуспешные).

Алгоритм реализации этой задачи потребует выполнения следующих действий:

1. Создайте в системе учебную пользовательскую учетную запись **Гость1** (тип учетной записи – *стандартная*).

2. Нажмите правой кнопкой мыши на папку «D:\Документы (общее)». В контекстном меню выберите пункт «Свойства».

3. В открывшемся диалоговом окне «Свойства: Документы (общее)» откройте вкладку «Безопасность». Нажмите кнопку «Дополнительно».

4. В открывшемся диалоговом окне «Дополнительные параметры безопасности для “Документы (общее)”» активизируйте вкладку «Аудит». Нажмите кнопку «Продолжить», а затем – кнопку «Добавить».

5. В открывшемся диалоговом окне «Элементы аудита для “Документы (общее)”» укажите тип аудита – *все*, а затем нажмите на ссылку «Выберите субъект».

6. В поле «Введите имена выбираемых объектов» открывшегося диалогового окна «Выбор: Пользователи” или “Группы”» введите наименование учетной записи **Гость1** и нажмите на кнопку «Проверить имена». Для завершения выбора нажмите «Ок».

7. В нижней части диалогового окна «Элементы аудита для “Документы (общее)”» нажмите на ссылку «Отображение дополнительный разрешений». Установите дополнительные разрешения аудита: *удаление подпапок и файлов*; *удаление* (рис. 16). Для завершения и закрытия диалоговых окон нажмите «Ок».

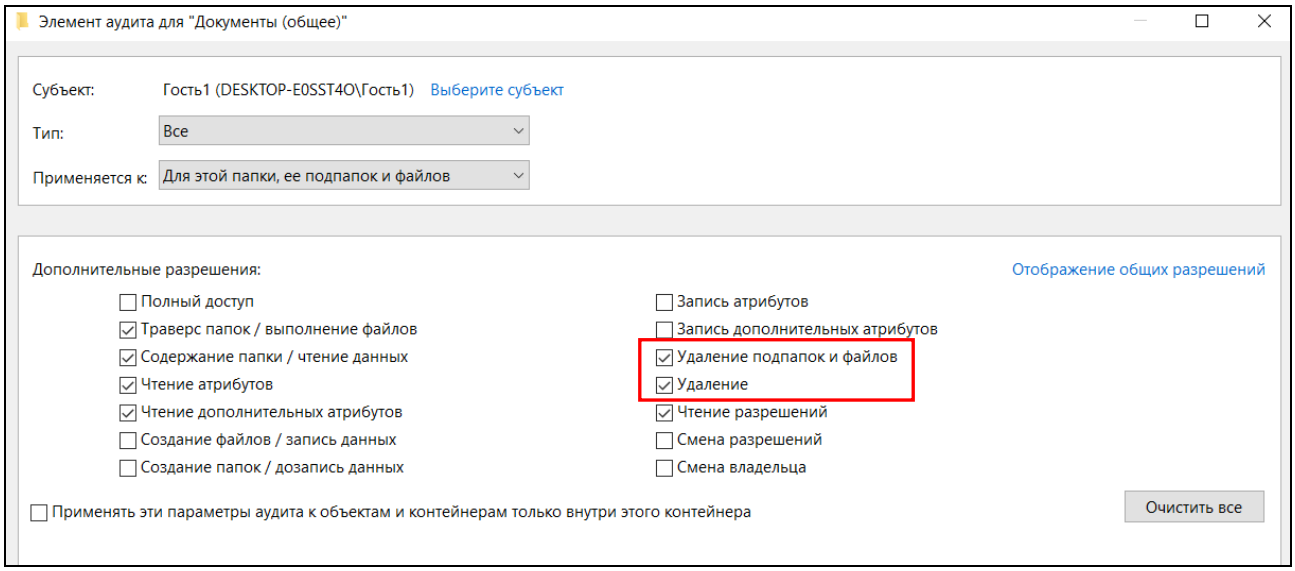


Рис. 16. Настройка дополнительных параметров аудита системы

Механизм контроля доступа, в том числе удаления файлов и папок из папки «D:\Документы (общее)» пользователем **Гость1** активизирован.

Теперь для проверки работы установленного механизма аудита следует зайти в ОС под учетной записью пользователя **Гость1** и удалить из указанной папки какой-нибудь файл, например «МК1.docx». Указанное действие будет зафиксировано в журнале безопасности ОС.

Для просмотра и управления журналами событий необходимо запустить в Windows стандартную программу «Просмотр событий» (Win+R → eventvwr.msc → Enter).

Откроется окно журнала событий (рис. 17).

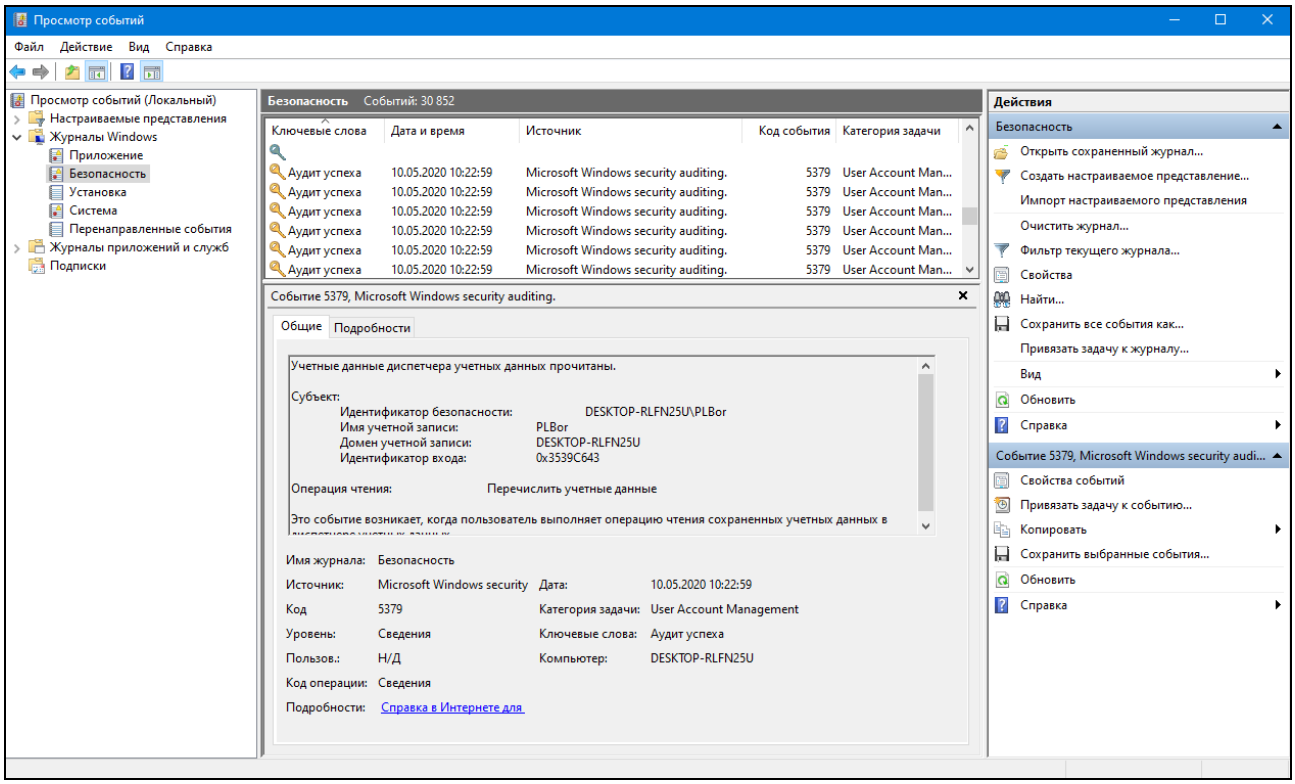


Рис. 17. Журнал событий ОС Windows 10.

Интерфейс данного инструмента администрирования можно условно разделить на три части.

В левой панели находится древовидная структура, в которой отсортированы журналы события по различным параметрам. При выборе того или иного журнала в центральном окне появляется список всех доступных в данном журнале событий вместе с информацией о дате и времени, когда произошло каждое событие, его источнике, типе и другими подобными сведениями.

Для нас наибольший интерес представляет раздел «Журналы Windows» – именно с ним чаще всего приходится работать, анализируя зарегистрированные события аудита. Данный раздел включает три основные и две дополнительные категории: основные – это «*Приложение*», «*Система*», «*Безопасность*»; дополнительные – «*Установка*» и «*Перенаправленные события*».

Названия данных журналов отображают события, которые в них фиксируются (системные события, события приложений и т.д.). Кроме этого, сюда же можно добавить собственные «*Настраиваемые представления*», в которых будут отображаться лишь нужные вам события.

В журнале «*Приложение*» содержатся данные, относящиеся к работе приложений и программ. Эти данные помогут системному администратору установить причину отказа той или иной программы.

В журнале «*Система*» содержатся события системных компонентов Windows (например, сбои при загрузке драйвера или других системных компонентов при запуске системы, неудачи при запусках служб или инициализации драйверов, общесистемные сообщения и прочие сообщения, относящиеся к системе в целом).

Журнал «*Безопасность*» содержит записи о таких событиях, связанных с безопасностью (например, успешные и безуспешные попытки доступа в систему, управление учётными записями, изменение разрешений и прав доступа к файлам и папкам и т. п.).

События подразделяются на типы, к которым относятся: а) *сведения*, б) *предупреждение* и в) *ошибка*.

События типа «*Сведения*» описывают успешное выполнение операций, таких как запуск или некоторое действие системной службы

События типа «*Предупреждение*» отображают некоторые проблемы, имеющие место в работе операционной системы. Данные события могут свидетельствовать и о незначительной проблеме в работе системы (приложения), не требующей немедленного вмешательства пользователя, но регулярное появление одного и того же события может со временем привести к ошибкам.

События «*Ошибка*» описывают ошибки, возникшие из-за неудачного выполнения задач, отображает проблемы, которые могут привести к потере работоспособности системы или потере информации.

По центру, при выборе одной из «папок» слева будет отображаться сам список событий, а при выборе любого из них, в нижней части вы увидите более подробную информацию о нем.

В правой части собраны ссылки на действия, позволяющие отфильтровать события по параметрам, найти нужные, создать настраиваемые представления, сохранить список и создать задачу в планировщике заданий, которая будет связана с определенным событием.

При выборе какого-либо события, в нижней части будет отображаться информация о нем, состоящая из различных блоков информации (рис. 18). Рассмотрим некоторые, наиболее важные из них.

Имя журнала – имя файла журнала, куда была сохранена информация о событии.

Источник – название программы, процесса или компонента системы, которое сгенерировало событие (если вы видите здесь Application Error), то имя самого приложение вы можете увидеть в поле выше.

Код – код события. Информацию о кодах событий можно найти в Интернете, например по адресу: **https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/default.aspx?i=j**. (рис. 19). Рекомендуется также искать в англоязычном сегменте интернета по запросу «**Event ID + цифровое обозначение кода + название приложения, вызывавшего сбой** (поскольку коды событий для каждой программы уникальны)». (рис. 20). Также для поиска

подойдет и текстовая информация об ошибке, указанная на вкладке «Общие» окна «Свойства событий».

Дата – дата и время события.

Пользователь и *компьютер* – сообщает о том, от имени какого пользователя и на каком компьютере был запущен процесс, вызвавший событие.

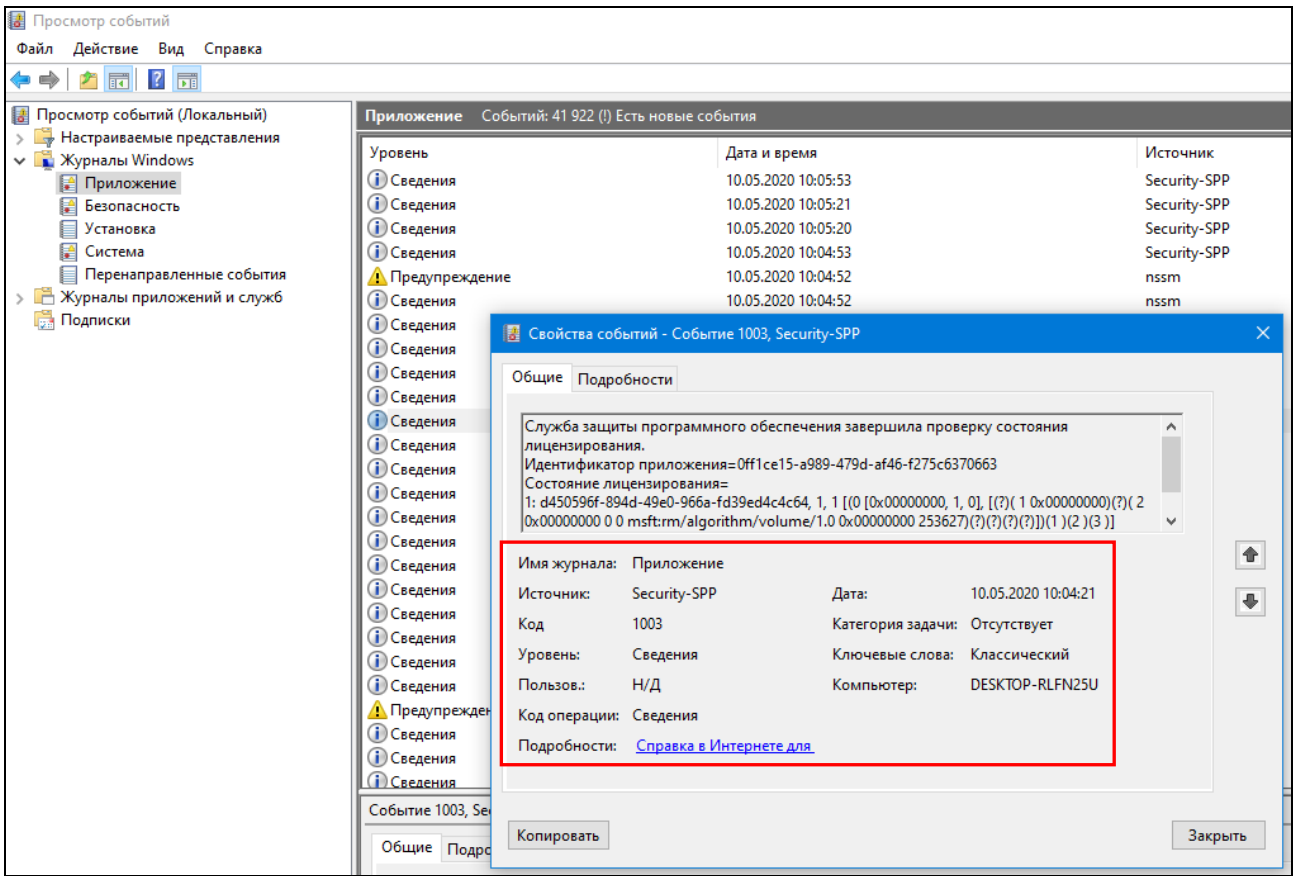


Рис. 18. Журнал событий ОС Windows 10.

Для проведения анализа проблейной ситуации, имевшей место на вашем ПК, необходимо открыть соответствующий журнал событий и найти события, которые предшествовали данной ситуации.

Возвращаясь к нашему примеру, нам необходимо установить пользователя ПК, который удалил файл **МК1.docx**, а также дату и время удаления. Алгоритм действий, предпринимаемых для решения данной задачи будет выглядеть следующим образом.

1. С помощью интернет-ресурсов выясняем код события, связанного с удалением объекта файловой структуры: 4660 (рис. 21).

2. В журнале событий «Безопасность» открываем «Фильтр текущего журнала». Устанавливаем: дату (*любое время*), уровень события (*сведения*), код события (*4660*), источники событий (*Microsoft Windows security auditing*), пользователя (*все пользователи*). Нажимаем «Ок» (рис. 22).

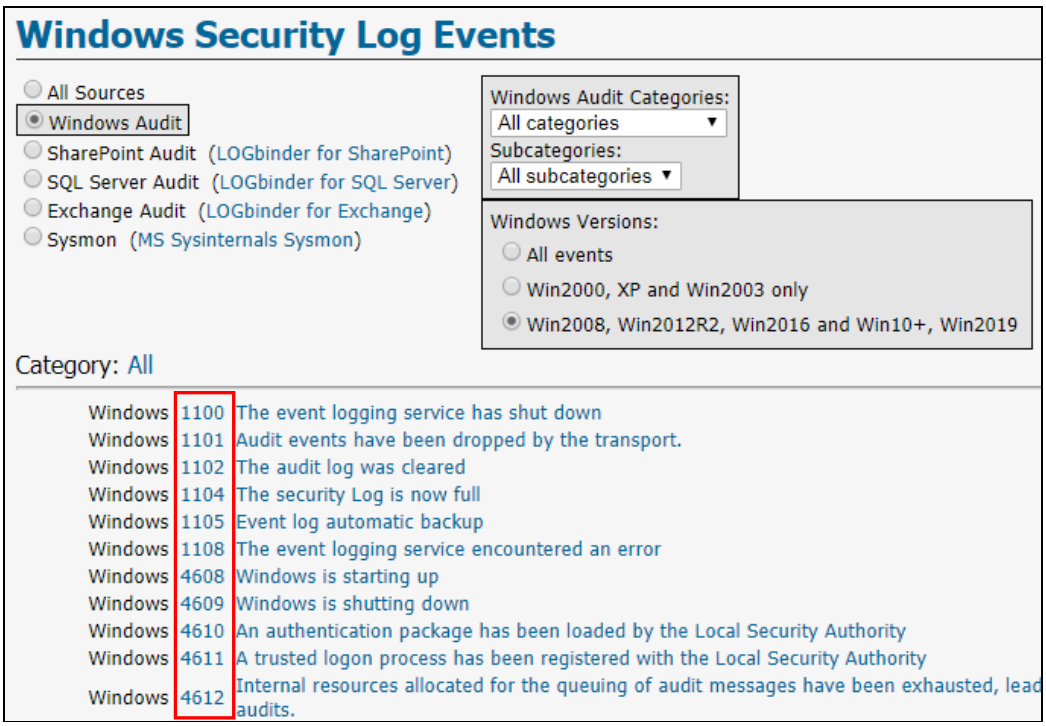


Рис. 19. Информация о кодах событий безопасности на специальном сайте по адресу https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/default.aspx?i=j

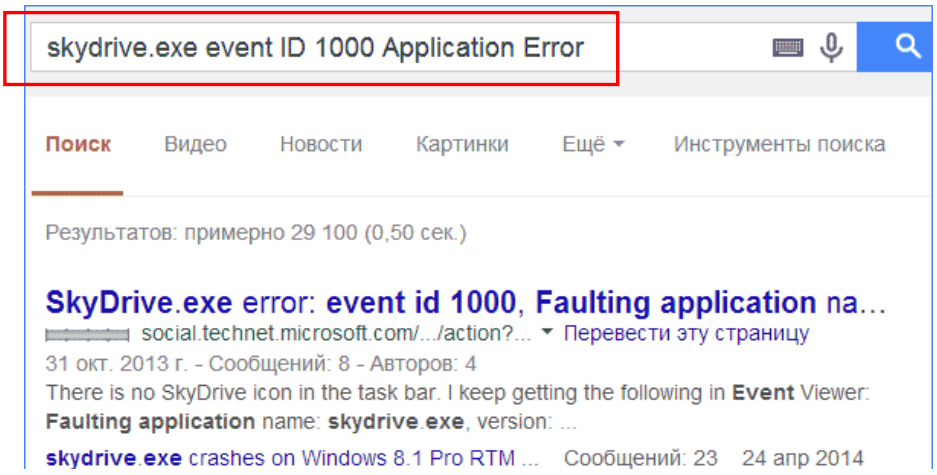


Рис. 20. Пример поиска информации о кодах событий безопасности в интернете

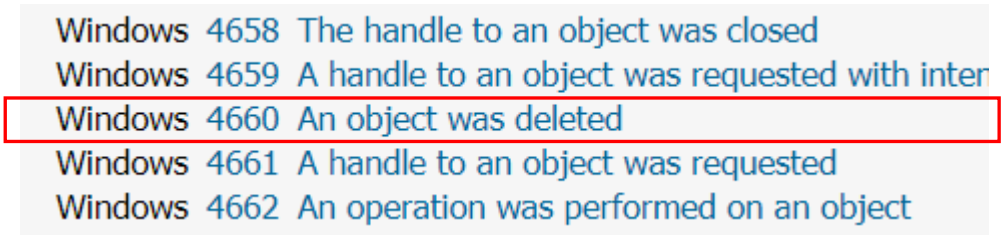


Рис. 21. Информация о кодах событий безопасности

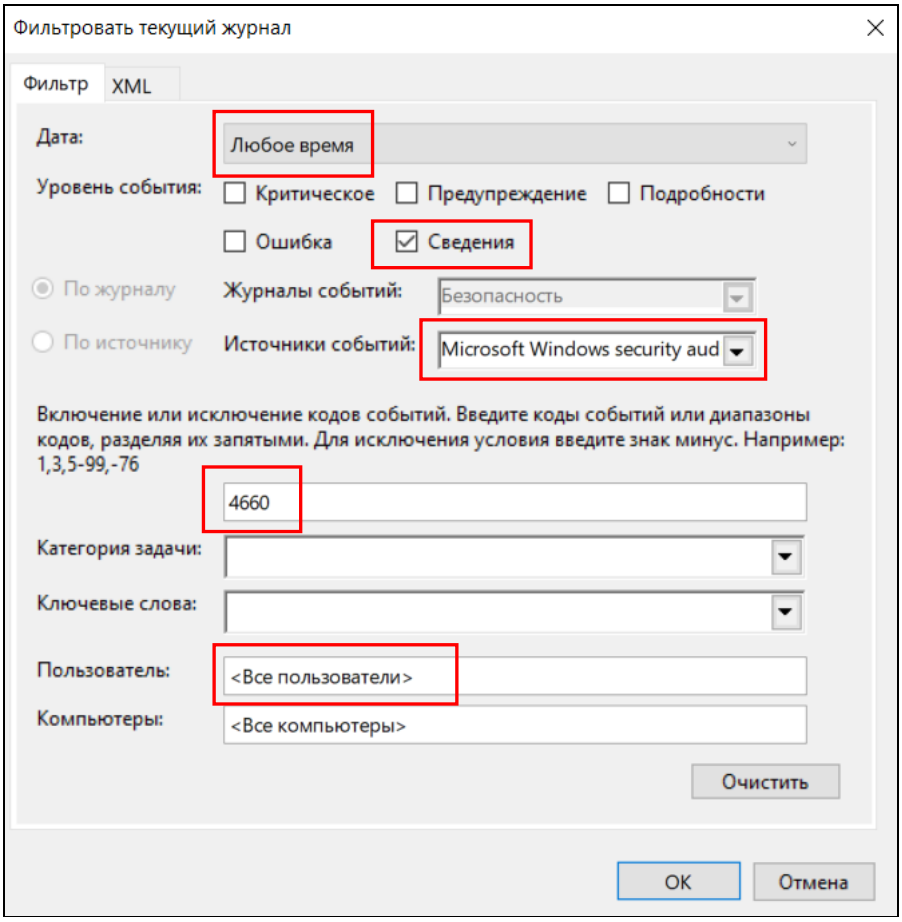


Рис. 22. Фильтр текущего журнала

3. В открывшемся окне отфильтрованных событий безопасности находим сообщение об искомомом событии (рис. 23). Однако, если внимательно изучить тело сообщения, то можно обнаружить, в нем содержится имя пользователя (**Гость1**), дата, время события, а также еще много всякой служебной информации, но нет имени файла. Зато есть код дескриптора объекта: **0x1730**.

Для того, чтобы точно знать какие файлы удалены, необходимо просто найти все события с ID 4660, а так же предшествующие каждому этому событию – событие с кодом 4663 (*An attempt was made to access an object, была сделана попытка получить доступ к объекту*), в котором будет содержаться номер нужного дескриптора и соответствующее ему имя файла.

4. В журнале событий «Безопасность» снова открываем «Фильтр текущего журнала». Устанавливаем: дату (*любое время*), уровень события (*сведения*), коды события (*4663, 4660*), источники событий (*Microsoft Windows security auditing*), пользователя (*все пользователи*). Нажимаем «Ок» (рис. 24).

5. В открывшемся окне отфильтрованных событий безопасности находим сообщение с кодом 4663, предшествующее событию с кодом 4660 (рис. 25).

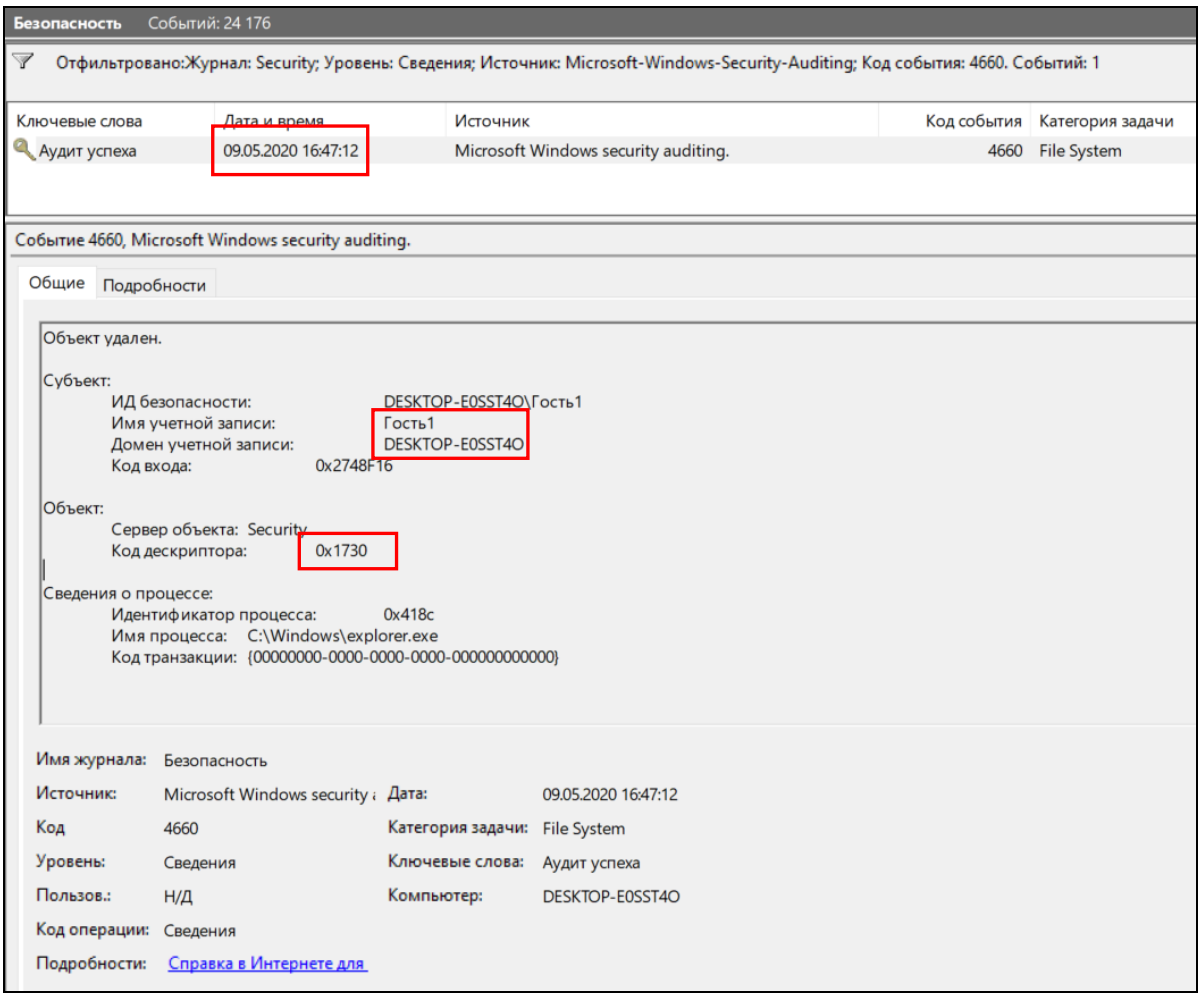


Рис. 23. Окно отфильтрованных событий безопасности журнала событий

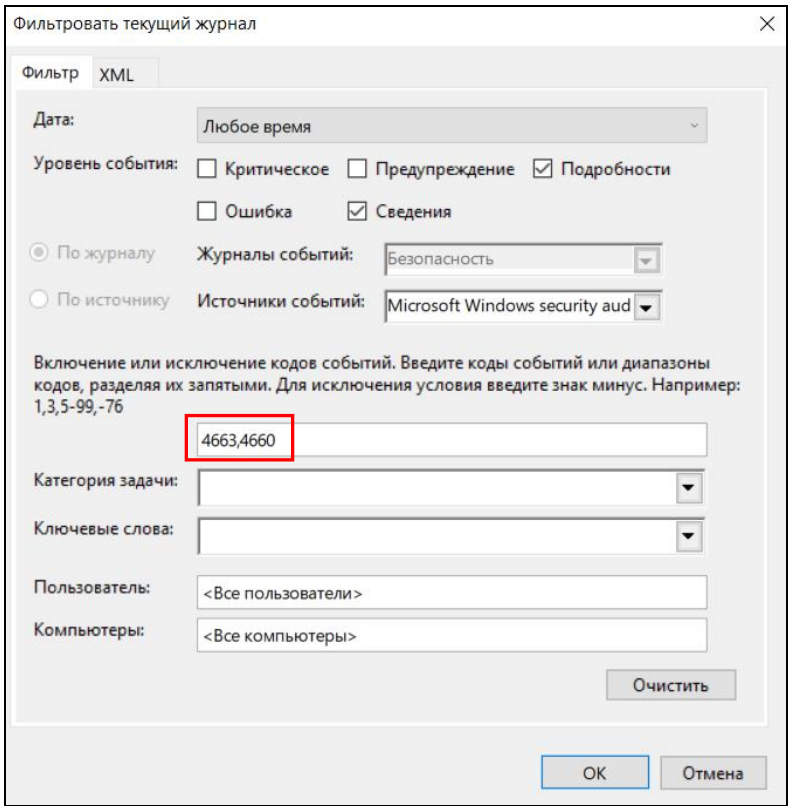
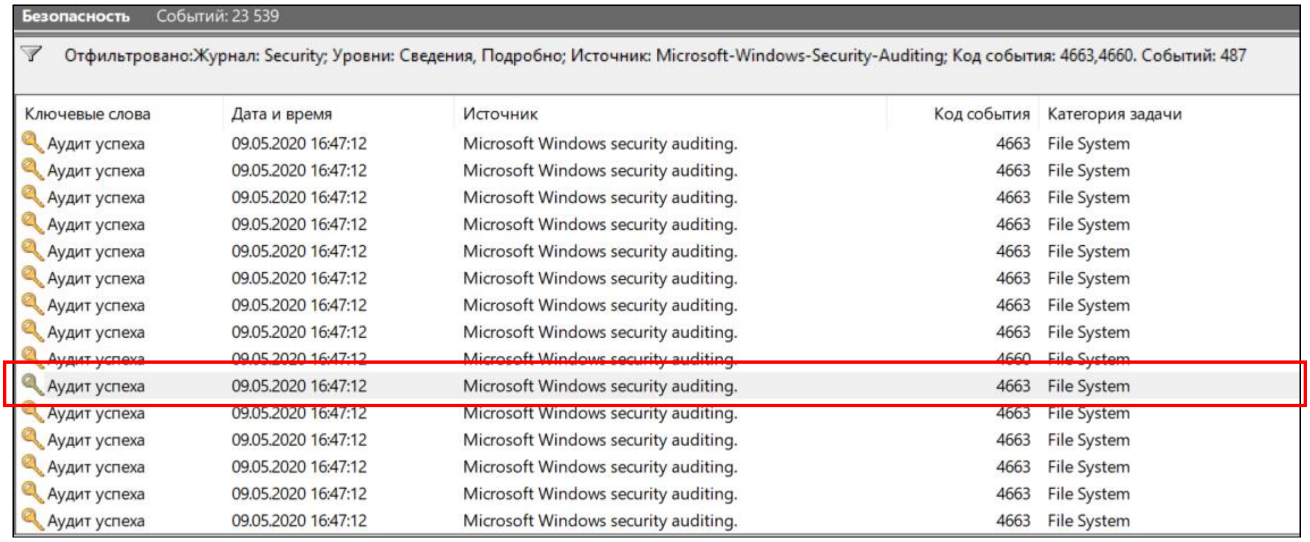


Рис. 24. Фильтр текущего журнала



Безопасность Событий: 23 539

Отфильтровано:Журнал: Security; Уровни: Сведения, Подробно; Источник: Microsoft-Windows-Security-Auditing; Код события: 4663,4660. Событий: 487

Ключевые слова	Дата и время	Источник	Код события	Категория задачи
Аудит успеха	09.05.2020 16:47:12	Microsoft Windows security auditing.	4663	File System
Аудит успеха	09.05.2020 16:47:12	Microsoft Windows security auditing.	4663	File System
Аудит успеха	09.05.2020 16:47:12	Microsoft Windows security auditing.	4663	File System
Аудит успеха	09.05.2020 16:47:12	Microsoft Windows security auditing.	4663	File System
Аудит успеха	09.05.2020 16:47:12	Microsoft Windows security auditing.	4663	File System
Аудит успеха	09.05.2020 16:47:12	Microsoft Windows security auditing.	4663	File System
Аудит успеха	09.05.2020 16:47:12	Microsoft Windows security auditing.	4663	File System
Аудит успеха	09.05.2020 16:47:12	Microsoft Windows security auditing.	4663	File System
Аудит успеха	09.05.2020 16:47:12	Microsoft Windows security auditing.	4660	File System
Аудит успеха	09.05.2020 16:47:12	Microsoft Windows security auditing.	4663	File System
Аудит успеха	09.05.2020 16:47:12	Microsoft Windows security auditing.	4663	File System
Аудит успеха	09.05.2020 16:47:12	Microsoft Windows security auditing.	4663	File System
Аудит успеха	09.05.2020 16:47:12	Microsoft Windows security auditing.	4663	File System
Аудит успеха	09.05.2020 16:47:12	Microsoft Windows security auditing.	4663	File System
Аудит успеха	09.05.2020 16:47:12	Microsoft Windows security auditing.	4663	File System

Рис. 25. Фильтр текущего журнала

Если изучить описание данного события, то можно обнаружить, что в нем содержится не только имя учетной записи из-под которой было выполнено удаление (имя пользователя) (**Гость1**), дата, время события, операция доступа (имя процесса) (*Delete*), но и имя удаленного файла (рис. 26).

Таким образом, два события от источника *Microsoft Windows security auditing* генерируются одновременно при успешном удалении файла, но записываются последовательно, сначала 4663, потом 4660. При этом их порядковые номера различаются на один. У 4660 порядковый номер на единицу больше чем у 4663. Именно по этому свойству и ищется нужное событие.

Примечание: не рекомендуеся злоупотреблять применением политик аудита доступа к объектам и регистрацией доступа к большому числу объектов, т.к. системой генерируется очень большое число записей, отыскать среди которых нужные будет весьма непросто. Наиболее рациональный способ применения аудита доступа к объектам – настройка данного аудита в те моменты, когда есть обоснованные опасения о наличии попыток несанкционированного доступа.

Кроме того, при наличии в журнале информации об удалении файла пользователем не следует спешить однозначно интерпретировать его как преднамеренное или даже злонамеренное. Многие программы (особенно этим грешат программы пакета MS Office) при сохранении данных сначала создают временный файл, сохраняют документ в него, а старую версию файла удаляют. В этом случае имеет смысл вести анализ удаления файлов с учетом этого факта. Либо совсем радикально отсеивать события от процессов, например, winword.exe, excel.exe и пр.

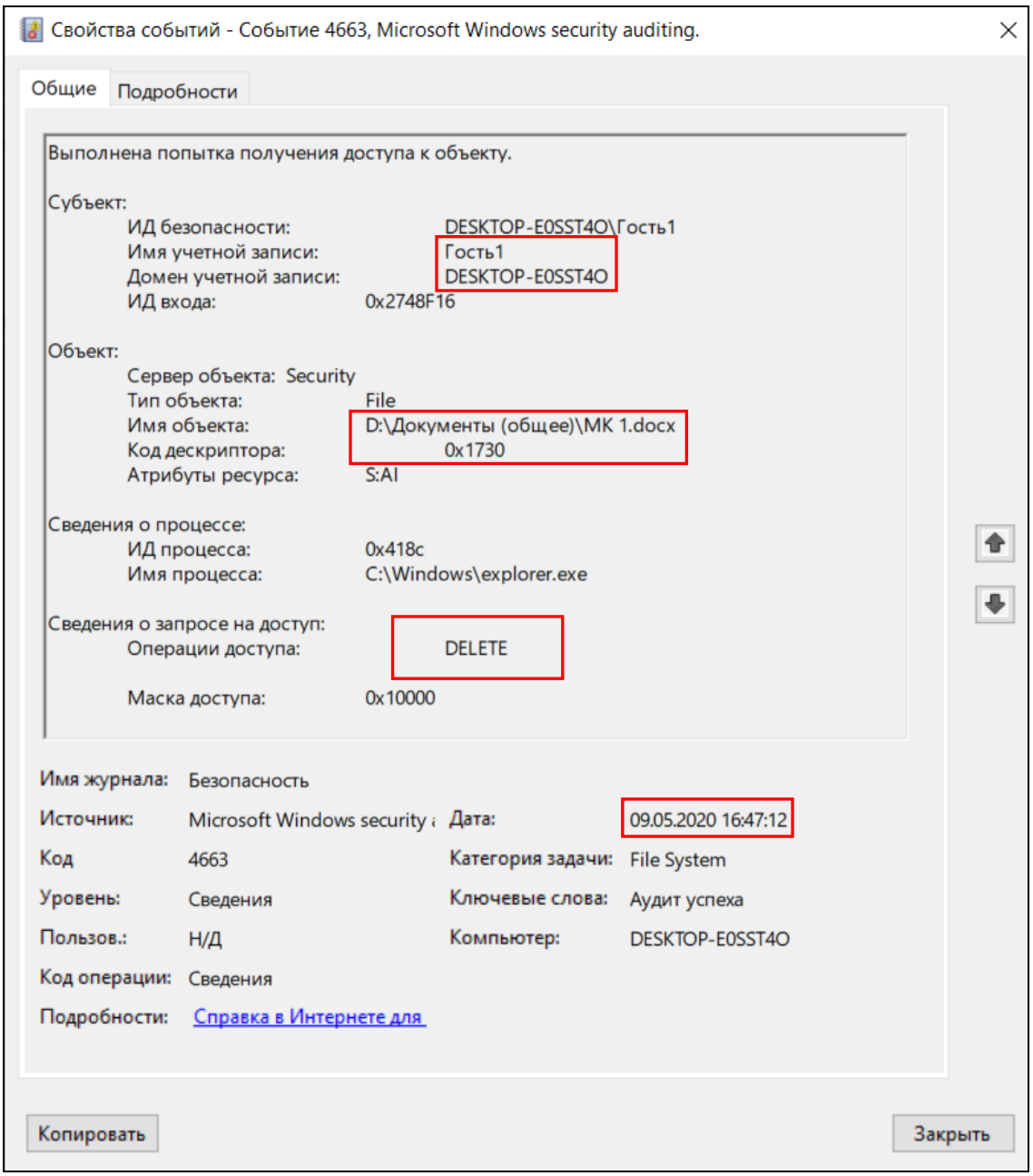


Рис. 26. Окно свойств события журнала безопасности.

Следует также отметить, что большое количество событий в журналах приводит к тому, что в них сложно ориентироваться. К тому же, большинство из них не несут в себе критически важной информации. Лучший способ отобразить только нужные события – использовать настраиваемые представления: вы можете задать уровень событий, которые нужно отображать – ошибки, предупреждения, критические ошибки, а также их источник или журнал.

Для того, чтобы создать настраиваемое представление, нажмите соответствующий пункт в панели справа. Уже после создания настраиваемого представления, вы имеете возможность применить к нему дополнительные фильтры, кликнув по «Фильтр текущего настраиваемого представления» (рис. 27).

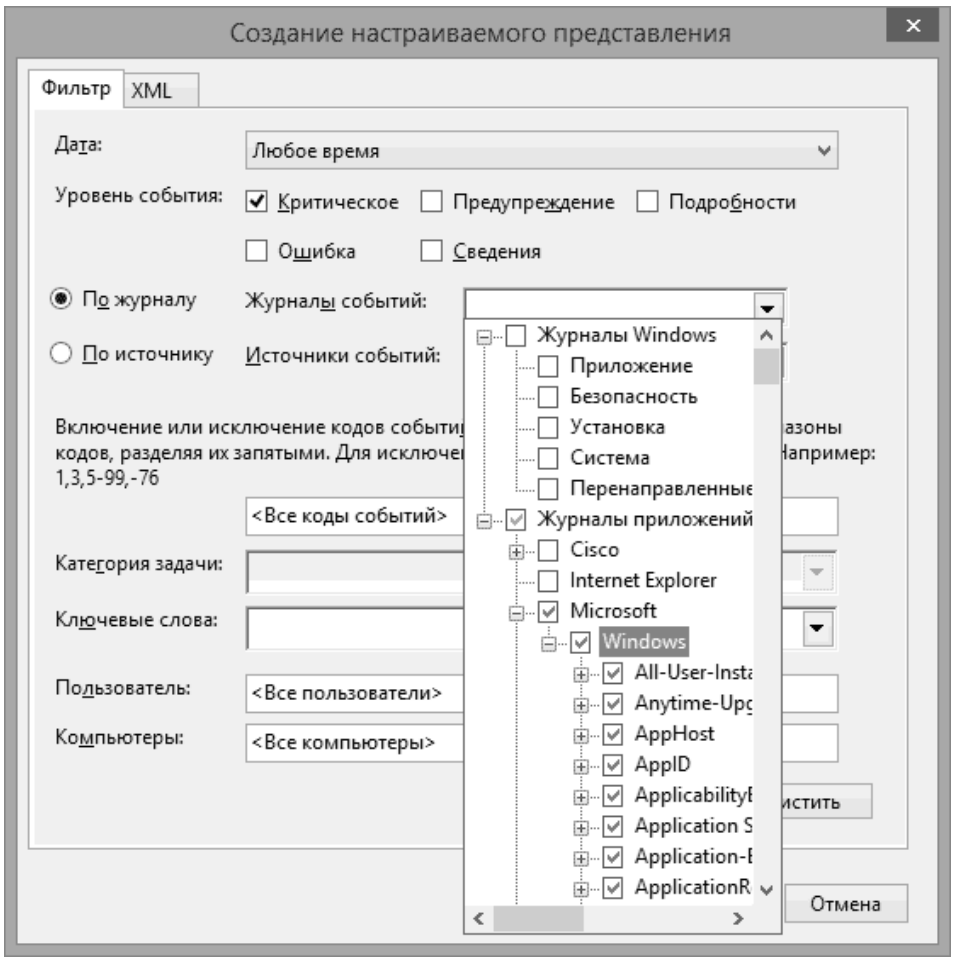


Рис. 27. Создание настраиваемого представления журнала безопасности

Кроме того, в журнале событий ОС Windows 10 существует возможность связать события с задачами, которые автоматически выполняются при возникновении события. Возвращаясь к предыдущему примеру, можно, например, обеспечить отправку уведомления системному администратору по электронной почте всякий раз при возникновении события, связанного с удалением файлов из общей папки. Для этого следует выделить нужное событие в журнале событий и нажать на ссылку «Привязать задачу к журналу» (в правой части журнала событий). При этом запустится мастер создания задачи (рис. 28), который запросит: имя задачи и просит определить программу, сообщение электронной почты или экранное сообщение. По окончании работы мастера можно просмотреть событие, его свойства и историю, открыв оснастку «Планировщик заданий» консоли управления MMC (Win+R → mmc → Enter) (рис. 29).

Для обеспечения безопасности компьютерной системы целесообразно разделить полномочия администраторов компьютерной системы и аудиторов (пользователей с правами доступа к журналу аудита и изменения параметров аудита). Если этого не сделать, то возникнет ситуация, при которой установка параметров политики безопасности и проверка ее соблюдения сосредоточатся в одних руках, что будет противоречить принципу разграничения полномочий.

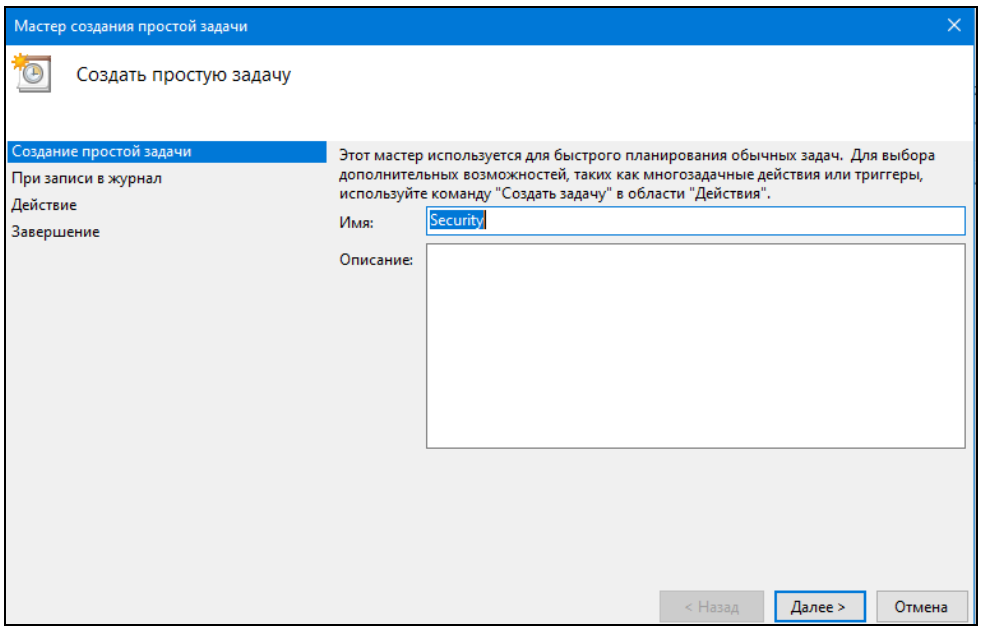


Рис. 28. Мастер создания задачи в журнале событий (первый шаг)

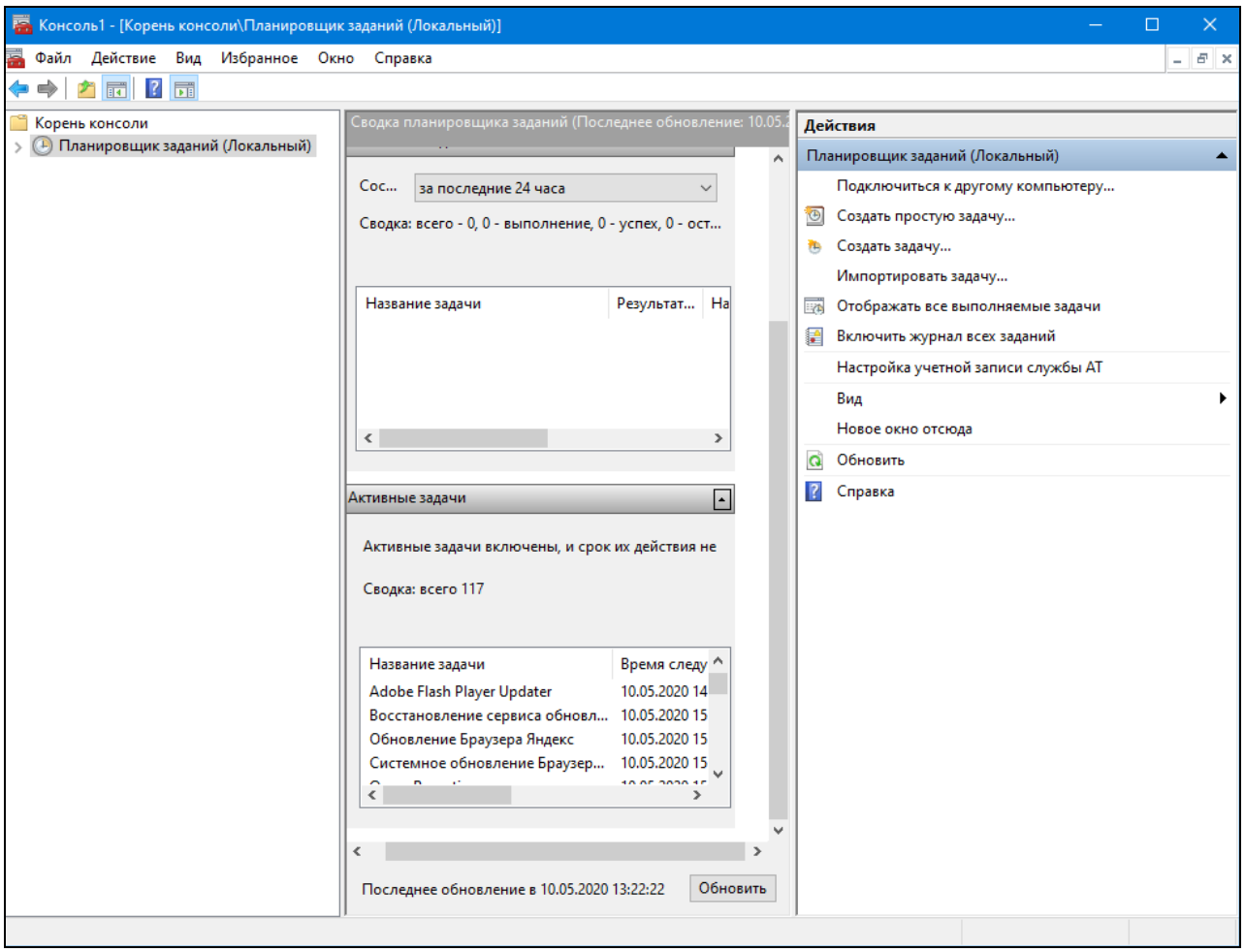


Рис. 29. Оснастка «Планировщик заданий» консоли управления MMC

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 1 (3.3)
(практические задания для самостоятельного выполнения)

Тема: 3.3 Каналы утечки информации и безопасность информационных систем.

Учебные вопросы:

1. Настройка параметров доверенной загрузки операционной системы.
2. Аутентификация, авторизация и управление доступом в ОС Windows.
3. Политики безопасности ОС.
4. Регистрация и оперативное оповещение о событиях безопасности.

В ходе выполнения практического задания слушателями ведется файл-отчет. Файл-отчет сохраняется в виде файла MS Word. Название для файла-отчета формируется по правилу: «номер группы» пробел «фамилия слушателя» пробел «тема занятия» (например: «0341 Иванов 2.5»). Файлы-отчеты в конце занятия сохраняются в сетевую папку, указанную преподавателем. При подготовке файла-отчета по каждому заданию данной темы необходимо не только указать конечный результат, но и кратко описать механизм его достижения (например, последовательность действий, промежуточные этапы и пр.). Рекомендуется использовать снимки (скриншоты) экрана, получаемые с помощью клавиши *PrtScr* либо функции *Фрагмент экрана,* доступной в области параметров уведомлений ОС.

После окончания занятия необходимо удалить все файлы и папки, учетные записи и настройки параметров ОС, созданные в ходе выполнения практического занятия.

ВОПРОС 1. Настройка параметров доверенной загрузки операционной системы

1. Используя программный эмулятор среды BIOS (находится в папке, указанной преподавателем), ознакомьтесь с его интерфейсом. Изучите структуру и основные разделы BIOS. С использованием сведений, указанных в табл. 1 (см. теоретические сведения), получите представление о функциональном назначении доступных опций и параметров безопасности BIOS ПК.

Используя полученные знания об основных функциональных возможностях BIOS, подготовьте файл-отчет, в котором выполните следующие действия[3]:

2. С помощью компонента ОС «Сведения о системе операционной системы Windows» (Win+R → msinfo32 → Enter) заполните таблицу:

Элемент системы	Значение
Версия BIOS	
Режим BIOS	

[3] Название для файла-отчета формируется по правилу: «номер группы» пробел «фамилия слушателя» пробел «тема занятия» (*например: «0341 Иванов 2.3»).* Файлы-отчеты в конце занятия сохраняются в сетевую папку, указанную преподавателем.

3. Опишите функциональное назначение опций (параметров) безопасности BIOS вашего ПК:

Наименование опции (параметра) безопасности BIOS	**Описание**

4. Перечислите последовательность действий по настройке параметров BIOS, необходимых для загрузки компьютера с загрузочного USB-диска.
5. Перечислите порядок действий для установления пароля BIOS на загрузку ОС.
6. Решите задачу. После изменения настроек BIOS (установки в BIOS некорректных параметров) система проходит процедуру инициализации POST, но компьютер не грузится. Укажите возможные причины.
7. Подготовьте ответы на контрольные вопросы (см. ниже).

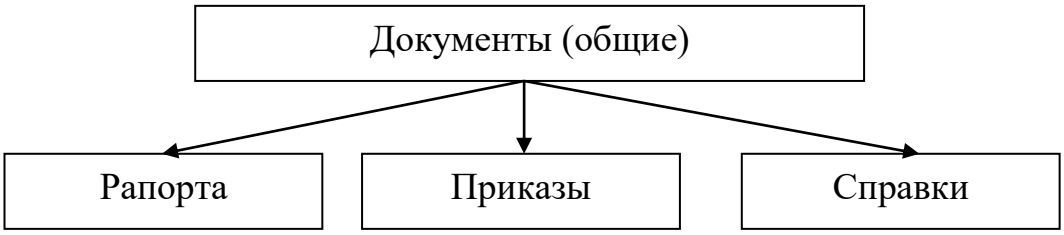
КОНТРОЛЬНЫЕ ВОПРОСЫ:

1. Какие возможности по ограничению несанкционированного доступа к компьютерной информации имеет базовая система ввода-вывода BIOS?
2. Какие функциональные клавиши позволяют осуществить вход в BIOS?
3. Какая опция BIOS позволит определить наличие вируса в загрузочном секторе? Как она действует?
4. Чем отличается пароль администратора от пользовательского пароля BIOS?
5. Каким образом можно изменить пароль пользователя BIOS?
6. Как удалить пароль на загрузку системы, установленный в BIOS?
7. Какая опция BIOS позволяет включить режим защиты от записи для жесткого диска?
8. Какая опция BIOS позволяет запретить возможность использования кнопки RESET на системном блоке?
9. Какая опция BIOS позволяет определить, в каких ситуациях будет запрашиваться пароль?
10. Какая опция BIOS позволяет устанавливать уровень безопасности?
11. Какая опция BIOS позволяет защитить загрузочный сектор и таблицу разделов жесткого диска?
12. Какая опция позволяет заблокировать возможность записи в микросхему Flash BIOS?
13. Какие функции BIOS позволяет осуществить защиту ПК от загрузки с внешних носителей информации?

ВОПРОС 2. Аутентификация, авторизация и управление доступом в ОС Windows

1. Создайте в системе две пользовательские учетные записи ***Курсант 1*** и ***Курсант 2*** (тип учетных записей – *стандартная*).

2. Создайте на диске **D:** следующую иерархию папок:



В каждой из папок второго уровня создайте одноименные текстовые документы произвольного содержания.

3. Установите права доступа пользователей ***Курсант 1*** и ***Курсант 2*** к указанным папкам согласно таблице 1.

Таблица 1

Матрица распределения права доступа (уровня разрешений) пользователей к объектам			
Наименование папки / Наименование учетной записи	Рапорта	Приказы	Справки
Курсант 1	Полный доступ	Чтение и выполнение	Полный запрет
Курсант 2	Чтение и выполнение	Полный запрет	Полный доступ

4. Задайте квоту на использование каждым пользователем дискового пространства в размере 100 Мб, а порог предупреждения задайте на 8 Мб.

5. Зайдите в систему от имени созданного вами пользователя. Проверьте настройки доступа и квот.

6. Подготовьте ответы на контрольные вопросы (см. ниже).

КОНТРОЛЬНЫЕ ВОПРОСЫ:

1. Что такое аутентификация и авторизация? Чем они отличаются?
2. Что такое учётная запись пользователя? Какие права доступа к объектам файловой системы существуют?
3. Перечислите порядок действий по настройке прав доступа.
4. Что такое квота дискового пространства?
5. Как осуществляется управления квотами дискового пространства на локальном компьютере?

6. Что означает протоколирование превышения квоты для тома?

ВОПРОС 3. Политики безопасности ОС

1. Вернитесь в систему под учетной записью администратора.

2. Добавьте ярлык оснастки «Локальная групповая политика безопасности» (*gpedit.msc)* на рабочий стол.

3. С использованием редактора локальной групповой политики настройте следующие параметры безопасности ПК:

3.1. Активизируйте обязательное нажатие клавиш CTRL+ALT+DEL перед входом в систему;

3.2. Отключите отображение учетных данных последнего пользователя на экране входа в систему;

3.3. Отключите отображение учетных данных последнего пользователя, выполнившего вход в систему;

3.4. Отключите функцию автозапуска для компакт-дисков и съемных носителей;

3.5. Отключите диспетчер задач;

3.6. Отключите автоматическое отправление в корпорацию Майкрософт отчетов об ошибках Windows;

3.7. Запретите переопределять предупреждения функции «SmartScreen Защитника Windows» о потенциально вредоносных веб-сайтах;

3.8. Включите уведомления для антивирусной программы при открытии вложений. При этом:

а) задайте уровень риска для вложений: *высокий риск*.

б) настройте список типов файлов с высоким уровнем риска: *.exe; *.com; *.pdf; *.zip.

в) установите логику доверия для вложенных файлов (способ определения риска – учитывать обработчик файлов и их типы).

3.9. Запретите предоставлять общий доступ к файлам при помощи мастера общего доступа.

3.10. Настройте следующие параметры политики паролей учетных записей ПК:

а) число новых уникальных паролей, которые должны быть назначены учетной записи пользователя до повторного использования старого пароля: 12;

б) период времени (в днях), в течение которого можно использовать пароль (максимальный срок действия): 30;

в) минимальная длина пароля: 8;

г) пароль должен отвечать требованиям сложности;

д) количество неудачных попыток входа в систему, приводящее к блокировке учетной записи пользователя: 3;

е) количество минут, в течение которых учетная запись остается заблокированной до ее автоматической разблокировки: 5.

3.11. Активизируйте аудит событий входа в систему. Задайте аудит отказов.

4. С помощью параметра оснастки «Все параметры» (Политика «Локальный компьютер > Конфигурация компьютера > Административные шаблоны > Все параметры) отобразите в правой части редактора локальной групповой политики все заданные вами параметры конфигурации компьютера, отсортировав их по столбцу «Состояние». Рядом со столбцом «Состояние» разместите столбец «Путь». Разверните окно консоли на весь экран. Сделайте экранную копию окна редактора локальной групповой политики и разместите ее в файл-отчете.

5. С помощью параметра оснастки «Все параметры» (Политика «Локальный компьютер > Конфигурация пользователя > Административные шаблоны > Все параметры) отобразите в правой части редактора локальной групповой политики все заданные вами параметры конфигурации пользователя, отсортировав их по столбцу «Состояние». Рядом со столбцом «Состояние» разместите столбец «Путь». Разверните окно консоли на весь экран. Сделайте экранную копию окна редактора локальной групповой политики и разместите ее в файл-отчете.

6. С помощью консоли управления *mmc* установите для локального пользователя *Курсант 1* следующие параметры политики безопасности:

6.1. Отключите возможность добавления компонентов Windows;

6.2. Отключите возможность выполнения программы «Звукозапись»;

6.3. Отключите доступ к приложению MS Store.

6.4. Установите максимальный размер для профиля пользователя (1 Гб), а также уведомление, если допустимый размер профиля превышен.

6.5. Отключите возможность предоставлять общий доступ к файлам в своем профиле.

6.6. Ограничить доступ к диску C:\

6.7. Удалить вкладку «Безопасность» из проводника.

6.8. Установите запрет на добавление файлов и папок в корневую папку с файлами пользователя в проводнике.

6.9. Отключить доступ к панели управления и параметрам компьютера

6.10. Установите запрет записи на съемные запоминающие устройства;

6.11. Установите запрет записи на компакт-диски и DVD-диски;

7. С помощью параметра оснастки «Все параметры» (Политика «Локальный компьютер\Курсант 1 > Конфигурация пользователя > Административные шаблоны > Все параметры) отобразите в правой части консоли ММС все заданные вами параметры политики безопасности, отсортировав их по столбцу «Состояние». Рядом со столбцом «Состояние» разместите столбец «Путь». Разверните окно консоли на весь экран. Сделайте экранную копию окна консоли ММС и разместите ее в файл-отчете.

8. Сохраните файл консоли управления на рабочем столе под именем «ММС для Гость» для последующего редактирования политик.

9. Оформите в файл-отчете таблицу, в которой опишите назначение каждого из установленных в п.п. 3.1-3.11, 6.1-6.11 параметров политик безопасности:

№ задания (п.п. 3.1-3.11, 6.1-6.11)	**Параметр политики безопасности**	**Основное назначение, результат применения**

10. С помощью интегрированного сервиса AppLocker создайте правило, которое позволит пользователю ***Курсант 1*** запускать все программы Windows за исключением редактора реестра (regedit.exe). Данному правилу присвойте имя «Правило 1». Установите режим применения политики AppLocker для этого правила: *только аудит.*

11. С помощью интегрированного сервиса AppLocker создайте правило, которое позволит пользователю ***Курсант 1*** запускать любые исполняемые файлы только из каталогов «Windows» и «Program Files». Данному правилу присвойте имя «Правило 2». Установите режим применения политики AppLocker для этого правила: *принудительное применение правил.*

12. Осуществите проверку выполнения правил AppLocker для каждой из учетных записей (***Курсант 1*** и ***Курсант 2***). Результаты зафиксируйте в файл-отчете.

13. Вернитесь в систему под учетной записью администратора. Просмотрите журнал событий AppLocker. Найдите и зафиксируйте в файл-отчете информационные события, свидетельствующие об успешном применении правила «*Правило 1*» для *Курсанта 1*.

Установите режим применения политики AppLocker для этого правила: *принудительное применение правил.*

14. Осуществите анализ имеющихся системных служб и сервисов Windows, не используемых на вашем ПК, но несущих потенциальные угрозы для безопасности системы.

Результаты оформите в файл-отчете в виде следующей таблицы:

№ п/п	**Наименование службы**	**Описание потенциальной угрозы**	**Тип запуска / состояние**	**Зависимость от других компонентов Windows**

15. Продемонстрируйте работу и файл-отчет преподавателю.

16. Осуществите сброс настроек правил AppLocker.

17. Осуществите сброс настроек политик безопасности.

18. Удалите учетные записи ***Курсант 1*** и ***Курсант 2***.

19. Подготовьте ответ на контрольные вопросы (см. ниже).

КОНТРОЛЬНЫЕ ВОПРОСЫ:

1. Политика безопасности ОС: сущность, содержание, классификация.
2. Локальная и групповая политики безопасности: соотношение понятий, способы запуска и настройки, особенности использования.
3. Особенности обновления (применения) параметров локальной групповой политики.
4. Локальные политики безопасности: назначение, структура и содержание.
5. Консоль управления MMC: основное назначение, примеры использования.
6. Оснастка Windows: понятие, виды, содержание, предназначение, примеры использования.
7. Особенности просмотра результирующей политики (RSoP) для конкретного пользователя и компьютера.
8. Последовательность действий для возврата к первоначальным настройкам локальных групповых политик безопасности ОС Windows.
9. Технологии управления доступом и сервис AppLocker: методологические различия в подходах к обеспечению безопасности системы.
10. Примеры сценариев, при которых может использоваться сервис AppLocker
11. Общий алгоритм действий по созданию и настройке правил с помощью сервиса AppLocker.
12. Анализ журнала событий AppLocker. Типы информационных событий AppLocker.
13. Основные уязвимости системных файлов и драйверов Windows.
14. Цифровая подпись системного файла как паспорт, гарантирующий его целостность и подлинность.
15. Проверка целостности системных файлов с помощью сервиса «File Signature Verification». Примеры использования.
16. Службы и сервисы ОС Windows. Характеристики. Потенциальные угрозы безопасности. Оснастка управления. Режимы работы.

ВОПРОС 4. Регистрация и оперативное оповещение о событиях безопасности

1. Используя возможности журнала событий ОС Windows, осуществите анализ истории включения, выключения компьютера (дата и время), а также времени его работы.

Проанализируйте также события, связанные с запуском системы после возможного некорректного завершения работы.

Указанные действия подробно отразите в файле-отчете.

2. Предъявите работу, а также файл-отчет преподавателю.

КОНТРОЛЬНЫЕ ВОПРОСЫ:

1. Что такое протоколирование и аудит событий безопасности? Какие цели преследуются при использовании данных средств?
2. Какие категории событий регистрируются в журналах безопасности?
3. Перечислите основные требования политики аудита в компьютерной системе.
4. Перечислите механизм настройки протоколирования и аудита наиболее важных событий безопасности ОС локального компьютера.
5. Что такое «Аудит успеха» и «Аудит отказа»?
6. Опишите основные элементы интерфейса журнала событий ОС Windows.
7. Какие виды журналов представлены в категории «Журналы Windows»? Каково их предназначение?
8. Что такое код события? Каким образом расшифровывается его значение?