Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Электронная тетрадь**

по основам защиты информации

Студент: Савостин А. Д.

ФИТ 2 курс 1 группа

Преподаватель: Берников В. О.

Минск 2020

**Практическое занятие №1**

**Тема «Концепция национальной безопасности Республики Беларусь»**

Цель: изучить концепцию национальной безопасности РБ.

**Информационная безопасность** ­– состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере.

**Национальные интересы** – совокупность потребностей государства по реализации сбалансированных интересов личности, общества и государства, позволяющих обеспечивать конституционные права, свободы, высокое качество жизни граждан, независимость, территориальную целостность, суверенитет и устойчивое развитие Республики Беларусь;

Национальные интересы Республики Беларусь охватывают все сферы жизнедеятельности личности, общества и государства, тесно взаимосвязаны и являются концептуальными ориентирами для ее долгосрочного развития.

Основные **национальные интересы** включают в себя следующие пункты:

* реализацию конституционных прав граждан на получение, хранение и распространение полной, достоверной и своевременной информации;
* формирование и поступательное развитие информационного общества;
* равноправное участие Республики Беларусь в мировых информационных отношениях;
* преобразование информационной индустрии в экспортно-ориентированный сектор экономики;
* эффективное информационное обеспечение государственной политики;
* обеспечение надежности и устойчивости функционирования критически важных объектов информатизации.
* деструктивное информационное воздействие на личность, общество и государственные институты, наносящее ущерб национальным интересам;
* нарушение функционирования критически важных объектов информатизации;
* недостаточные масштабы и уровень внедрения передовых информационно-коммуникационных технологий;
* снижение или потеря конкурентоспособности отечественных информационно-коммуникационных технологий, информационных ресурсов и национального контента;
* утрата либо разглашение сведений, составляющих охраняемую законодательством тайну и способных причинить ущерб национальной безопасности.

Источники **угроз безопасности** делятся на внешние и внутренние.

**Внутренние источники угроз информационной безопасности:**

* распространение недостоверной или умышленно искаженной информации, способной причинить ущерб национальным интересам Республики Беларусь;
* зависимость Республики Беларусь от импорта информационных технологий, средств информатизации и защиты информации, неконтролируемое их использование в системах, отказ или разрушение которых может причинить ущерб национальной безопасности;
* несоответствие качества национального контента мировому уровню;
* недостаточное развитие государственной системы регулирования процесса внедрения и использования информационных технологий;
* рост преступности с использованием информационно-коммуникационных технологий;
* недостаточная эффективность информационного обеспечения государственной политики;
* несовершенство системы обеспечения безопасности критически важных объектов информатизации.

**Внешние источники информационных угроз:**

* открытость и уязвимость информационного пространства Республики Беларусь от внешнего воздействия;
* доминирование ведущих зарубежных государств в мировом информационном пространстве, монополизация ключевых сегментов информационных рынков зарубежными информационными структурами;
* информационная деятельность зарубежных государств, международных и иных организаций, отдельных лиц, наносящая ущерб национальным интересам Республики Беларусь, целенаправленное формирование информационных поводов для ее дискредитации;
* нарастание информационного противоборства между ведущими мировыми центрами силы, подготовка и ведение зарубежными государствами борьбы в информационном пространстве;
* развитие технологий манипулирования информацией;
* препятствование распространению национального контента Республики Беларусь за рубежом;
* широкое распространение в мировом информационном пространстве образцов массовой культуры, противоречащих общечеловеческим и национальным духовно-нравственным ценностям;
* попытки несанкционированного доступа извне к информационным ресурсам Республики Беларусь, приводящие к причинению ущерба ее национальным интересам.

С целью нейтрализации внутренних источников угроз и защиты от внешних угроз национальной безопасности в информационной сфере приняты следующие меры:

* разработка и реализация стратегии всеобъемлющей информатизации, ориентированной на развитие электронной системы осуществления административных процедур и переход государственного аппарата на работу по принципу информационного взаимодействия;
* последовательное повышение качества, объема и конкурентоспособности национального контента, который призван занимать доминирующее положение внутри страны, и его продвижение во внешнее информационное пространство;
* совершенствование нормативной правовой базы обеспечения информационной безопасности и завершение формирования комплексной государственной системы обеспечения информационной безопасности;
* наращивание деятельности правоохранительных органов по предупреждению, выявлению и пресечению преступлений против информационной безопасности, а также надежному обеспечению безопасности информации, охраняемой в соответствии с законодательством;
* разработка и внедрение современных методов и средств защиты информации в информационных системах, используемых в жизненно важной для страны инфраструктуре;
* доведении до граждан Республики Беларусь и внешней аудитории объективной информации о государственном курсе во всех сферах жизнедеятельности общества, официальной позиции по общественно значимым событиям внутри страны и за рубежом, о деятельности государственных органов;
* расширение каналов и повышение качества информирования зарубежной общественности;
* информационное противоборство, представляющее собой комплексное использование информационных, технических и иных методов, способов и средств для воздействия на информационную сферу с целью достижения политических, экономических и иных задач либо защиты собственного информационного пространства;
* участие Республики Беларусь в международных договорах, регулирующих на равноправной основе мировой информационный обмен, в создании и использовании межгосударственных, международных глобальных информационных сетей и систем.

**Практическое занятие №2**

**Тема «Решение задачи разработки средств защиты для обеспечения максимальной эффективности объекта в условиях несанкционированного доступа»**

Цель: научится решать задачи разработки средств защиты для обеспечения максимальной эффективности объекта в условиях несанкционированного доступа.

**Теоретическое введение**

Все методы защиты информации по характеру проводимых действий можно разделить на:

– законодательные (правовые);

– организационные;

– технические;

– комплексные.

Для обеспечения защиты объектов информационной безопасности должны быть соответствующие правовые акты, устанавливающие порядок защиты и ответственность за его нарушение. Законы должны давать ответы на следующие вопросы: что такое информация, кому она принадлежит, как может с ней поступать собственник, что является посягательством на его права, как он имеет право защищаться, какую ответственность несет нарушитель прав собственника информации.

Установленные в законах нормы реализуются через комплекс организационных мер, проводимых прежде всего государством, ответственным за выполнение законов, и собственниками информации. К таким мерам относятся издание подзаконных актов, регулирующих конкретные вопросы по защите информации (положения, инструкции, стандарты и т. д.), и государственное регулирование сферы через систему лицензирования, сертификации, аттестации.

Поскольку в настоящее время основное количество информации генерируется, обрабатывается, передается и хранится с помощью технических средств, то для конкретной ее защиты в информационных объектах необходимы технические устройства. В силу многообразия технических средств нападения приходится использовать обширный арсенал технических средств защиты. Наибольший положительный эффект достигается в том случае, когда все перечисленные способы применяются совместно, т.е. комплексно.

Принципиальным вопросом при определении уровня защищенности объекта является выбор критериев. Рассмотрим один из них ‑ широко известный критерий "эффективность - стоимость".

Пусть имеется информационный объект, который при нормальном (идеальном) функционировании создает положительный эффект (экономический, политический, технический и т.д.). Этот эффект обозначим через *Е0*. Несанкционированный доступ к объекту уменьшает полезный эффект от его функционирования (нарушается нормальная работа, наносится ущерб из-за утечки информации и т.д.) на величину *ΔЕ*. Тогда эффективность функционирования объекта с учетом воздействия несанкционированного доступа:

|  |  |
| --- | --- |
|  | (2.1) |

Относительная эффективность:

|  |  |
| --- | --- |
|  | (2.2) |

Уменьшение эффективности функционирования объекта приводит к материальному ущербу для владельца объекта. В общем случае материальный ущерб есть некоторая неубывающая функция от ΔЕ:

|  |  |
| --- | --- |
|  | (2.3) |

Будем считать, что установка на объект средств защиты информации уменьшает негативное действие несанкционированного доступа на эффективность функционирования объекта. Обозначим снижение эффективности функционирования объекта при наличии средств защиты через ΔЕ3, а коэффициент снижения негативного воздействия несанкционированного доступа на эффективность функционирования объект ‑ через К, тогда:

|  |  |
| --- | --- |
|  | (2.4) |

где К≥1.

Выражения (1) – (2) примут вид:

|  |  |
| --- | --- |
|  | (2.5) |

|  |  |
| --- | --- |
|  | (2.6) |

Стоимость средств защиты зависит от их эффективности, и в общем случае К – есть возрастающая функция от стоимости средств защиты (С):

|  |  |
| --- | --- |
|  | (2.7) |

Поскольку затраты на установку средств защиты можно рассматривать как ущерб владельцу объекта от возможности осуществления несанкционированного доступа, то суммарный ущерб объекту:

|  |  |
| --- | --- |
|  | (2.8) |

Если эффективность функционирования объекта имеет стоимостное выражение (доход, прибыль и т.д.), то UΣ непосредственно изменяет эффективность:

|  |  |
| --- | --- |
|  | (2.9) |

Таким образом, классическая постановка задачи разработки средств защиты для обеспечения максимальной эффективности объекта в условиях несанкционированного доступа имеет вид:

|  |  |
| --- | --- |
|  | (2.10) |

или

|  |  |
| --- | --- |
|  | (2.11) |

Несмотря на кажущуюся простоту классической постановки задачи, на практике воспользоваться приведенными результатами удается редко. Это объясняется отсутствием зависимостей K = f(C) и особенно ущерба от несанкционированного доступа. И если зависимость коэффициента защищенности от стоимости средств защиты можно получить, имея технические и стоимостные характеристики доступных средств защиты, то оценить реальный ущерб от несанкционированного доступа чрезвычайно трудно, так как этот ущерб зависит от множества трудно прогнозируемых факторов: наличия физических каналов несанкционированного доступа, квалификации злоумышленников, их интереса к объекту, последствий несанкционированного доступа и т.д.

Вместе с тем для объектов, на которые возлагаются ответственные задачи и для которых несанкционированный доступ влечет катастрофические потери эффективности их функционирования, влиянием стоимости средств защиты на эффективность можно пренебречь, т.е. если:

|  |  |
| --- | --- |
|  | (2.12) |

то:

|  |  |
| --- | --- |
|  | (2.13) |

В этом случае (2.11) и (2.12) принимают вид:

|  |  |
| --- | --- |
|  | (2.14) |

Или:

|  |  |
| --- | --- |
|  | (2.15) |

где Cдоп — допустимые расходы на защиту.

**Задание на выполнение**

Решить задачу разработки средств защиты для обеспечения максимальной эффективности объекта в условиях несанкционированного доступа в соответствии с вариантом. Вариант 15

**Исходные данные**

Положительный эффект функционирования объекта:

Положительный эффект функционирования объекта с учетом воздействия несанкционированного доступа:

Коэффициент снижения негативного воздействия несанкционированного доступа на эффективность функционирования объекта:

Стоимость средств защиты:

**Решение:**

Определим уменьшение положительного эффекта функционирования объекта, вызванное воздействием несанкционированного доступа в соответствии с вариантом, по формуле (2.1).

Пусть эта величина также представляет собой материальный ущерб, вызванный уменьшением эффективности функционирования объекта, по формуле (2.3):

Определим относительную эффективность функционирования объекта, используя формулу (2.6):

Определим уменьшение положительного эффекта функционирования объекта, вызванное воздействием несанкционированного доступа, при наличии средств защиты, по формуле (2.4):

Определим положительный эффект функционирования объекта с учетом воздействия несанкционированного доступа при наличии средств защиты, используя формулу (2.9):

Определим относительную эффективность функционирования объекта при наличии средств защиты, по формуле (2.2):

Определим суммарный ущерб объекту при наличии средств защиты, формула (2.8):

**Вывод:** в результате выполнения практического занятия №2 я решил задачу разработки средств защиты для обеспечения максимальной эффективности объекта в условиях несанкционированного доступа.

**Практическое занятие №3**

**Тема «Разработка политики информационной безопасности бизнес-компании»**

Учреждение образование

«Белорусский государственный технологический университет»

Кафедра информационных систем и технологий

Разработка политики информационной

безопасности OAO «Полевской молочный комбинат»

Выполнил студент 2 курса 1 группы

Савостин Антон Дмитриевич

Минск 2020

# Введение

В XXI веке – веке информатизации, происходит формирование и развитие информационного общества. Роль информации в современном мире огромна. Информация становится ключевым ресурсом, поэтому без решения задач информационной безопасности не может продолжать работу ни одно из предприятий. В любой организации, как большой, так и маленькой, возникает проблема безопасного хранения, передачи, использования информации.

Обеспечение информационной безопасности автоматизированной системы управления технологическими процессами необходимо для повышения уровня устойчивости ее функционирования, стабильности исполнения реализуемых технологических процессов путем предотвращения и/или снижения возможного ущерба от несанкционированных воздействий на объекты защиты автоматизированной системы управления технологическими процессами.

# 3.1 Общие положения

В данной работе приведены термины и сокращения:

– АРМ – автоматизированное рабочее место;

– АСЗ – антивирусная система защиты;

– АСУ ТП – автоматизированная система управления технологическими процессами;

– ИБ – информационная безопасность;

– ИУС ПХД – информационно-управляющая система производственно-хозяйственной деятельности;

– ЛВС – локальная вычислительная сеть;

– ОС – операционная система;

– ПО – программное обеспечение.

Под автоматизированной системой управления технологическими процессами понимается система, состоящая из персонала и комплекса средств автоматизации его деятельности и формирующая управляющее воздействие на технологические процессы.

Комплекс средств автоматизации включает:

– системы диспетчерского управления (АРМ пользователей и серверы, на которых установлено системное и прикладное ПО, а также набор сетевого оборудования для организации ЛВС и средств ее защиты (средства межсетевого экранирования, средства обнаружения и предотвращения вторжений));

– системы локальной автоматики (системы автоматического управления, концентраторы, контроллеры, пункты управления технологическими объектами, устройства сопряжения с объектами).

Объектами защиты автоматизированной системы управления технологическими процессами являются:

– серверное оборудование (архивные, коммуникационные и другие серверы);

– системы локальной автоматики (системы автоматического управления, концентраторы, контроллеры, пункты управления технологическими объектами);

– АРМ операторов и специалистов;

– сетевое оборудование (коммутаторы, маршрутизаторы, фронтальные процессоры, интегрирующие контроллеры, контроллеры связи с объектами);

– каналы передачи данных;

– ПО;

– технологическая информация (в том числе сигналы, команды управления, данные о параметрах (состоянии) управляемого технологического объекта (процесса)).

# 3.2 Структура предприятия

Для того чтобы разработать план по информационной безопасности OAO «Полевской молочный комбинат» нужно сначала понять, что из себя представляет его структура информации. Информация представляется в бумажном и электронном виде.

Так как в OAO «Полевской молочный комбинат» хранится большая и важная документация, то доступ к информации имеется в зависимости от прав работника. Права работника назначаются в зависимости от должности. Перечень должностей данного предприятия представлен на рисунке 1.1.

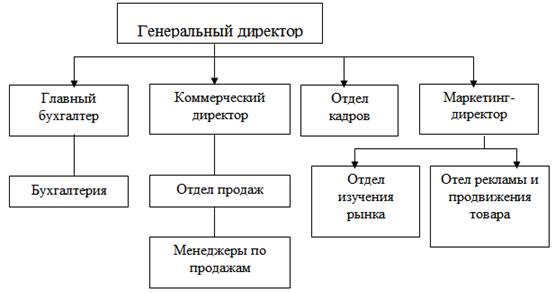


Рисунок 1.1 – Перечень должностей предприятия OAO «Полевской молочный комбинат»

Существуют две группы пользователей, с различным уровнем доступа к информации. Обычные пользователи могут только просматривать информацию, а привилегированные пользователи – администраторы, могут вносить какие-либо изменения, поправки. Так как важность документов очень велика, то доступ ко всей информации не может быть скопирован ни одним из уровней пользования. Такая же система работает как с электронными, так и с бумажными вариантами документации, которая хранится в архиве.

# 3.3 Оценка рисков

Угрозы информационной безопасности могут быть классифицированы по различным признакам:

– по размерам наносимого ущерба:

а) общие (нанесение ущерба объекту безопасности в целом, причинение значительного ущерба);

б) локальные (причинение вреда отдельным частям объекта безопасности);

в) частные (причинение вреда отдельным свойствам элементов объекта безопасности);

– по аспекту информационной безопасности, на который направлены угрозы:

а) угрозы конфиденциальности (неправомерный доступ к информации);

б) угрозы целостности (неправомерное изменение данных);

в) угрозыдоступности (осуществление действий, делающих невозможным или затрудняющих доступ к ресурсам информационной системы);

– по расположению источника угроз:

а) внутренние (источники угроз располагаются внутри системы);

б) внешние (источники угроз находятся вне системы);

– по степени преднамеренности действий:

а) случайные (неумышленные действия, например, сбои в работе систем, стихийные бедствия);

б) преднамеренные (умышленные действия, например, шпионаж и диверсии);

– по степени воздействия на информационную систему:

а) пассивные (структура и содержание системы не изменяются);

б) активные (структура и содержание системы подвергается изменениям).

Основными угрозами ИБ АСУ ТП являются:

– несанкционированное вмешательство в управление технологическими процессами;

– нарушение функционирования АСУ ТП или ее отдельных элементов;

– несанкционированный доступ к информации, хранимой в базах данных АСУ ТП и передаваемой по каналам передачи данных.

В результате реализации угроз ИБ могут быть нарушены:

– целостность (утрата, уничтожение, модификация) информации;

– доступность (блокирование) информации и отдельных элементов АСУ ТП;

– конфиденциальность (утечка, перехват, съем, копирование, хищение, разглашение) информации.

Обеспечение ИБ АСУ ТП осуществляется по следующим направлениям, реализуемым организационно-техническими мерами защиты.

Физическая защита, включая:

– защиту технических средств обработки, хранения и передачи информации;

– защиту зданий, сооружений и помещений.

Обеспечение ИБ при эксплуатации средств обработки, хранения и передачи информации и использовании информационных ресурсов, включая:

– защиту от вредоносного ПО;

– резервирование серверов, сетевого оборудования, средств защиты и каналов передачи данных;

– обеспечение безопасности сетевой инфраструктуры;

– защиту программного обеспечения;

– регистрацию и учет событий ИБ;

– организацию безопасного использования, преобразования, хранения и передачи информации;

– криптографическую защиту.

Контроль доступа, в том числе:

– управление доступом пользователей;

– определение ответственности пользователей;

– контроль доступа к прикладным системам;

– контроль доступа к ОС;

– контроль сетевого доступа;

– обеспечение безопасности при использовании мобильных устройств;

– обеспечение безопасности в беспроводных сетях;

– контроль доступа к сетевому оборудованию.

Реализация организационно-технических мер обеспечения ИБ АСУ ТП достигается в первую очередь путем:

– корректного использования и администрирования встроенных механизмов безопасности технических средств обработки, хранения и передачи информации и средств защиты, входящих в состав АСУ ТП;

– наделения пользователей автоматизированной системы управления технологическими процессами правами доступа и привилегиями по работе в АСУ ТП;

– физической защиты технических средств обработки, хранения и передачи информации от неправомерного доступа к ним;

– контроля функционирования и настроек механизмов безопасности, а также соблюдения требований по ИБ.

Обязанности пользователей АСУ ТП по обеспечению ИБ зависят от занимаемой должности и определены в их должностных инструкциях.

# 3.4 Разработка мер защиты

## 3.4.1 Физическая защита

**3.4**.1.1 Защита технических средств обработки, хранения и передачи информации

В целях защиты информации от несанкционированного доступа и ее утечки, предотвращения хищения технических средств обработки и хранения информации и несанкционированного управления ими, а также простоев в функционировании АСУ ТП обеспечивается физическая защита входящих в нее технических средств. Серверное оборудование и критичное сетевое оборудование размещаются в запираемых шкафах с сигнализацией, располагаемых в специализированных помещениях (серверных), ограничивающих доступ к ним посторонних лиц. Перед утилизацией или передачей в ремонт технических средств выполняется гарантированное удаление информации с них. Кабельные сети прокладываются так, чтобы максимально ограничить несанкционированный доступ к ним. Для защиты от перебоев электричества в эксплуатацию вводятся централизованные системы бесперебойного питания. Система ИБ включает в себя максимальное количество элементов, обеспечивающих эффективную защиту системы при критической нагрузке.

### 3.4.1.2 Защита зданий, сооружений и помещений

В целях обеспечения безопасности технических средств автоматизированной системы управления технологическими процессами осуществляется защита зданий, сооружений и помещений АСУ ТП. Здания и сооружения, в которых размещаются технические средства АСУ ТП, обеспечиваются инженерно-техническими средствами охраны и средствами защиты от противоправных действий. Помещения, в которых размещаются критически важные технические средства АСУ ТП, оборудуются средствами пожарной безопасности, вентиляции и кондиционирования. Доступ в такие помещения разрешается работникам только для выполнения должностных обязанностей по обслуживанию технических средств АСУ ТП. Доступ в помещения ограничивается средствами контроля и управления доступом. При выполнении работ в помещениях, где размещаются критически важные технические средства автоматизированной системы управления технологическими процессами, лицами, чья деятельность не связана непосредственно с их обслуживанием, обеспечивается контроль их деятельности.

## 3.4.2 Обеспечение информационной безопасности при эксплуатации средств обработки, хранения и передачи информации и использовании информационных ресурсов

### 3.4.2.1 Организация безопасной эксплуатации средств обработки, хранения и передачи информации

Функции по администрированию и контролю эксплуатации средств обработки, хранения и передачи информации разделяются и возлагаются на специально выделенных для этого работников. Изменения конфигурации средств обработки и хранения информации, а также изменения сетевой инфраструктуры, конфигурации сетевого оборудования выполняются администратором. Все изменения регистрируются в соответствующих журналах. Самостоятельное изменение конфигурации средств обработки, хранения и передачи информации пользователями АСУ ТП запрещено. Использование съемных носителей информации в автоматизированной системе управления технологическими процессами запрещено. При размещении средств разработки, тестирования и эксплуатации обеспечивается их физическое или логическое разделение в целях снижения риска несанкционированного доступа или внесения изменений в систему.

### 3.4.2.2 Защита от вредоносного программного обеспечения

В целях предотвращения проникновения, обнаружения внедрения и нейтрализации вредоносного ПО в АСУ ТП применяются средства защиты от вредоносного ПО. Средства защиты от вредоносного ПО устанавливаются на серверном оборудовании и АРМ операторов и специалистов автоматизированной системы управления технологическими процессами. Управление и обновление средств защиты от вредоносного ПО осуществляются централизованно. Разрешается использование только сертифицированных на соответствие требованиям безопасности информации средств защиты от вредоносного ПО. Администрирование средств защиты от вредоносного ПО осуществляется системным администратором. Настройки системы защиты от вредоносного ПО согласовываются и контролируются администратором ИБ.

Используемая антивирусная система защиты имеет:

– стойкую систему самозащиты, которая не по­зволит неизвестной вредоносной программе нарушить нормальную работу АСУ ТП и сделает возможным функционирование АСЗ до поступления обновления;

– систему обновлений, находящуюся под контролем системы самозащиты антивирусной системы и не использующую компоненты операционной системы, которые могут быть скомпрометированы;

– систе­му обновления, позволяющую мгновенно, по сигна­лу системы централизованного управления доставить на защищаемый антивирусом объект обновления для устранения активного заражения;

– дополнительные механизмы для обнаружения новых неизвестных вредоносных программ;

– проверяет все поступающие из локальной сети файлы до момента получения их используемыми приложениями, что исключает использование вредоносными приложениями неизвестных уязвимостей данных приложений;

– систему централизованного сбора информации с удаленных рабочих станций и серверов, позволяющую максимально быстро передавать в антиви­русную лабораторию всю необходимую для решения проблемы информацию.

### 3.4.2.3 Обеспечение безопасности сетевой инфраструктуры

Для обеспечения непрерывного и устойчивого функционирования АСУ ТП осуществляется защита ее сетевой инфраструктуры. Защита сетевой инфраструктуры обеспечивается:

– контролем логического доступа к сетевому оборудованию;

– контролем сетевых соединений;

– шифрованием каналов управления;

– защитой информации ограниченного доступа при ее передаче вне контролируемых зон;

– физической защитой сетевого оборудования и средств защиты;

– мониторингом подключаемых к ЛВС автоматизированной системы управления технологическими процессами сетевых устройств;

– обнаружением и предотвращением вторжений;

– использованием встроенных в сетевое оборудование средств защиты от подмены адреса (средств антиспуфинга);

– применением средств мониторинга и регистрации событий.

Контроль сетевых соединений между ЛВС АСУ ТП и подключаемыми к ней беспроводными сетями также осуществляется средствами межсетевого экранирования. Защита информации ограниченного доступа при ее передаче вне контролируемых зон осуществляется применением сертифицированных средств криптографической защиты информации (построением защищенных виртуальных сетей). Защита от вторжений в ЛВС АСУ ТП осуществляется средствами обнаружения и предотвращения вторжений, размещаемыми на входе в ЛВС. Базы данных сигнатур средств обнаружения и предотвращения вторжений регулярно обновляются с сайта производителя применяемых средств. Категорически запрещается удаленное администрирование АСУ ТП.

В целях поддержания работоспособности ПО осуществляются меры по устранению уязвимостей ПО, а также другие меры защиты от:

– умышленного либо неумышленного раскрытия, модификации или уничтожения защищаемых данных. В частности, это подразумевает использования средств ограничения доступа к различным ресурсам офисного контроля;

– установки средств защиты кем-либо, кроме администратора, несанкционированного внесения изменений в порядок функционирования системы защиты, изменения ее возможностей. Данное требование приводит к необходимости разграничения прав доступа к настройкам системы, защите ее от несанкци­онированного воздействия. Это подразумевает использование в локальной сети только программных продуктов, поддерживающих ролевой принцип доступа, а также применение функций офисного контроля. Средства защиты должны устанавливаться как на рабочие станции, так и на сервер. В организации, соответствующей требованиям стандарта, должна использо­ваться только защищенная почта, что вместе с требованием о наличии защиты от вирусов и спама подразумевает установку средств антивирусной фильтрации почтовых сообщений. В свою очередь доступ в сеть Интернет должен использоваться только для обеспе­чения банковской деятельности. Устранение уязвимостей ПО достигается регулярным централизованным получением и установкой обновлений, предоставляемых разработчиками ПО. Обновление ОС, другого общесистемного и прикладного ПО осуществляется системными администраторами и администраторами прикладных систем. Обновления для ПО АСУ ТП получаются с серверов обновлений, размещенных в ИУС ПХД.

### 3.4.2.5 Криптографическая защита

В целях обеспечения конфиденциальности информации при ее передаче вне контролируемых зон применяются сертифицированные установленным порядком средства криптографической защиты информации. Это специальные методы шифрования, кодирования в результате которых содержание передаваемых файлов становится недоступным, без предъявления ключа криптограммы и обратного преобразования. Криптографическая защита информации на предприятии реализована с помощью метода криптосистемы с открытым ключом. В системе с открытым ключом используются два ключа — открытый и закрытый, которые математически связаны друг с другом. Информация шифруется с помощью открытого ключа, который доступен всем желающим, а расшифровывается с помощью закрытого ключа, известного только получателю сообщения.

## 3.4.3 Контроль доступа

### 3.4.3.1 Управление доступом пользователей

В целях устойчивого функционирования АСУ ТП и обеспечения безопасности информационных ресурсов осуществляется управление доступом пользователей к операционным и прикладным системам, а также сетевому оборудованию. Пользователи наделяются минимальными правами доступа и привилегиями, необходимыми им для выполнения служебных задач. Наделение пользователей правами доступа и привилегиями основывается на установленной в ОАО формализованной процедуре предоставления прав доступа. Права доступа и привилегии пользователей подлежат регулярному пересмотру. Каждый пользователь обеспечивается уникальным персональным идентификатором. Подтверждение подлинности идентификатора (аутентификация) пользователя осуществляется при помощи паролей и/или средств усиленной аутентификации. Длина, сложность и срок действия паролей устанавливаются в зависимости от степени критичности защищаемых систем.

# Заключение

Политика безопасности — совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов. Основная цель политики безопасности – определение технических требований к защите компьютерных систем и сетевой аппаратуры, способы настройки систем администратором с точки зрения их безопасности.

На политике безопасности нельзя экономить, так как данные, которые могут быть подвержены хищению, копированию или изменению, могут стоить дороже, чем ресурсы, потраченные на ее разработку и осуществление.

Разработаны технические меры обеспечения безопасности, организационные меры обеспечения безопасности, сетевая безопасность и общие меры предосторожностей.

Политика безопасности должна быть разработана таким образом, чтобы ее несанкционированный доступ к информации стоил дороже, чем сама информация.

**Практическое занятие №4**

**Тема «Настройка Брандмауэра Windows»**

Цель: Овладение навыками настройки и использования Брандмауэра Windows.

**Теоретическое введение**

Брандмауэр (Межсетевой экран) – это аппаратный или программный комплекс, позволяющий проверять (фильтровать) входные и выходные потоки данных, проходящие через интернет или сеть. В случаи нарушения политики безопасности компьютера, брандмауэр блокирует эти данные.

Межсетевой экран является одним из основных компонентов защиты сетей. Наряду с Internet-протоколом межсетевого обмена (Internet Security Protocol –IPSec). Межсетевой экран является одним из важнейших средств защиты, осуществляя надежную аутентификацию пользователей и защиту от несанкционированного доступа. Отметим, что большая часть проблем с информационной безопасностью сетей связана с "прародительской" зависимостью коммуникационных решений от ОС UNIX – особенности открытой платформы и среды программирования UNIX сказались на реализации протоколов обмена данными и политики информационной безопасности. Вследствие этого ряд Internet-служб и совокупность сетевых протоколов (Transmission Control Protocol/Internet Protocol – TCP/IP) имеет "бреши" в защите.

К числу таких служб и протоколов относятся:

* служба сетевых имен (Domain Name Server – DNS);
* доступ к всемирной паутине WWW;
* программа электронной почты Send Mail;
* служба эмуляции удаленного терминала Telnet;
* простой протокол передачи электронной почты (Simple Mail Transfer Protocol – SMTP);
* протокол передачи файлов (File Transfer Protocol);
* графическая оконная система X Windows.

Настройки межсетевого экрана, т.е. решение пропускать или отсеивать пакеты информации, зависят от топологии распределенной сети и принятой политики информационной безопасности. В связи с этим политика реализации межсетевых экранов определяет правила доступа к ресурсам внутренней сети. Эти правила базируются на двух общих принципах ­­­­­­– запрещать всё, что не разрешено в явной форме, и разрешать всё, что не запрещено в явной форме. Использование первого принципа дает меньше возможностей пользователям и охватывает жёстко очерченную область сетевого взаимодействия. Политика, основанная на втором принципе, является более мягкой, но во многих случаях она менее желательна, так как она предоставляет пользователям больше возможностей "обойти" межсетевой экран и использовать запрещенные сервисы через нестандартные порты (User Data Protocol – UDP), которые не запрещены политикой безопасности.

**Задания для самостоятельной работы**

Для 1 программы на блокировку подключения для входящих подключений:

Первым этапом (рис 4.1) необходимо включить брандмауэр, в случае, если он был ранее выключен.

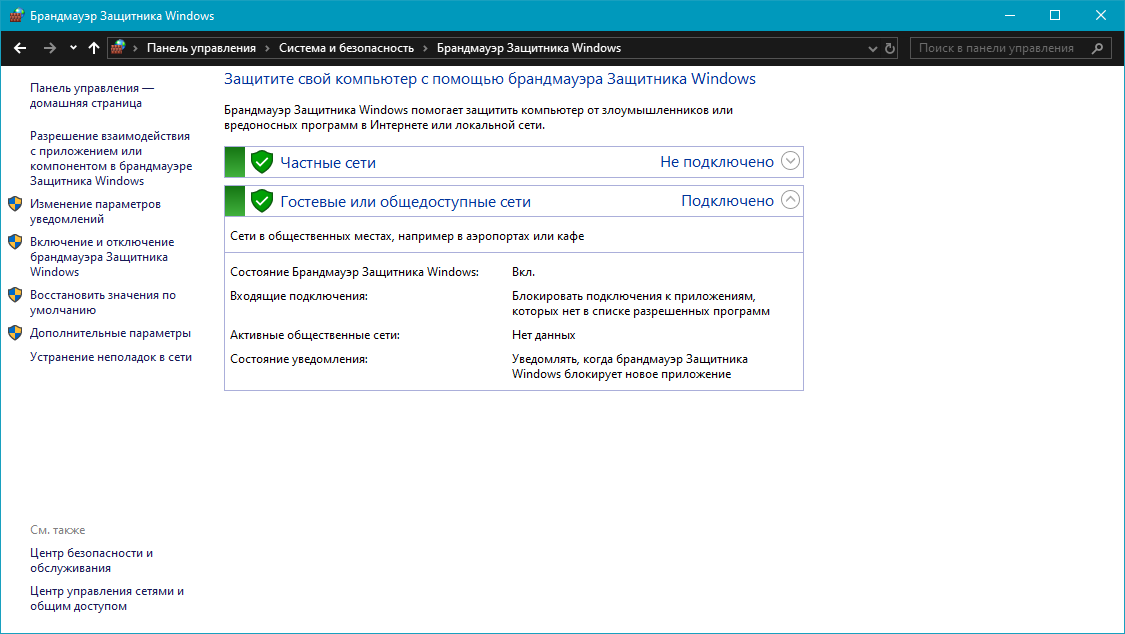


Рисунок 4.1 – Главное окно

В открывшемся окне (рис. 4.2) выбираем в левой панели правила для входящих подключений, затем во вкладке меню «Действие» выбираем «Создать правило», либо нажимаем «Создать правило» в правой панели.

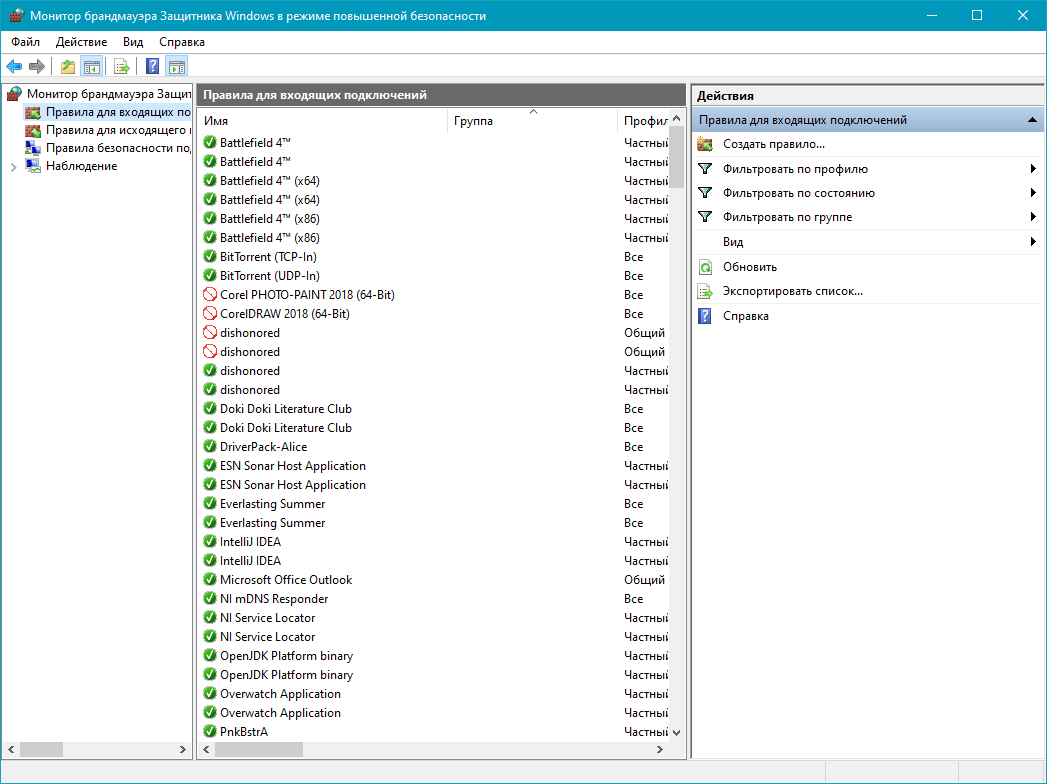


Рисунок 4.2 – Правила для входящих подключений

В открывшемся мастере создания (рис. 4.3) правила выбираем «Для программы», в случае если необходимо перекрыть доступ к сети конкретной программе, либо «Для порта» (например, если есть необходимость отключить часть возможностей программы).

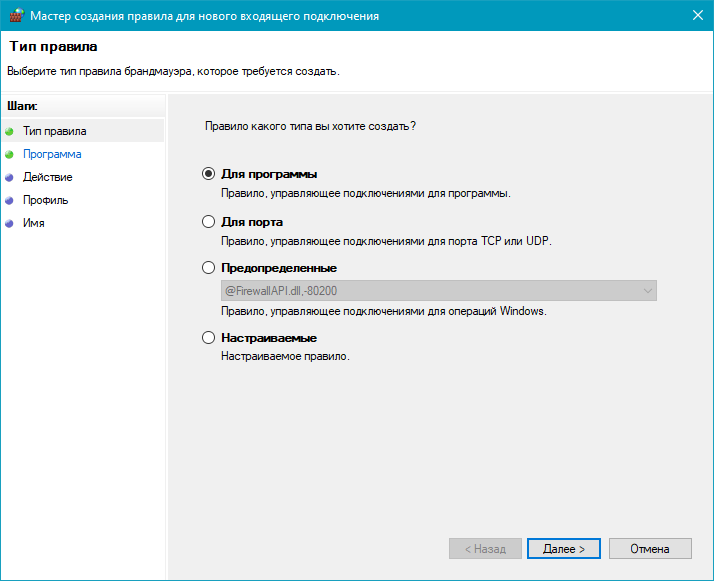


Рисунок 4.3 – Тип правила

При ограничении работы программы далее необходимо указать ее путь. (рис. 4.4).

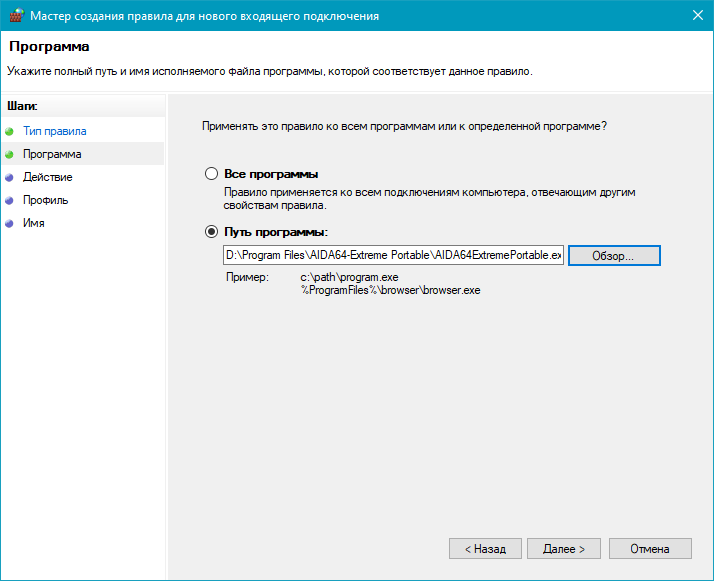


Рисунок 4.4 – Программы

Далее указывается какое именно действие вы хотите применить. В данном случае (рис. 4.5) необходимо блокировать подключение.

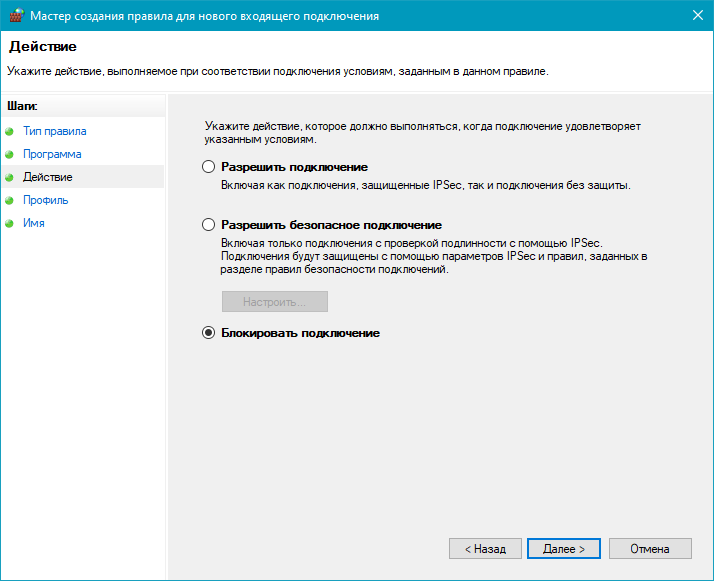


Рисунок 4.5 – Действие

Далее указывается профиль правила (рис. 4.6).

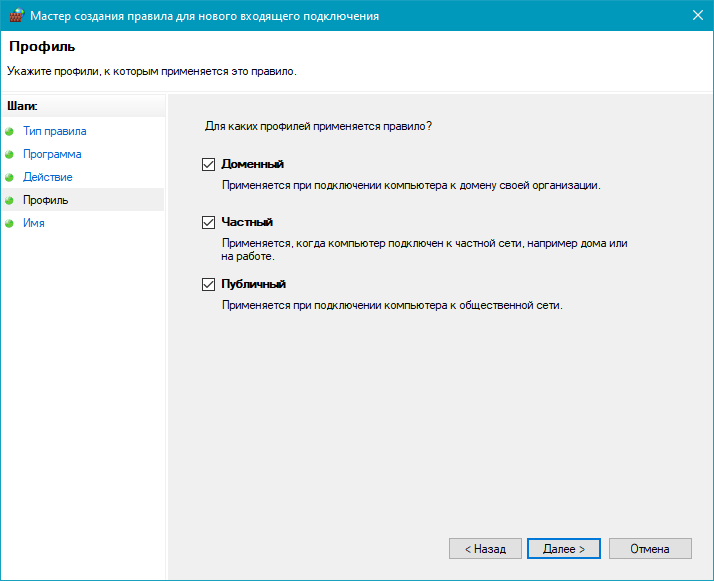


Рисунок 4.6 – Профиль

В следующем окне (рис. 4.7) указывается имя правила.

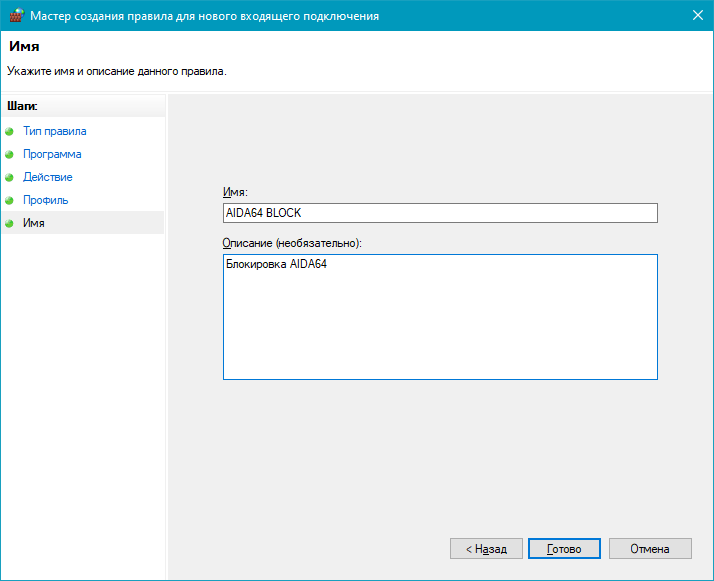


Рисунок 4.7 – Имя

В общем списке (рис. 4.8) появилось созданное правило. Правила можно отключать, копировать, удалять с помощью кнопок на правой панели.

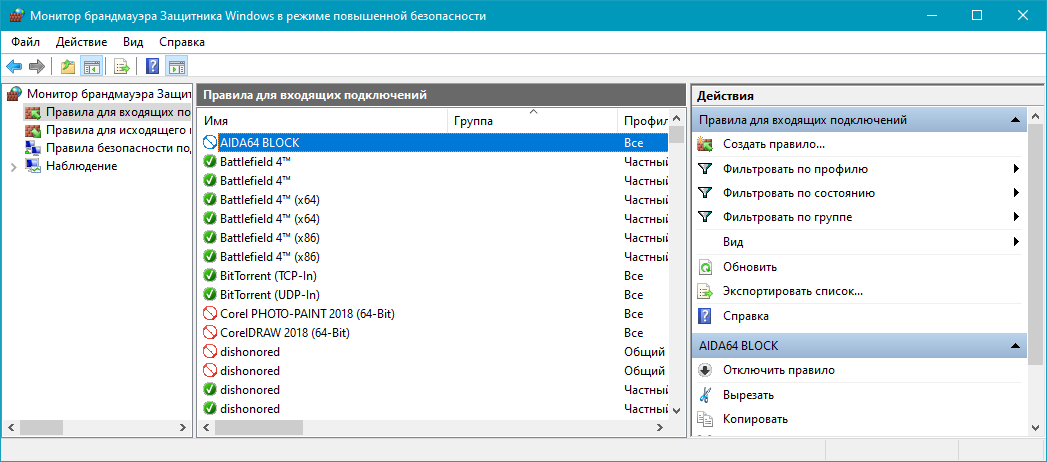


Рисунок 4.8 – Правила для входящих подключений

Для 1 программы (по выбору) на разрешение подключения (рис. 4.9):

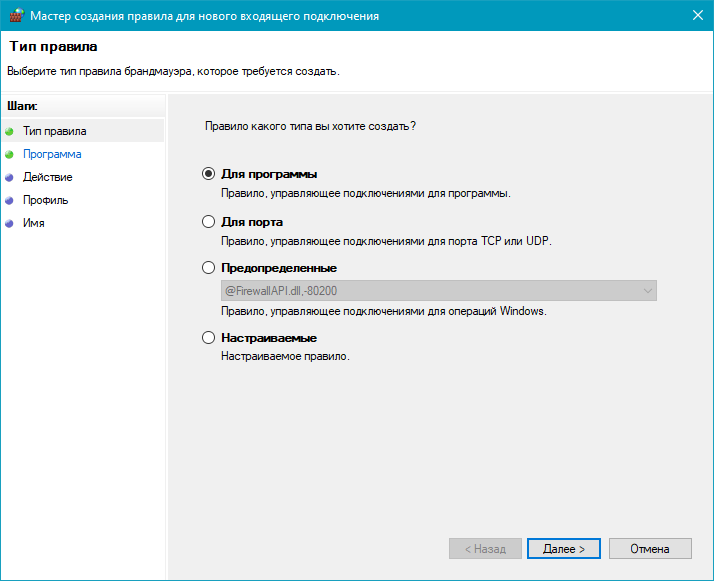


Рисунок 4.9 – Тип правила

При ограничении работы программы далее необходимо указать ее путь.

(рис. 4.10):

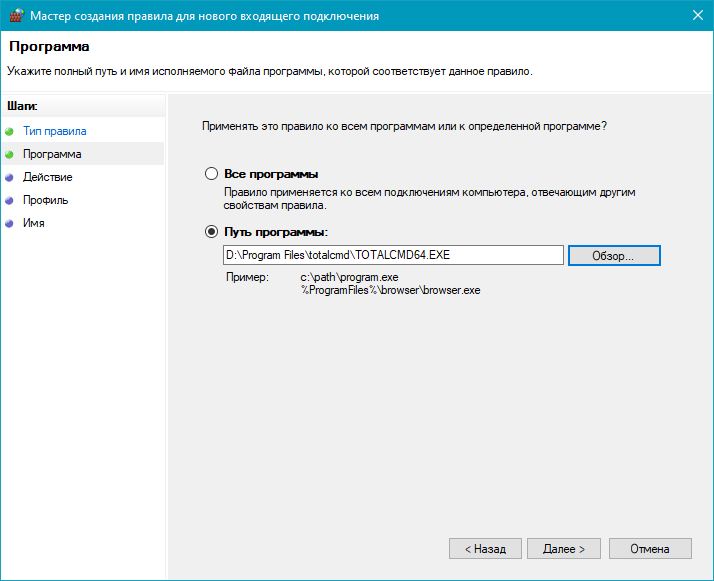


Рисунок 4.10 – Программа

Далее указывается какое именно действие вы хотите применить. В данном случае (рис. 4.11) необходимо разрешить подключение.

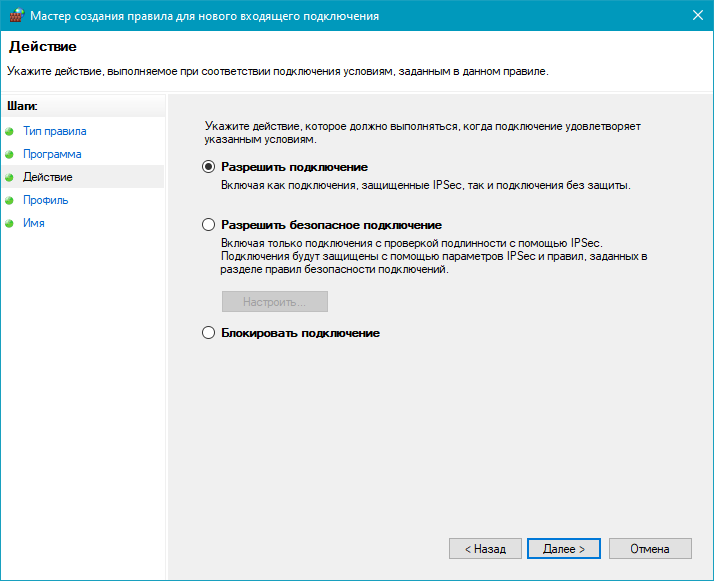
- 

Рисунок 4.11 – Действие

Далее указывается профиль правила (рис. 4.12).

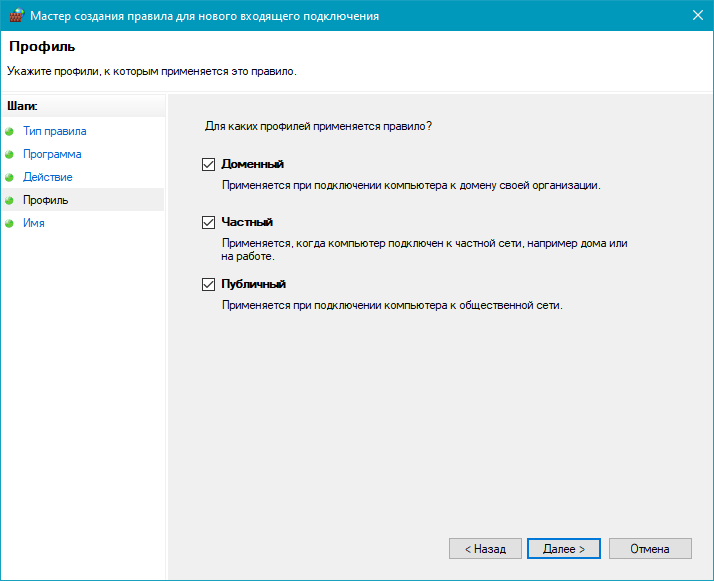
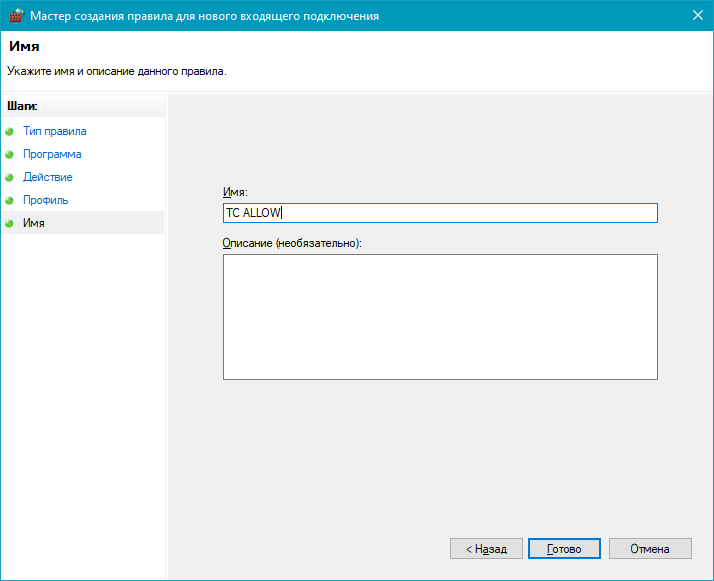


Рисунок 4.12 – Профиль

В следующем окне (рис. 4.13) указывается имя правила.

 Рисунок 4.13 – Имя

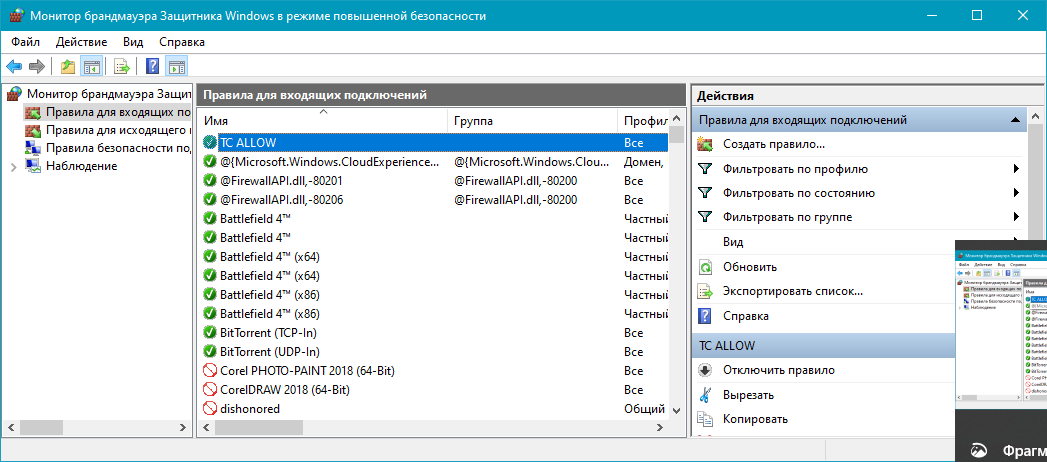
В общем списке (рис. 4.14) появилось созданное правило. Правила можно отключать, копировать, удалять с помощью кнопок на правой панели. 

Рисунок 4.14 – Правила для входящих подключений

Для 1 программы (по выбору) на блокировку подключения:

Переходим на вкладку “правила для исходящих подключений” (рис. 4.15) и выбираем “Действие ­– Создать правило…”.

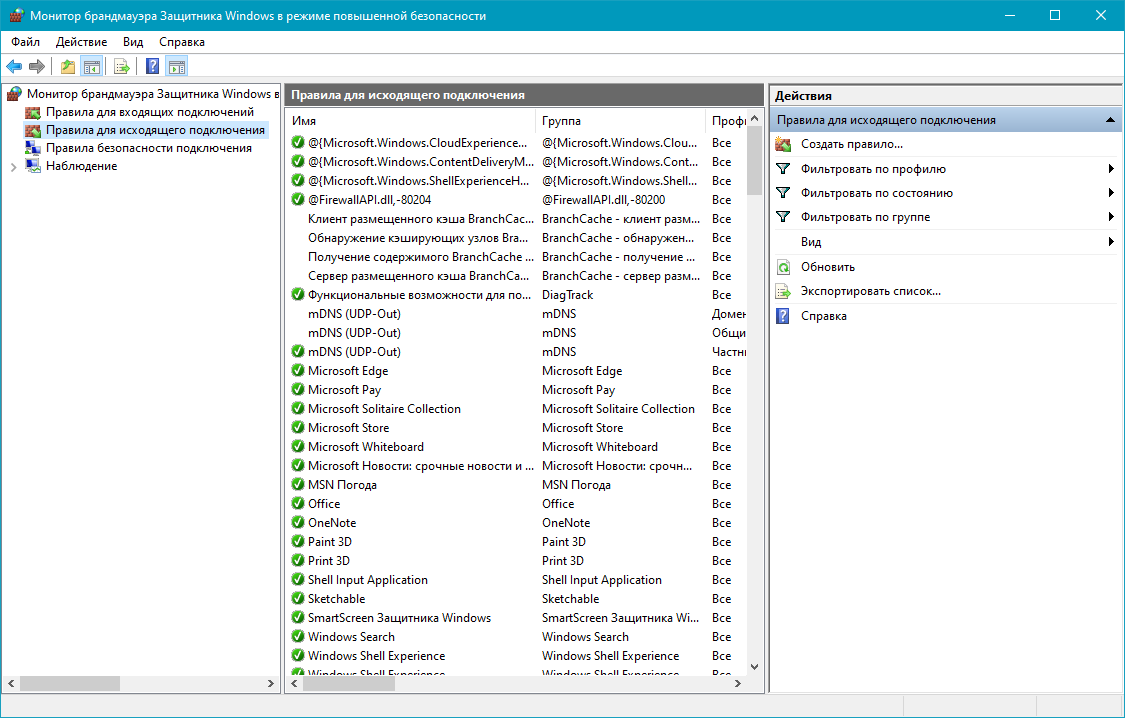


Рисунок 4.15 – Правила для исходящих подключений

В открывшемся мастере создания (рис. 4.16) правила выбираем «Для программы», в случае если необходимо перекрыть доступ к сети конкретной программе, либо «Для порта» (например, если есть необходимость отключить часть возможностей программы).

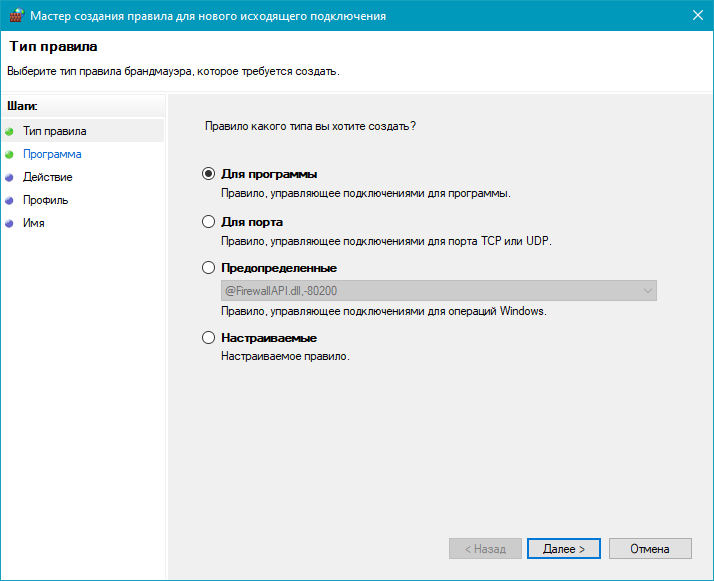


Рисунок 4.16 – Тип правила

При ограничении работы программы далее необходимо указать ее путь. (рис. 4.17).

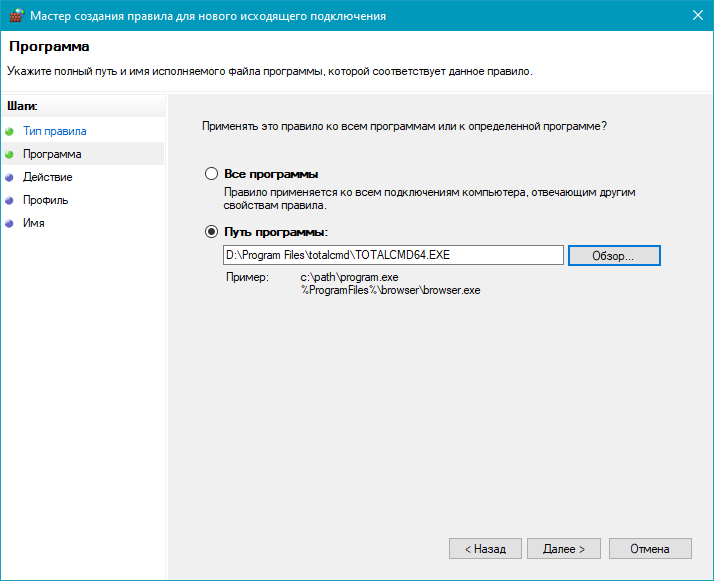


Рисунок 4.17 – Программы

Далее указывается какое именно действие вы хотите применить. В данном случае (рис. 4.18) необходимо блокировать подключение.

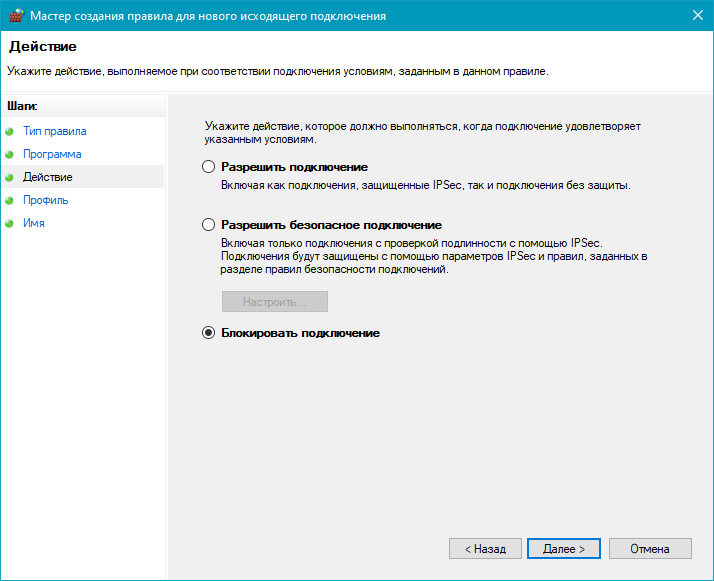


Рисунок 4.18 – Действие

Далее указывается профиль правила (рис. 4.19).

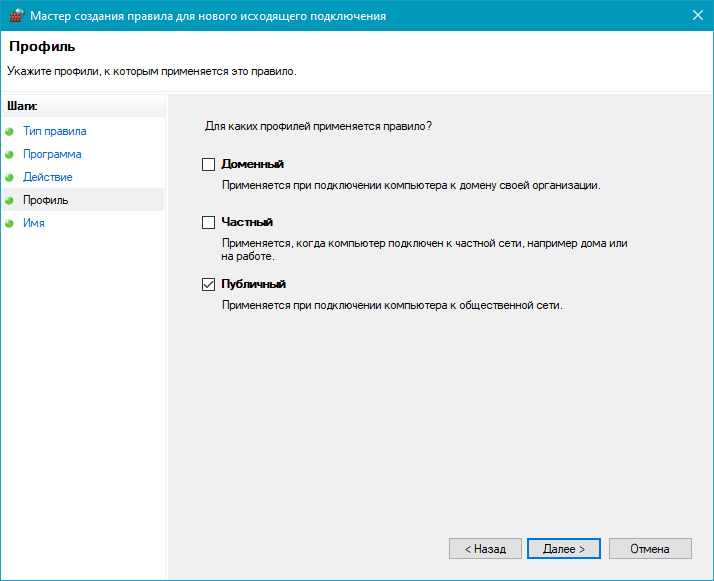


Рисунок 4.19 – Профиль

В следующем окне (рис. 4.20) указывается имя правила.

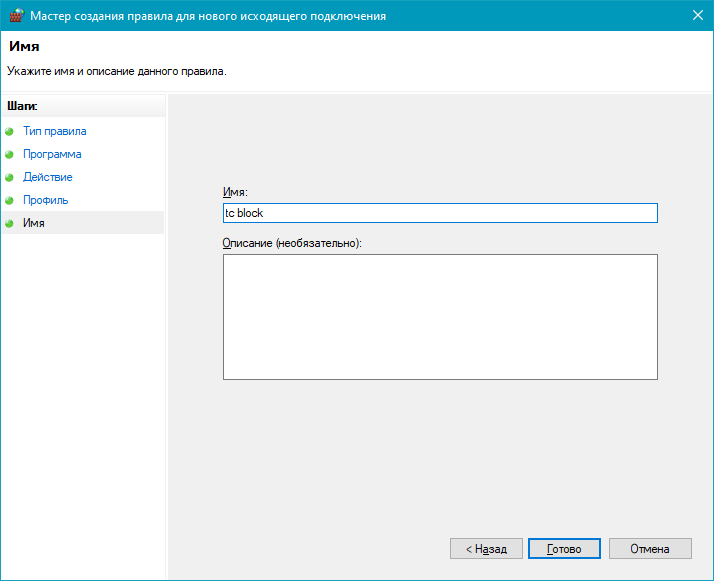


Рисунок 4.20 – Имя

В общем списке (рис. 4.21) появилось созданное правило. Правила можно отключать, копировать, удалять с помощью кнопок на правой панели.

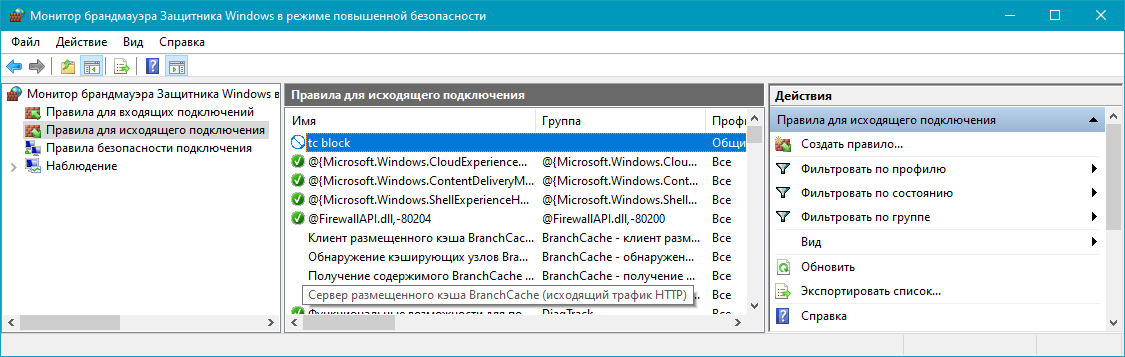


Рисунок 4.21 – Правила для исходящих подключений

Для 1 программы (по выбору) на разрешение подключения (рис. 4.22):

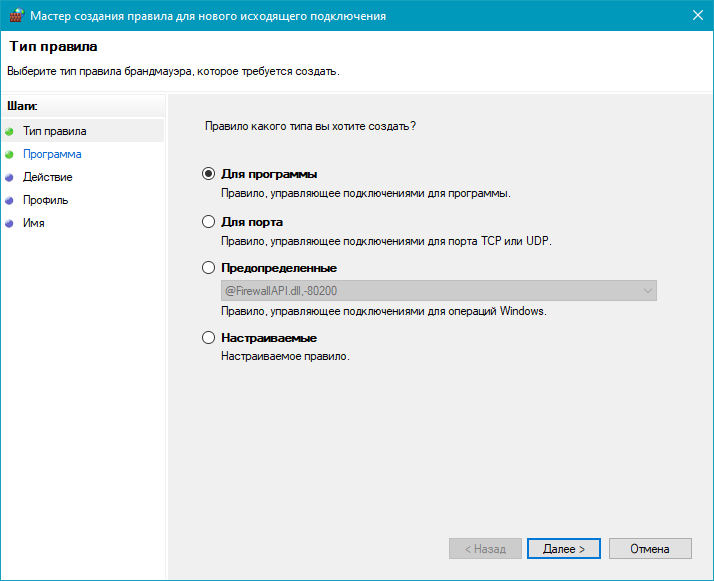


Рисунок 4.22 – Тип правила

При ограничении работы программы далее необходимо указать ее путь.

(рис. 4.23):

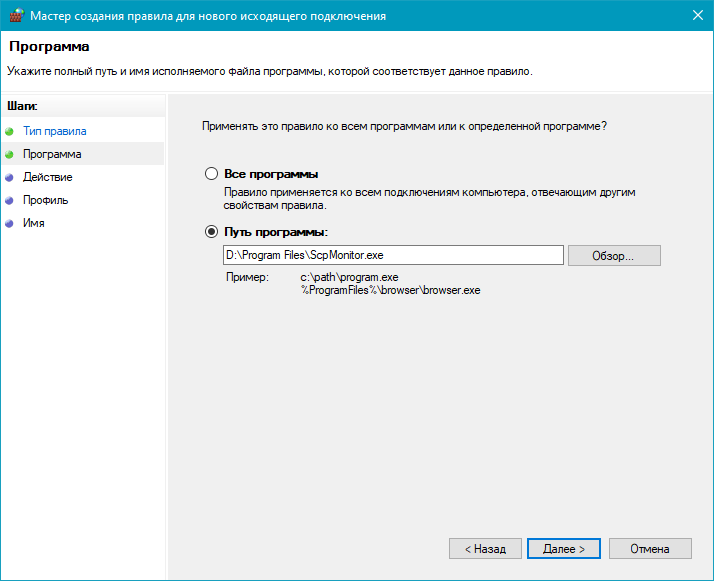


Рисунок 4.23 – Программа

Далее указывается какое именно действие вы хотите применить. В данном случае (рис. 4.24) необходимо разрешить подключение.

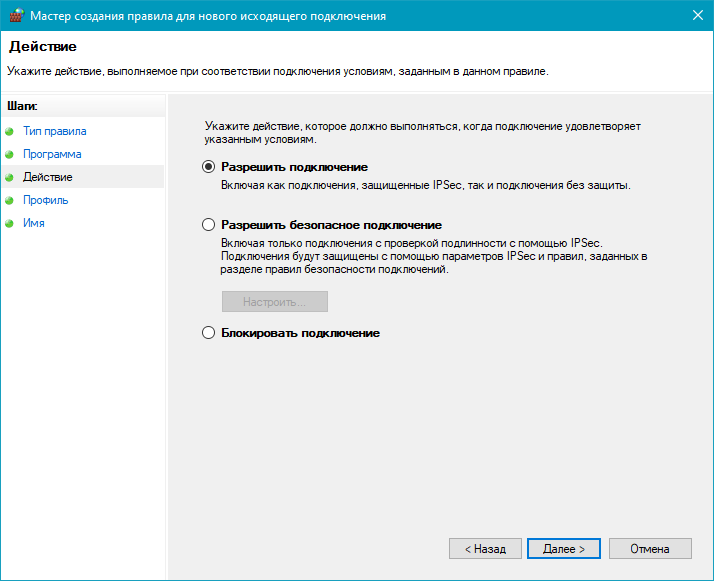
- 

Рисунок 4.24 – Действие

Далее указывается профиль правила (рис. 4.25).

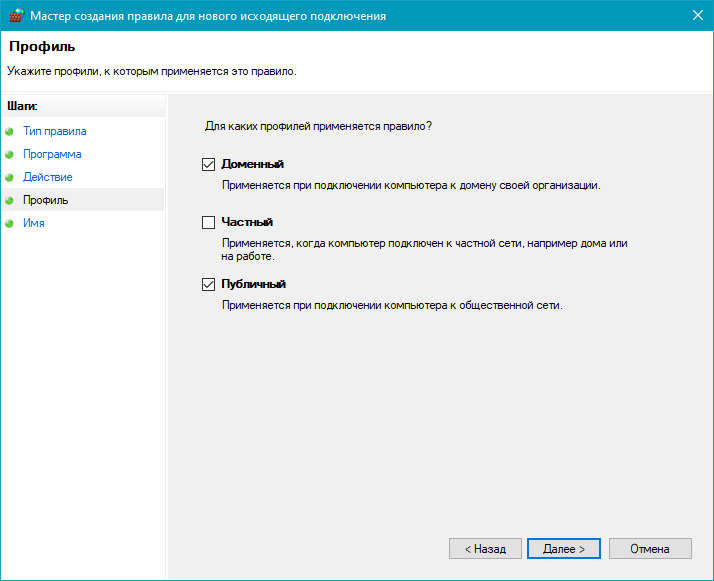
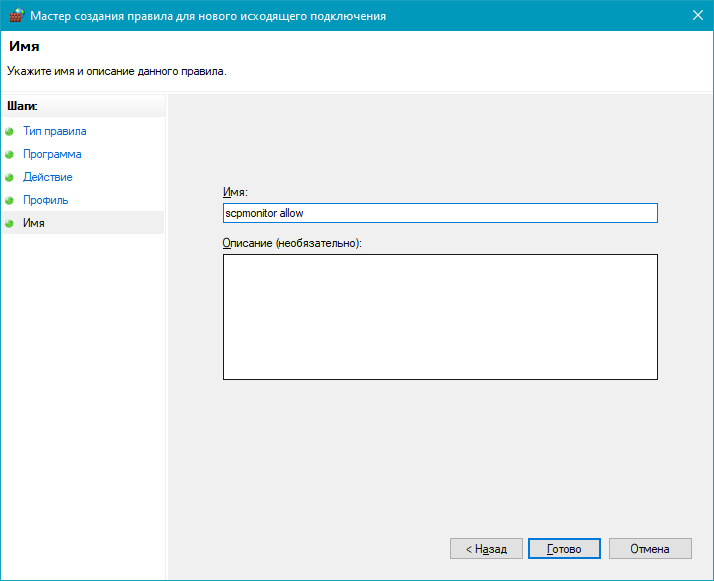


Рисунок 4.25 – Профиль

В следующем окне (рис. 4.26) указывается имя правила.

 Рисунок 4.26 – Имя

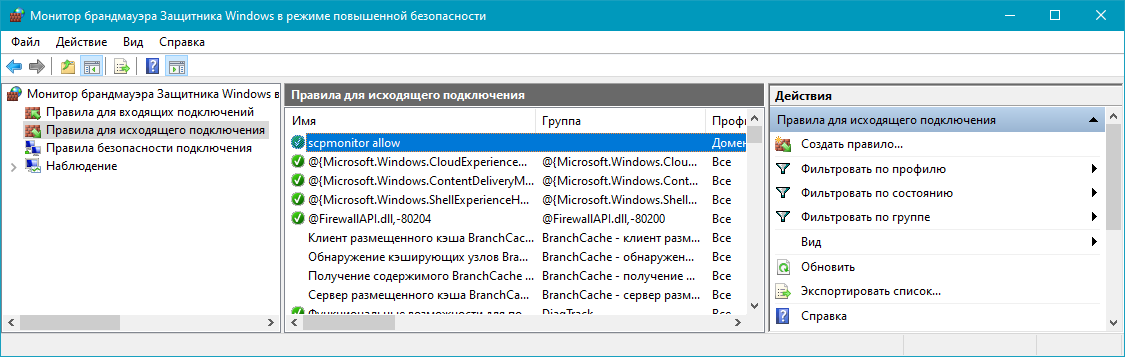
В общем списке (рис. 4.27) появилось созданное правило. Правила можно отключать, копировать, удалять с помощью кнопок на правой панели. 

Рисунок 4.27 – Правила для исходящих подключений

Опробовать действие нескольких команд (с помещением в электронный конспект копий экрана с пояснениями действий):

Открываем интерпретатор командной строки (рис. 4.28):

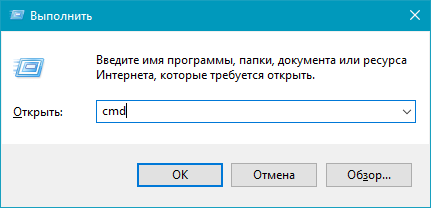


Рисунок 4.28 – Вызов командной строки

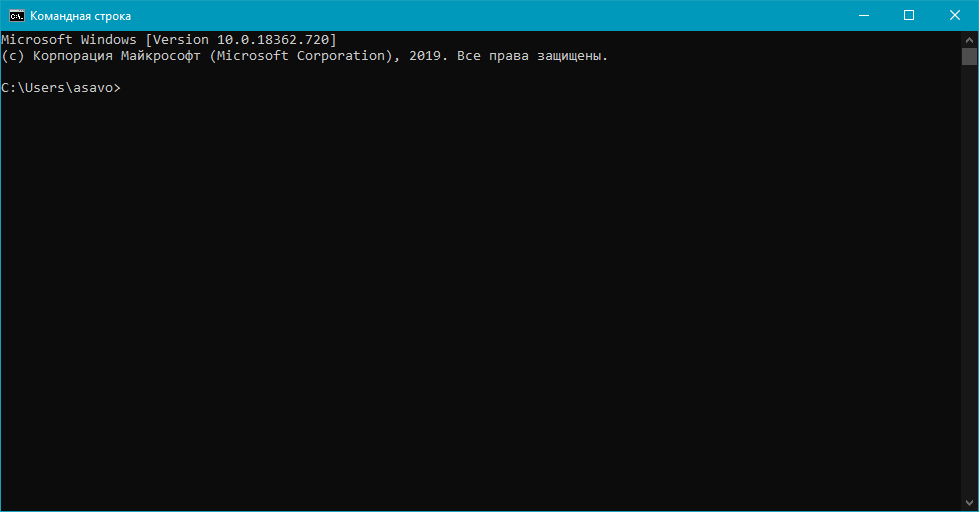


Рисунок 4.29 – ­­­Командная строка

Вызываем меню “Службы” (рис. 4.30)

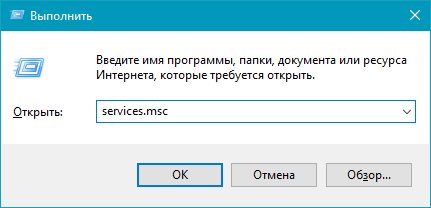


Рисунок 4.30 – Вызов меню “Службы”

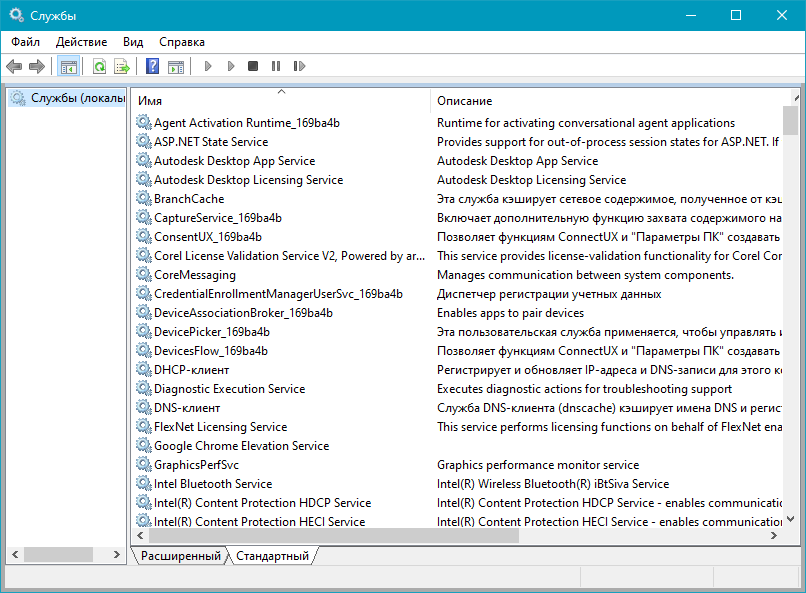


Рисунок 4.31 – Меню “Службы”

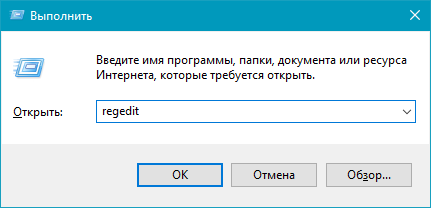
Вызываем редактор реестра (рис. 4.32): 

Рисунок 4.32 – Вызов редактора реестра

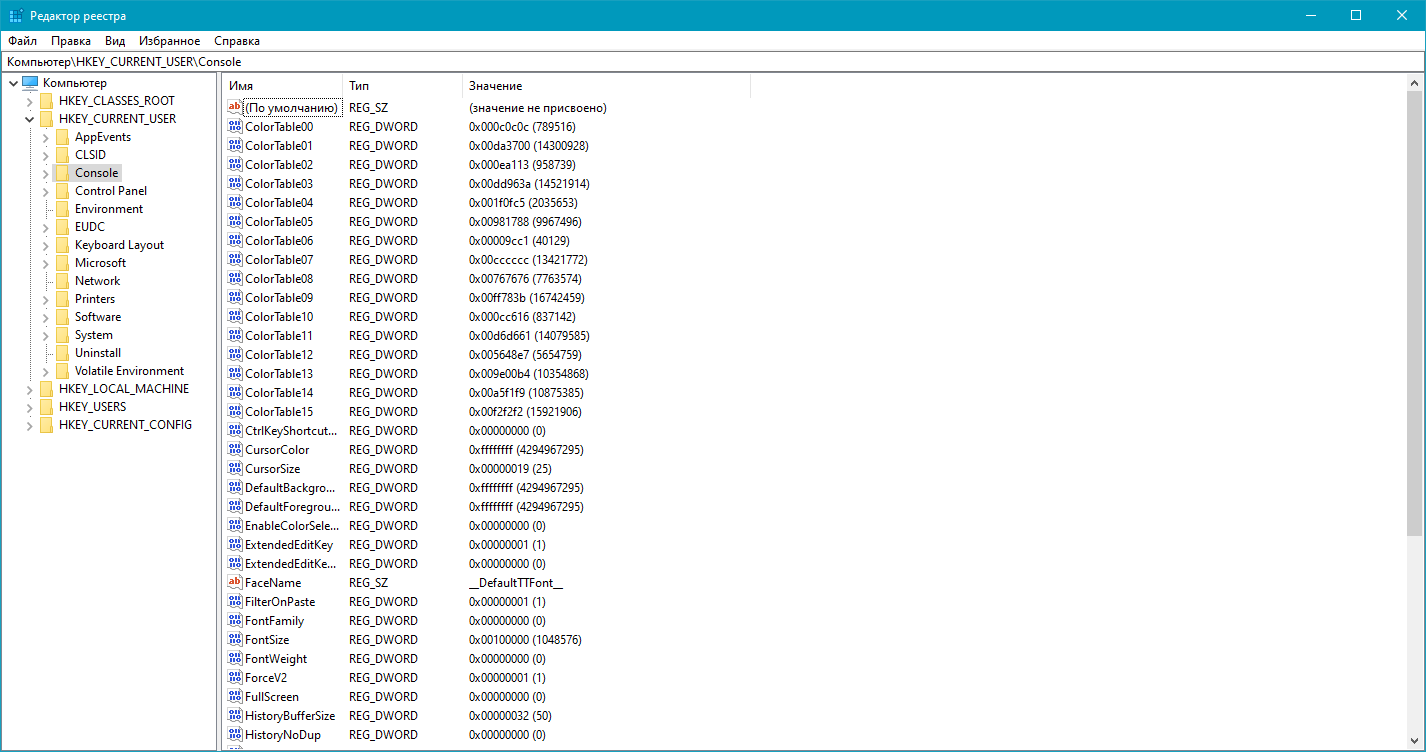


Рисунок 4.33 – Редактор реестра

**Вывод**

Я овладел навыками настройки и использования Брандмауэра Windows. Создал правила для входящих и исходящих подключений на разрешение и блокировку подключения. Протестировал несколько команд администрирования.

**Практическое занятие №5**

**Тема «**Настройка антивирусов**»**

Цель: Овладение навыками настройки и использования различных антивирусов.

**Теоретическое введение**

**Признаки заражения компьютера вредоносными программами.**

При заражении компьютера вредоносными программами важно их обнаружить. Для этого следует знать об основных признаках проявления вредоносных программ. К ним можно отнести следующие:

* прекращение работы или неправильная работа ранее успешно функционировавших программ;
* медленная работа компьютера;
* невозможность загрузки операционной системы;
* исчезновение файлов и каталогов или искажение их содержимого;
* изменение даты и времени модификации файлов;
* изменение размеров файлов;
* неожиданное значительное увеличение количества файлов на диске;
* существенное уменьшение размера свободной оперативной памяти;
* вывод на экран непредусмотренных сообщений или изображений;
* подача непредусмотренных звуковых сигналов;
* частые зависания и сбои в работе компьютера.

**Режимы работы файервола ESET NOD32 Smart Security и взаимодействие с пользователем**

Персональный файервол – это устройство, выполняющее функции драйвера сетевого трафика и управляющее взаимодействием в рамках локальной сети или Интернета. При помощи заранее определенных правил файервол анализирует это взаимодействие и принимает решение о его разрешении или запрете. Самая основная функция файервола – защита частных сетей или компьютеров от вторжения со стороны потенциально опасных внешних сетей и компьютеров.

Доступны 5 отдельных режимов работы файервола, выбор которых зависит от требуемого уровня ограничений. Чтобы изменить поведение файервола, необходимо выбрать нужный режим фильтрации. Для изменения режима фильтрации нужно выполнить следующие действия:

1. Открыть программу ESET NOD32 Smart Security, щелкнув по значку программы в области уведомлений Windows или выбрав команды Пуск - Все программы - ESET- ESET NOD32 Smart Security.

2. Открыть дополнительные настройки, нажав клавишу F5 на клавиатуре – Персональный файервол. Откроется окно расширенной настройки. В расположенном справа раскрывающемся меню **Режим фильтрации**(рис.5.1) выбрать нужный режим фильтрации и нажать кнопку **OK**.

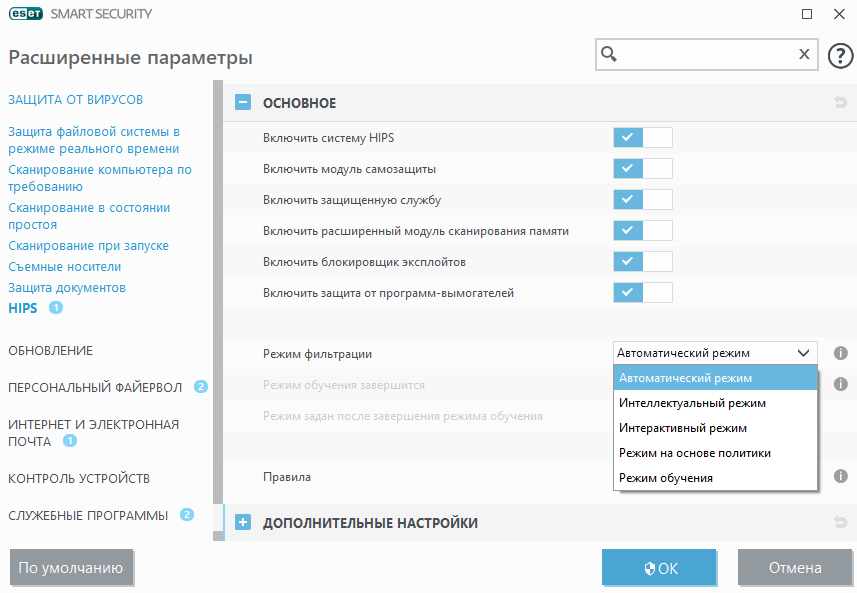


Рисунок 5.1 – Режим фильтрации

Самая основная функция файервола – защита частных сетей или компьютеров от вторжения со стороны потенциально опасных внешних сетей и компьютеров.

**Автоматический режим**

В автоматическом режиме сетевое взаимодействие автоматически контролируется параметрами, определенными пользователем. После подключения к сети пользователь решает, следует ли считать ее доверенной зоной. Взаимодействие в доверенной зоне не ограничивается в обоих направлениях. Взаимодействие в зоне ограничений: взаимодействие с Интернетом – разрешается только приложениям, устанавливающим исходящие подключения. Такие приложения считаются доверенными и для входящих подключений. Данный режим не требует участия пользователя (за исключением момента подключения к новой сети).

В общем, автоматический режим не использует заранее определенные правила, но при этом автоматически анализирует взаимодействие. Приложениям разрешается устанавливать исходящие подключения. Приложения, уже установившие исходящие подключения, считаются доверенными и для установки входящих подключений.

**Интерактивный режим**

В интерактивном режиме сетевое взаимодействие анализируется в соответствии с заранее определенными правилами. Если для подключения нет доступных правил, пользователю при помощи диалогового окна предлагается разрешить или запретить подключение. Через некоторое время пользователем будет создана группа правил, соответствующая его потребностям. Будьте осторожны, устанавливая этот режим в корпоративной среде, поскольку со временем некоторые пользователи могут начать игнорировать регулярно появляющиеся диалоговые окна и просто разрешать все, что предлагает им программа.

**Режим на основе политик**

В режиме на основе политик сетевое взаимодействие анализируется в соответствии с правилами, определенными администратором. Если доступных правил нет, подключение автоматически блокируется без уведомления пользователя. Данный режим рекомендуется выбирать только администраторам, желающим контролировать сетевое взаимодействие и знающим, каким приложениям следует его разрешить или запретить.

**Режим обучения**

Автоматическое создание и сохранение правил, предназначен для первоначальной настройки персонального брандмауэра. Участие пользователя не требуется, потому что **ESET Smart Security** сохраняет правила согласно предварительно настроенным параметрам. Режим обучения является небезопасным, поэтому рекомендуется использовать его только до момента создания правил для всех необходимых соединений.

**Задание к выполнению**

**1. Настройка режима фильтрации файервола антивируса.**

Открыть программу ESET NOD32 Smart Security, щелкнув по значку программы в области уведомлений Windows или выбрав команды Пуск - Все программы - ESET- ESET NOD32 Smart Security.

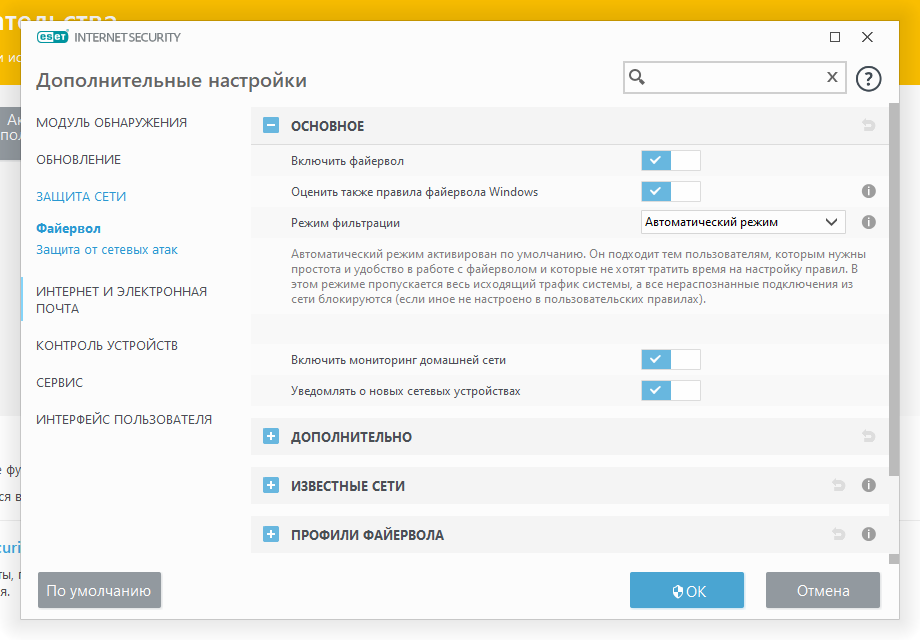


Рисунок 5.2 – Настройка файервола Eset Smart Security.

C помощью клавиши F5 заходим в расширенные параметры антивируса и выбираем пункт меню «Защита сети – Персональный файервол» (рис. 5.1). Затем в разделе режим фильтрации выбираем нужный режим. (рис. 5.2).

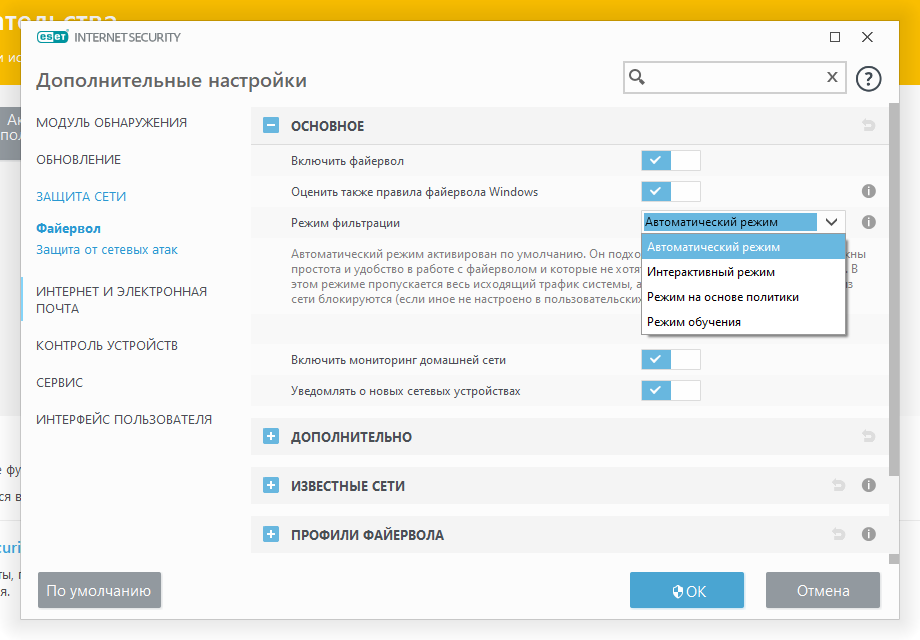


Рисунок 5.3 – Выбор режима фильтрации.

Существуют следующие режимы фильтрации файервола антивируса:

* автоматический режим;
* интерактивный режим;
* режим на основе политики;
* режим обучения.

**2. Настройка Оффлайн обновления сигнатур угроз из локальной папки.**

Обновление сигнатур угроз для Eset Nod Antivirus 4.2.76.1.

В дополнительных настройках (при нажатии клавиши F5) необходимо выбрать пункт «Обновление». В строке «Сервер обновлений» выбрать «Изменить» и вставить путь к файлам сигнатур.

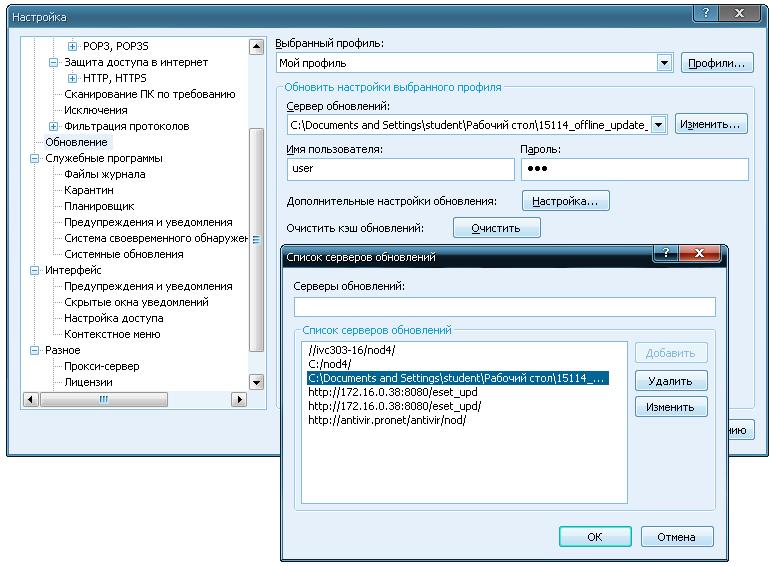


Рисунок 5.4 – Оффлайн обновление.

Для [обновления](https://support.kaspersky.ru/6582) компьютеров по локальной сети или отдельно стоящих компьютеров был реализован процесс ретрансляции антивирусных баз и программных модулей в локальный источник (папку на диске, сетевой ресурс). Для организации обновления антивирусных баз из локальной папки необходим как минимум один компьютер, имеющий доступ к сети Интернет.

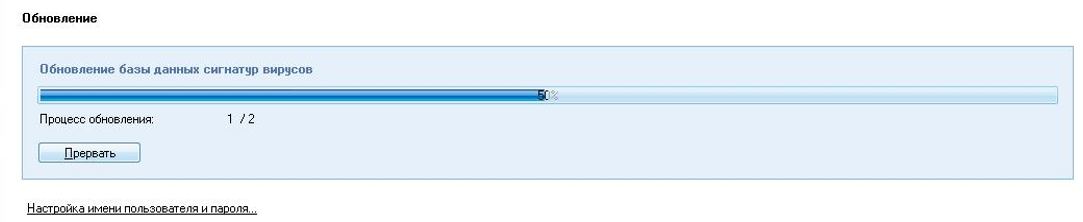


Рисунок 5.5 – Обновление баз данных.

Если у вас в локальной сети установлено несколько копий антивируса, то обновление для каждой копии можно настроить из локальной папки с помощью ретрансляции (приема и передачи) баз в эту папку.

**3. Настройка оффлайн обновления сигнатур угроз с локального сервера по HTTP**

Можно настроить клиент для загрузки обновления сигнатур вирусов с помощью сервера в локальной сети. Для этого необходимо добавить ip-адрес сервера в список “Сервер обновлений”.

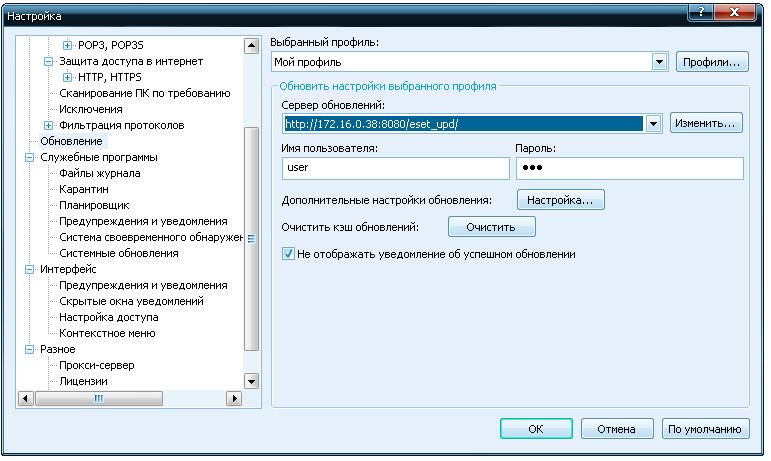
****

Рисунок 5.6 – Обновление по HTTP

Файлы обновлений можно увидеть по введенному адресу и данным пользователя через проводник.

**Вывод**

Антивирус – программа, специально разработанная для обнаружения и удаления компьютерных вирусов и вредоносных программ других типов.

Современные антивирусные программы способны эффективно обнаруживать вредоносные объекты внутри файлов программ и документов. В некоторых случаях антивирус может удалить тело вредоносного объекта из зараженного файла, восстановив файл.

Антивирус способен в большинстве случаев удалить вредоносный программный объект не только из программного файла, но и из файла офисного документа, не нарушив его целостность.

Использование антивирусных программ не требует высокой квалификации и доступно практически любому пользователю компьютера.