Учреждение образования

«Белорусский государственный технологический университет»

**Отчёт за практические занятия по предмету:**

Основы защиты информации

Выполнила:

Студентка 2 курса 1 группы ФИТ

Гринцевич Юлия Сергеевна

**2021г.**

# **Практическое занятие №1**

**Концепция национальной безопасности РБ**

**Цель работы:** Изучить концепцию национальной безопасности РБ.

**Ответы:**

1. **Что такое информационная безопасность?**

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

**Информационная безопасность** – такое состояние рассматриваемой системы, при котором она, с одной стороны, способна противостоять дестабилизирующему воздействию внешних и внутренних информационных угроз, а с другой – ее функционирование не создает информационных угроз для элементов самой системы и внешней среды.

1. **Перечислить основные национальные интересы 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;

Основные национальные интересы в информационной сфере:

* реализация 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.

1. **Основные угрозы национальной безопасности, связанные с ИТ-сферой?**

**Источник угрозы национальной безопасности** - фактор или совокупность факторов, способных при определенных условиях привести к возникновению угрозы национальной безопасности;

**Угроза национальной безопасности -** потенциальная или реально существующая возможность нанесения ущерба национальным интересам Республики Беларусь;

1)нарушение функционирования критически важных объектов информатизации;

2)деструктивное информационное воздействие на личность, общество и государственные институты, наносящее ущерб национальным интересам;

3)недостаточные масштабы и уровень внедрения передовых информационно-коммуникационных технологий;

4)снижение или потеря конкурентоспособности отечественных информационно-коммуникационных технологий, информационных ресурсов и национального контента;

1. **Назвать основные внутренние и внешние источники угроз национальной безопасности в информационной сфере?**

**Внутренние:**

1)зависимость Республики Беларусь от импорта информационных технологий, средств информатизации и защиты информации, неконтролируемое их использование в системах;

2)несоответствие качества национального контента мировому уровню;

3)недостаточное развитие государственной системы регулирования процесса внедрения и использования информационных технологий;

4)распространение недостоверной или умышленно искаженной информации, способной причинить ущерб национальным интересам Республики Беларусь;

5)рост преступности с использованием информационно-коммуникационных технологий;

6)недостаточная эффективность информационного обеспечения государственной политики;

7)несовершенство системы обеспечения безопасности критически важных объектов информатизации.

**Внешние:**

1)открытость и уязвимость информационного пространства Республики Беларусь от внешнего воздействия;

2)доминирование ведущих зарубежных государств в мировом информационном пространстве;

3)информационная деятельность зарубежных государств, международных и иных организаций, отдельных лиц, наносящая ущерб национальным интересам Республики Беларусь;

4)нарастание информационного противоборства между ведущими мировыми центрами силы, подготовка и ведение зарубежными государствами борьбы в информационном пространстве;

5)развитие технологий манипулирования информацией;

6)препятствование распространению национального контента Республики Беларусь за рубежом;

7)широкое распространение в мировом информационном пространстве образцов массовой культуры, противоречащих общечеловеческим и национальным духовно-нравственным ценностям;

8)попытки несанкционированного доступа извне к информационным ресурсам Республики Беларусь;

1. **Основные направления нейтрализации внутренних источников угроз и защиты от внешних угроз национальной безопасности в информационной сфере?**

Нейтрализация внутренних источников угроз национальной безопасности обеспечивается путем принятия своевременных и действенных мер по устранению условий и предпосылок формирования политической и социально-экономической напряженности в обществе, практического воплощения принципов демократического социального правового государства, взаимной ответственности личности, общества и государства по обеспечению национальной безопасности.

**Вывод:** изучая концепцию национальной безопасности РБ были получены знания о национальной безопасности: основные положения и тенденции современного мира, национальные интересы, состояния национальной безопасности на современном этапе, основные угрозы, внутренние и внешние источники угроз национальной безопасности.

**Международные стандарты информационной безопасности**

**Ответы на вопросы:**

**2. Охарактеризуйте основные положения Оранжевой книги.**

В Оранжевой книге предложены три категории требований безопасности - политика безопасности, аудит и корректность, в рамках которых сформулированы шесть базовых требований безопасности. Первые четыре требования направлены не посредственно на обеспечение безопасности информации, а два последних - на качество самих средств защиты.

1. Политика безопасности.

• Политика безопасности

Возможность осуществления субъектами доступа к объектам должна определяться на основе их идентификации и набора правил управления доступом.

• Метки

Для реализации нормативного управления доступом система должна обеспечивать возможность присваивать каждому объекту метку или набор атрибутов, определяющих степень конфиденциальности (гриф секретности) объекта и/или режимы доступа к этому объекту.

2. Аудит.

• Идентификация и аутентификация

Все субъекты должны иметь уникальные идентификаторы. Контроль доступа должен осуществляться на основании результатов идентификации субъекта и объекта доступа, подтверждения подлинности их идентификаторов (аутентификации) и правил разграничения доступа. Данные, используемые для идентификации и аутентификации, должны быть защищены от несанкционированного доступа, модификации и уничтожения и ассоциированы со всеми активными компонентами компьютерной системы, функционирование которых критично с точки зрения безопасности.

• Регистрация и учет

Для определения степени ответственности пользователей за действия в системе все происходящие в ней события, имеющие значение с точки зрения безопасности, должны отслеживаться и регистрироваться в защищенном протоколе. Система регистрации должна осуществлять анализ общего потока событий и выделять из него только те события, которые оказывают влияние на безопасность для сокращения объема протокола и повышения эффективность его анализа. Протокол событий должен быть надежно защищен от несанкционированного доступа, модификации и уничтожения.

3. Корректность.

• Контроль корректности функционирования средств защиты

Средства защиты должны содержать независимые аппаратные и/или программные компоненты, обеспечивающие работоспособность функций защиты. Это означает, что все средства защиты, обеспечивающие политику безопасности, управление атрибутами и метками безопасности, идентификацию и аутентификацию, регистрацию и учёт, должны находиться под контролем средств, проверяющих корректность их функционирования. Основной принцип контроля корректности состоит в том, что средства контроля должны быть полностью независимы от средств защиты.

•Непрерывность защиты

Все средства защиты (в т. ч. и реализующие данное требование) должны быть защищены от несанкционированного вмешательства и/или отключения, причем эта защита должна быть постоянной и непрерывной в любом режиме функционирования системы защиты и компьютерной системы в целом. Данное требование распространяется на весь жизненный цикл компьютерной системы. Кроме того, его выполнение является одним из ключевых аспектов формального доказательства безопасности системы.

**4. Каковы основные положения Европейских критериев безопасности информационных технологий?**

Европейские критерии рассматривают следующие задачи средств информационной безопасности:

\*защита информации от несанкционированного доступа с целью обеспечение конфиденциальности;

\*обеспечение целостности информации посредством защиты от ее несанкционированной модификации или уничтожения;

\*обеспечение работоспособности систем с помощью противодействия угрозам отказа в обслуживании.

**5. Чем отличается «информационная система» и «продукт информационных технологий»?**

Система - это конкретная аппаратно-программная конфигурация, построенная с вполне определенными целями и функционирующая в известном окружении.

Продукт – это аппаратно-программный «пакет», который можно купить и по своему усмотрению встроить в ту или иную систему.

Таким образом, с точки зрения информационной безопасности основное отличие между системой и продуктом состоит в том, что система имеет конкретное окружение, которое можно определить и изучить сколь угодно детально, а продукт должен быть рассчитан на использование в различных условиях. Угрозы безопасности системы носят вполне конкретный и реальный характер. Относительно угроз продукту можно лишь строить предположения. Разработчик может специфицировать условия, пригодные для функционирования продукта; дело покупателя обеспечить выполнение этих условий.

**7. Что такое Профиль защиты?**

**Профиль защиты** - это нормативный документ, который регламентирует все аспекты безопасности ИТ-продукта в виде требований к его проектированию, технологии разработки и квалификационному анализу.

**9. Опишите структуру общих критериев безопасности информационных технологий.**

Общие критерии состоят из 3-х частей:

1. Введение и общая модель.

2. Функциональные требования безопасности.

3. Требования доверия к безопасности.

**10. Опишите технологию применения общих критериев безопасности информационных технологий.**

Единые критерии сохраняют совместимость с существующими стандартами и развивают их путем введения новых концепций, соответствующих современному уровню развития информационных технологий и интеграции национальных информационных систем в единое мировое информационное пространство.

*Производители* используют предлагаемую Едиными критериями технологию для обоснования своих претензий на то, что поставляемый ими ИТ-продукт успешно противостоит угрозам безопасности, на основании того, что он удовлетворяет выдвинутым функциональным требованиям и их реализация осуществлена с достаточным уровнем адекватности. Для осуществления этой технологии Единые критерии предлагают производителям специальный механизм, названный Проект защиты, дополняющий Профиль защиты и позволяющий соединить описания требований, на которые ориентировался разработчик, спецификации механизмов реализации этих требований.

**11. Каковы тенденции развития международной нормативной базы в области информационной безопасности?**

Первые версии стандартов создавались в основном исходя из нужд обороны и были нацелены на обеспечение секретности информации. С развитием средств вычислительной техники и телекоммуникаций возникла потребность создания новых стандартов, отражающих особенности современного уровня информационных технологий.

# **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, организационные, технические, комплексные.

Е0− положительный эффект (экономический, политический, технический и т.д.

∆E− на такую величину несанкционированный доступ к объекту уменьшает полезный эффект от его функционирования.

E− эффективность функционирования объекта с учетом воздействия несанкционированного доступа.

Тогда эффективность функционирования объекта с учетом воздействия несанкционированного доступа: 𝐸=𝐸0−∆𝐸

∆𝐸3− снижение эффективности функционирования объекта при наличии средств защиты

K− это коэффициент снижения негативного воздействия несанкционированного доступа на эффективность функционирования объекта; возрастающая.

Таким образом, для обеспечения максимальной эффективности объекта в условиях несанкционированного доступа имеет вид:

**Задание на выполнение:**

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № варианта | *E*0 | *E* | *K* | *C* |
| 6 | 12000 | 11000 | 6 | 300 |

Исходные данные: E0 =12000(руб.) E =11000(руб.) K=6 C=300(руб.).

Рассчитаем ∆E: ∆𝐸=𝐸0−𝐸=12000-11000=1000(руб.)

Находим значение относительной эффективности функционирования по формуле:



Относительная эффективность = 1-(1000/12000)=0,92

Вычислим коэффициент снижения негативного воздействия несанкционированного доступа на эффективность функционирования объекта по формуле:



Получим коэффициент снижения негативного воздействия несанкционированного доступа на эффективность функционирования объекта равный 1000/6=166,67 (руб.)

Находим эффективность функционирования по формуле:



Получим 12000-166,67= 11833,33 (руб.)

Найдём относительную эффективность функционирования по формуле:



Получим 1 - ( 1000 / 6 / 12000 ) = 0,99

В том случае, если эффективность функционирования имеет стоимостное значение, то вычисляем по формуле:



Получим 12000 – ( 1000 / 6 ) - 300 = 11533,33

**Вывод:** В итоге получим прибыль 11533,33 – 11000 = 533,33 (руб.);

В результате проведения лабораторной работы был приобретён опыт решения задач для создания средств защиты информации. На данных, полученных в результате работы, строится система для обеспечения максимальной эффективности объекта в условиях несанкционированного доступа.

# **Практическое занятие №3**

**Разработка политики информационной безопасности завода**

**Цель работы**: Разработать проект политики информационной безопасности бизнес-компании.

**Введение**

Информационные ресурсы в современном обществе являются наиболее значимыми, но при этом, очень уязвимыми т.к. механизм их распространения становится все более гибким и количество возможностей их передачи растет. В связи с этим информационная безопасность — одно из важнейших условий функционирования любой структуры, будь то государственное учреждение или частное предприятие.

Темпы развития современных информационных технологий значительно опережают темпы разработки рекомендательной и нормативно-правовой базы руководящих документов, действующих на территории Беларуси. Поэтому решение вопроса об разработке эффективной политики информационной безопасности на современном предприятии обязательно связано с проблемой выбора критериев и показателей защищенности, а также эффективности корпоративной системы защиты информации. Вследствие этого, в дополнение к требованиям и рекомендациям стандартов, Конституции, законам и иным руководящим документам приходится использовать ряд международных рекомендаций. В том числе адаптировать к отечественным условиям и применять на практике методики международных стандартов, таких, как ISO 17799, ISO 9001, ISO 15408, BSI, COBIT, ITIL и другие, а также использовать методики управления информационными рисками в совокупности с оценками экономической эффективности инвестиций в обеспечение защиты информации предприятия.

Информационная безопасность компании, общественной организации или производственного предприятия – это комплекс мероприятий, направленных на предотвращение несанкционированного доступа к внутренней IT-инфраструктуре, незаконного завладения конфиденциальной информацией и внесения изменений в базы данных.

Безопасность информационной инфраструктуры компании подразумевает защиту от случайных или умышленных действий, которые могут нанести вред владельцам данных или их пользователям. Действия лиц, несущих ответственность за эту сферу, должны быть направлены на создание защиты, препятствующей утечкам данных, а не борьбу с их последствиями. Но при этом важно сохранять простой доступ к информации тем людям, которые на законных основаниях пользуются базами данных.

**Общие положения**

Цели и задачи

Концептуальная схема информационной безопасности предприятия направлена на защиту его информационных активов от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий персонала, технических сбоев, неправильных технологических и организационных решений в процессах обработки, передачи и хранения информации и обеспечение нормального функционирования технологических процессов.

- разработка и совершенствование нормативно-правовой базы обеспечения информационной безопасности;

- выявление, оценка и прогнозирование угроз информационной безопасности;

- организация технической защиты информации, участие в проектировании систем защиты;

- проведение периодического контроля состояния ИБ, учет и анализ результатов с выработкой решений по устранению уязвимостей и нарушений;

- контроль за использованием закрытых каналов связи и ключей с цифровыми подписями;

- организация плановых проверок режима защиты, и разработка соответствующей документации, анализ результатов, расследование нарушений;

- разработка и осуществление мероприятий по защите персональных данных;

- организация взаимодействия со всеми структурами, участвующими в их обработке, выполнение требований законодательства к информационным системам персональных данных, контроль действий операторов, отвечающих за их обработку.

**Структура организации**

Под организационной структурой управления предприятием понимается состав отделов, служб и подразделений в аппарате управления, системная их организация, характер соподчиненности и подчиненности друг другу и высшему органу управления, а также набор координационных и информационных связей, порядок распределения функций управления по различным уровням и подразделениям.

Директор является исполнительным органом организационной структуры. Директор предприятия осуществляет также контролирующую функцию, т.е. он подписывает и утверждает документы, договора и сделки с другими организациями, а также контракты о приёме на работу.

В организации разработаны положения о структурных подразделениях и должностные инструкции. Каждое подразделение взаимосвязано с другими подразделениями и выполняет свою функцию. Например, отдел кадров занимается вопросами формирования и развития стабильного трудового коллектива, созданием благоприятного социально-психологического климата, осуществляет эффективную кадровую политику, оказывает методическую помощь руководителям подразделений по проблемам управления персоналом. Является самостоятельным структурным подразделением и подчиняется непосредственно директору организации.

Во главе завода традиционно стоит **директор**. По каждому крупному направлению работы – у директора и других сотрудников некоторых должностей есть заместители – главный бухгалтер, главный инженер.

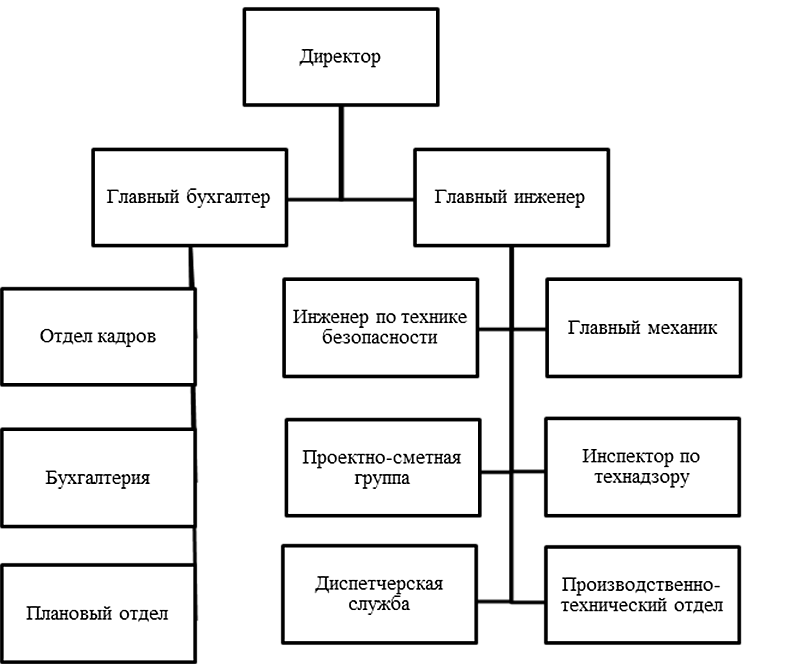
**Главный бухгалтер** непосредственно подчиняется директору предприятия и принимает участие в производственных, технических совещаниях.

Непосредственно главному бухгалтеру подчиняется планово-экономический отдел

В планово-экономическом отделе осуществляется разработка направлений перспективного развития предприятия, а также планирование объема, ассортимента и качества продукции, разрабатывается и утверждается годовой план экономического и социального развития.

**Главный инженер** организует обучение и повышение квалификации рабочих и инженерно-технических работников.

Является первым заместителем директора организации и несет ответственность за результаты и эффективность производственной деятельности.



Производственная структура предприятия – это состав и соотношение его внутренних звеньев: цехов отделов, лабораторий и других компонентов, составляющих единый хозяйственный объект; определяется размером предприятия, отраслью производства, уровнем технологии и специализации предприятия.

**Оценка рисков**

Угрозы информационной безопасности могут быть классифицированы по различным признакам:

*– 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 степени преднамеренности действий:*

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

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

*– по расположению источника угроз:*

а) внутренние (источники угроз располагаются внутри системы);

б) внешние (источники угроз находятся вне системы);

*– 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 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 (автоматизированным системам управления технологическим процессом) 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.

Защита 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:**

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

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

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

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

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

**Защита технических средств обработки, хранения и передачи информации**

В целях предотвращения несанкционированного доступа к информации и ее утечки, 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 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.

**Защита от вредоносного ПО**

В целях предотвращения проникновения, обнаружения внедрения и нейтрализации вредоносного ПО в АСУ ТП применяются *средства защиты* от вредоносного ПО, они *устанавливаются на серверном оборудовании и автоматизированные рабочие места 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.

**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.*

**Локальная безопасность**

**Локальная политика безопасности**, то есть точное описание настроек для корректной реализации правил аутентификации пользователей, управления доступом, защиты трафика и др., необходима любому средству защиты, реализующему какой-либо сервис информационной безопасности. При традиционном подходе администратору приходится отдельно настраивать каждое средство защиты или реплицировать какие-то простейшие настройки на большое число узлов с последующей их корректировкой. Очевидно, что это неизбежно приводит к большому числу ошибок администрирования и, как следствие, к существенному снижению уровня защищенности корпоративной сети.

***Антивирусная защита***

Антивирусная защита предназначена для обеспечения антивирусной защиты серверов и автоматизированных рабочих мест пользователей предприятий. *На каждом работающем компьютере, или сервере при вводе в эксплуатацию или после переустановки ОС* сотрудниками ЦНИТ *в обязательном порядке устанавливается и активируется антивирусная программа.*

**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 её разработку и осуществление.

Разработаны технические меры обеспечения безопасности, организационные меры обеспечения безопасности, сетевая безопасность, общие меры предосторожностей, так же такие пункты как люди, и процессы, и избыточность, и непрерывность работы.

Политика безопасности должна быть разработана так, чтобы её взлом стоил дороже, чем сама информация.

# **Практическое занятие №4**

**Настройка Брандмауэра Windows**

**Цель работы:** Овладение навыками настройки и использования Брандмауэра Windows.

**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 потоки данных.

1. **Создать правила для входящих подключений (с помещением в электронный конспект копий экрана с пояснениями промежуточных действий):**

Для создания правила по ограничению доступа программ к сети необходимо открыть Панель управления в меню Пуск (рис. 1)

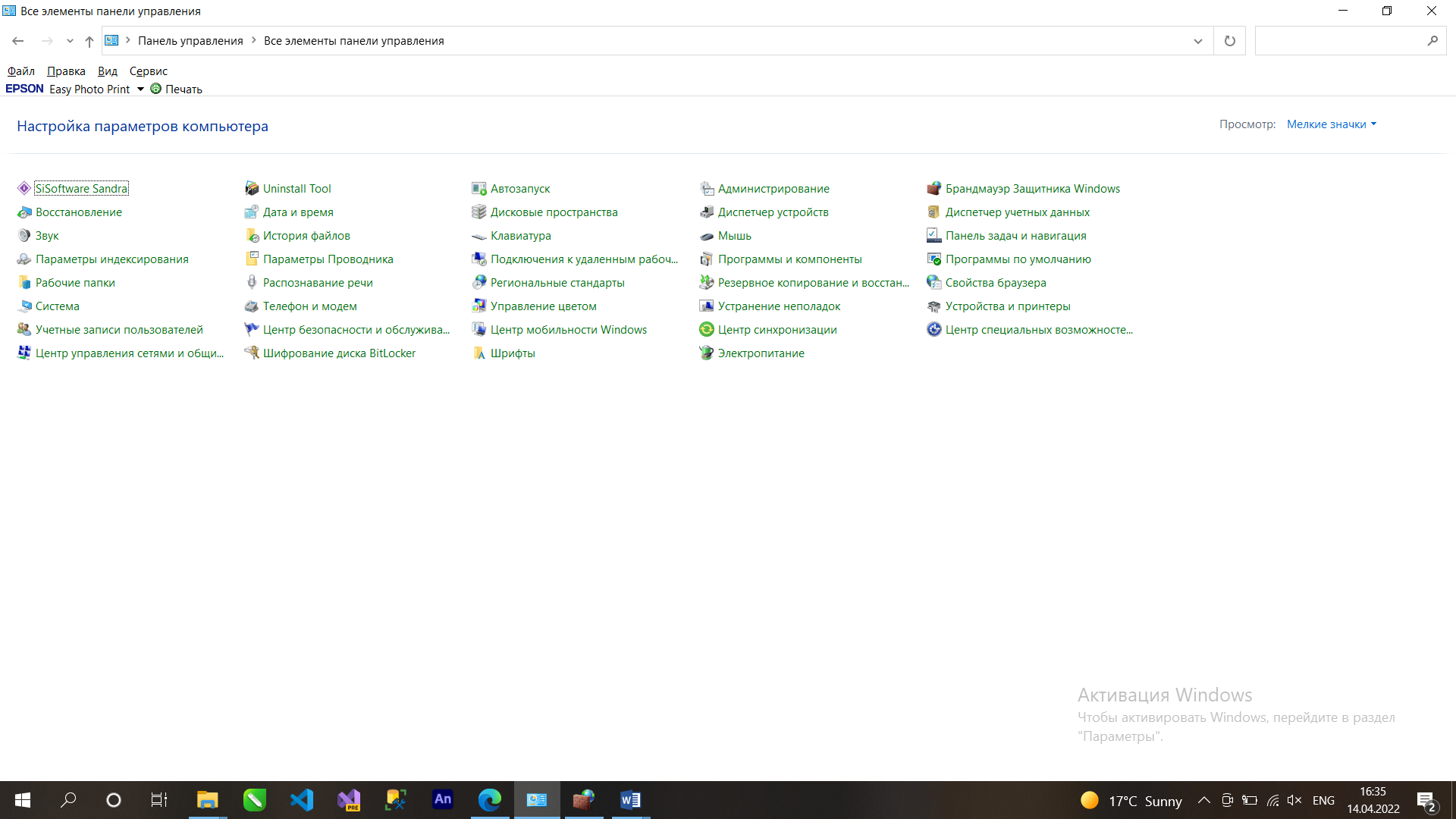


Рисунок 1 – Классический вид

Первым этапом необходимо включить брандмауэр, в случае, если он был ранее выключен. Необходимо выбрать в левой панели управления вкладку «Включение и отключение брандмауэра Windows» (рис. 2). В появившемся окне переключаем параметры на значение «Включение брандмауэра Windows»

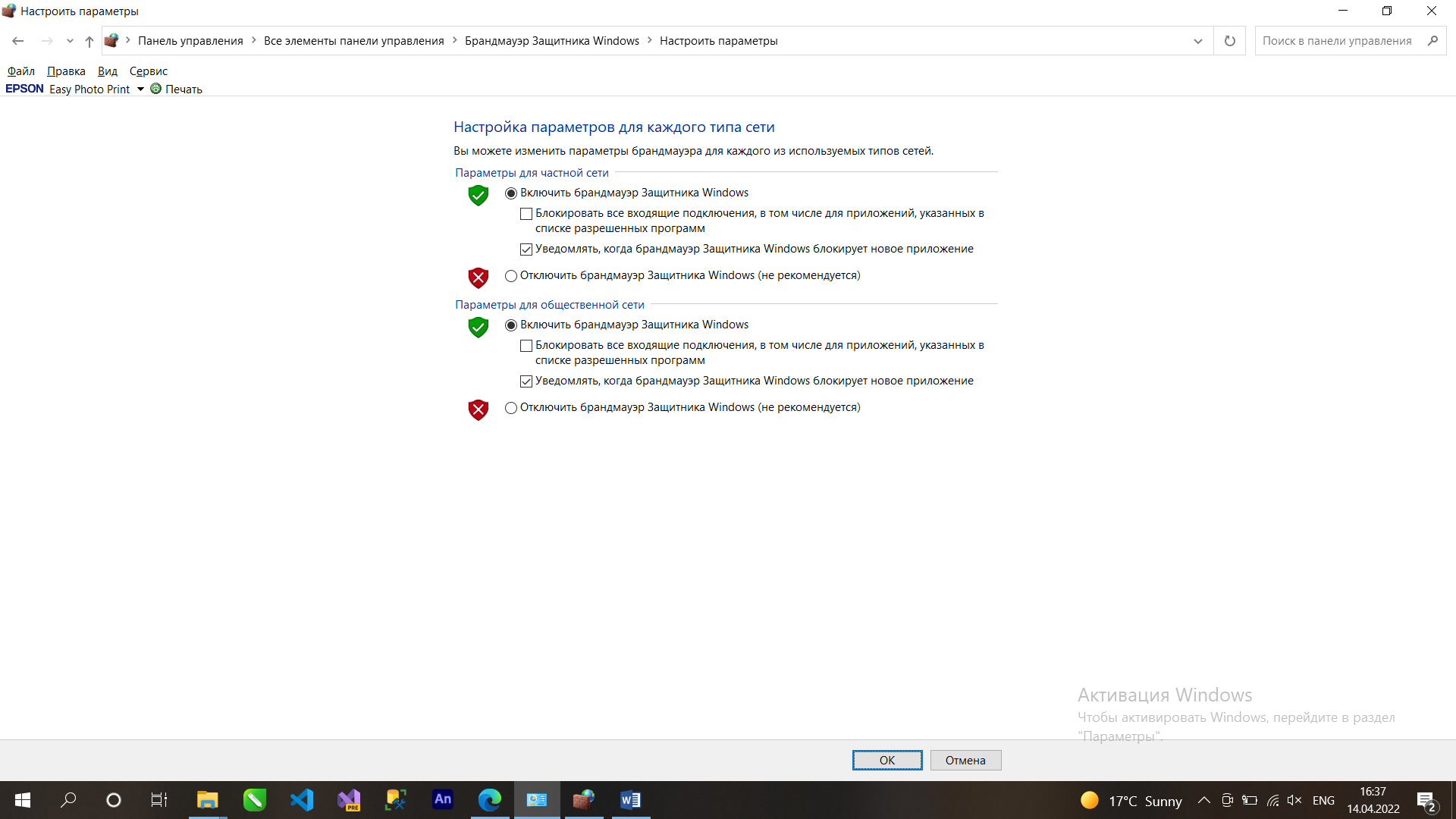


Рисунок 2 – Включение брандмауэра Windows

Вторым этапом является настройка правил для входящих и исходящих подключений. Для этого во вкладке «Дополнительные параметры» (рис. 3).

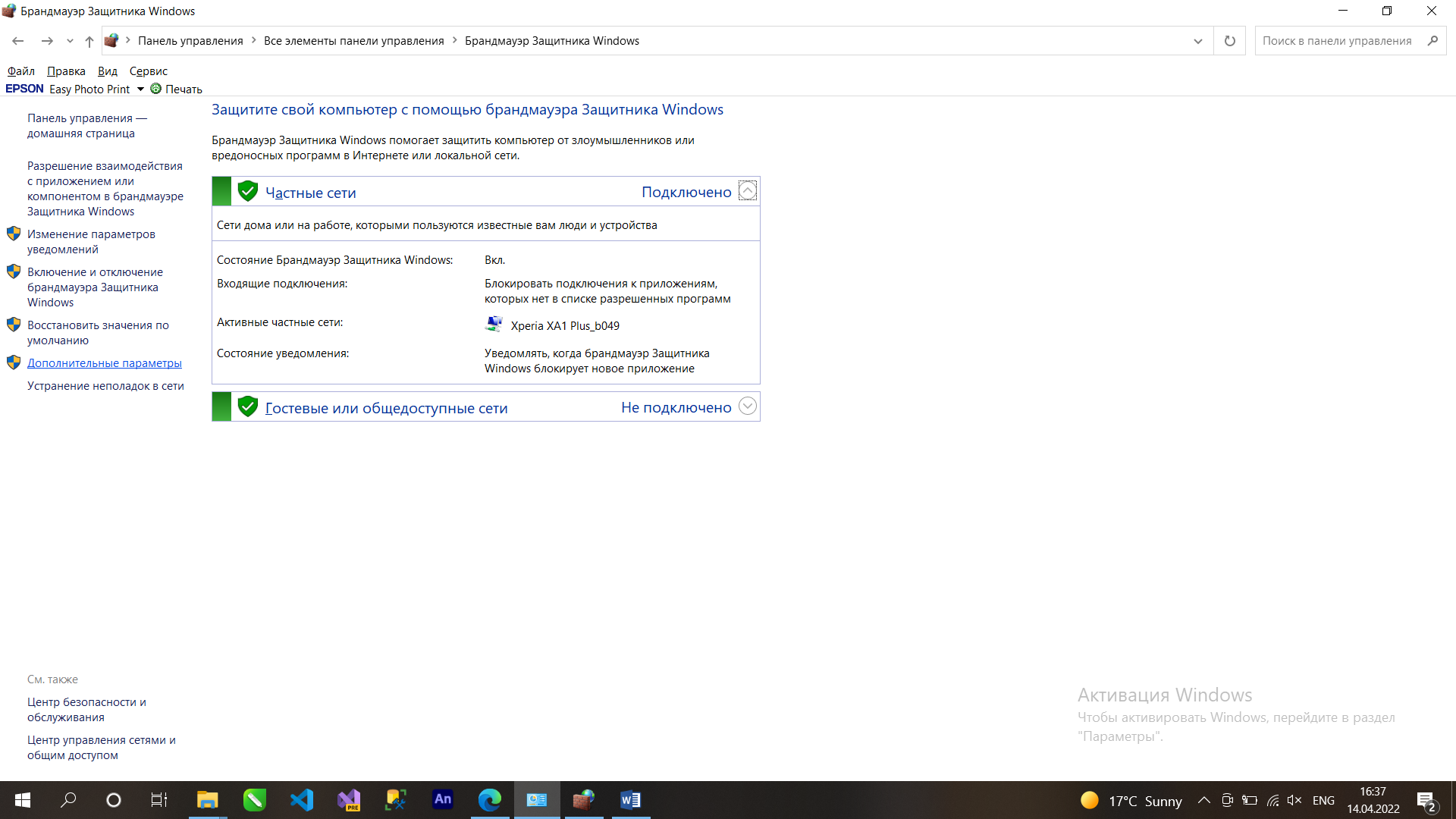


Рисунок 3 – Включение брандмауэра Windows

В открывшемся окне выбираем в левой панели правила для входящих подключений, затем во вкладке меню «Действие» выбираем «Создать правило», либо нажимаем «Создать правило» в правой панели (рис. 4).

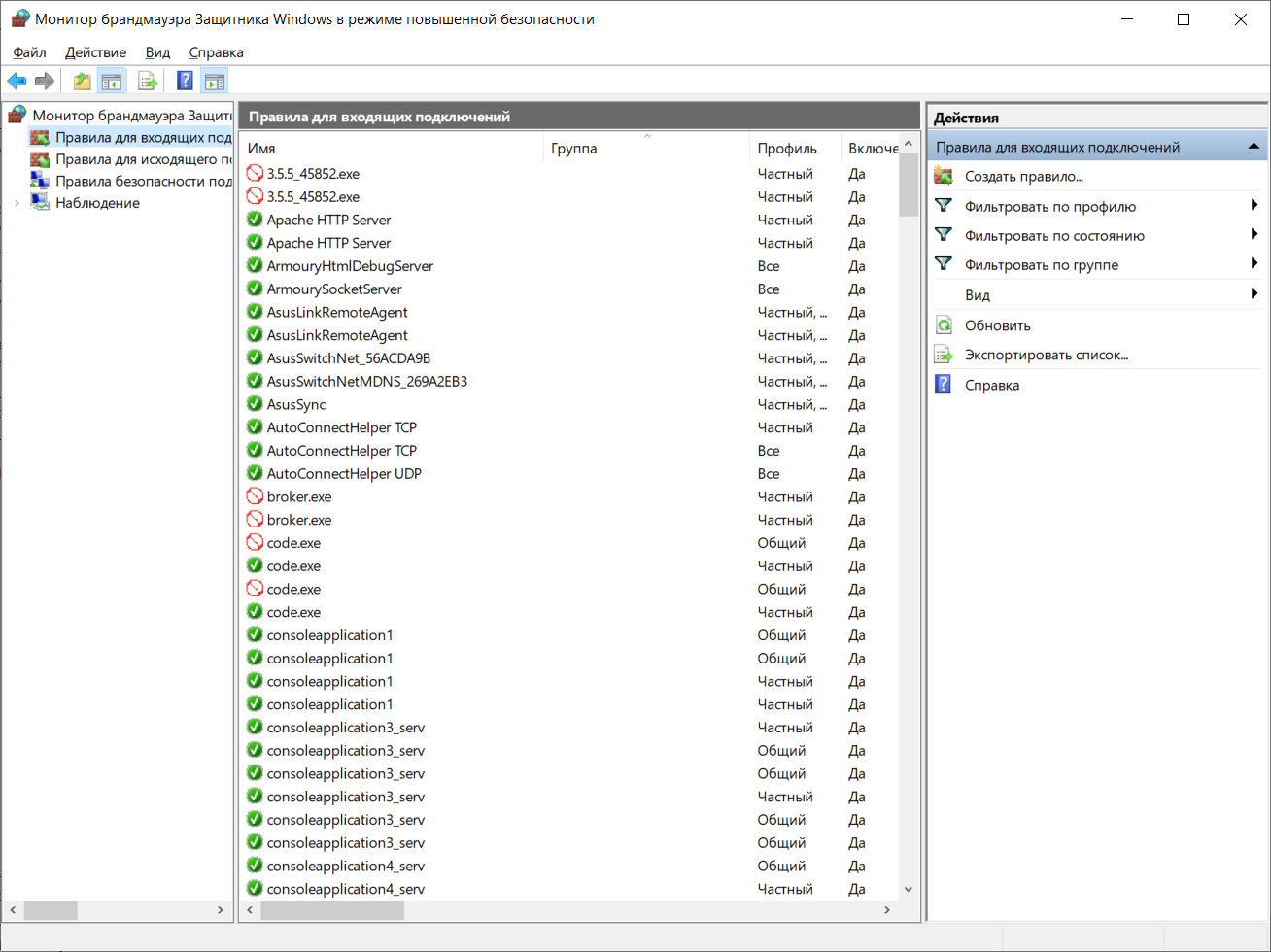


Рисунок 4 – Создание правила

В открывшемся мастере создания 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) (рис. 5).

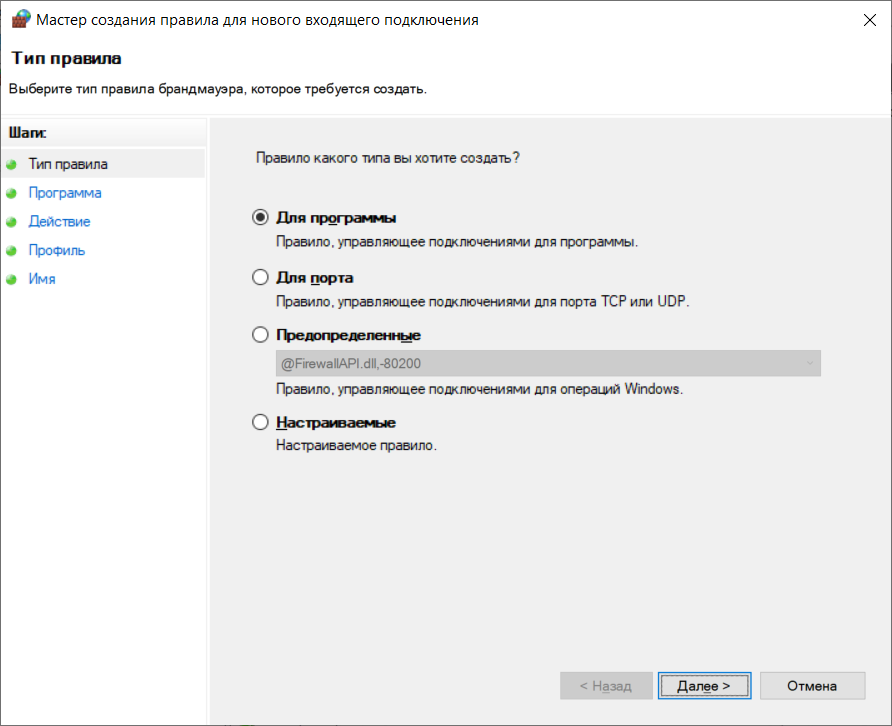


Рисунок 5 – Выбор типа правила

При ограничении работы программы, далее необходимо указать её путь, обязательно через папку в которой она установлена, а не через ярлыки(Рис. 6).

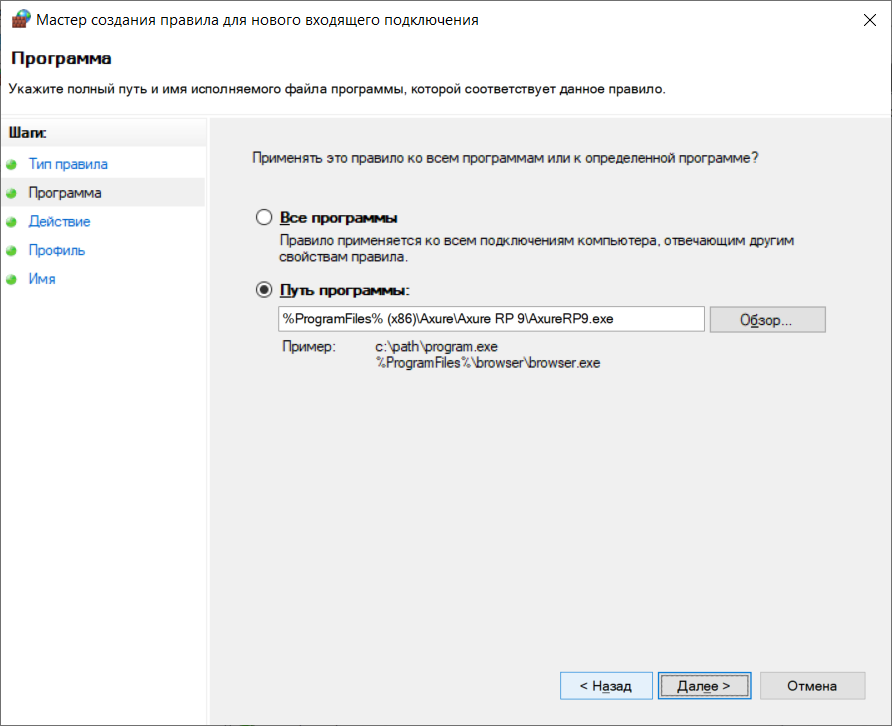


Рисунок 6 – Настройка пути программы

***Далее указывается какое именно действие мы хотите применить.***

* 1. Для 1 программы (по выбору) на блокировку подключения;

*В данном случае необходимо блокировать подключение (рис. 7).*

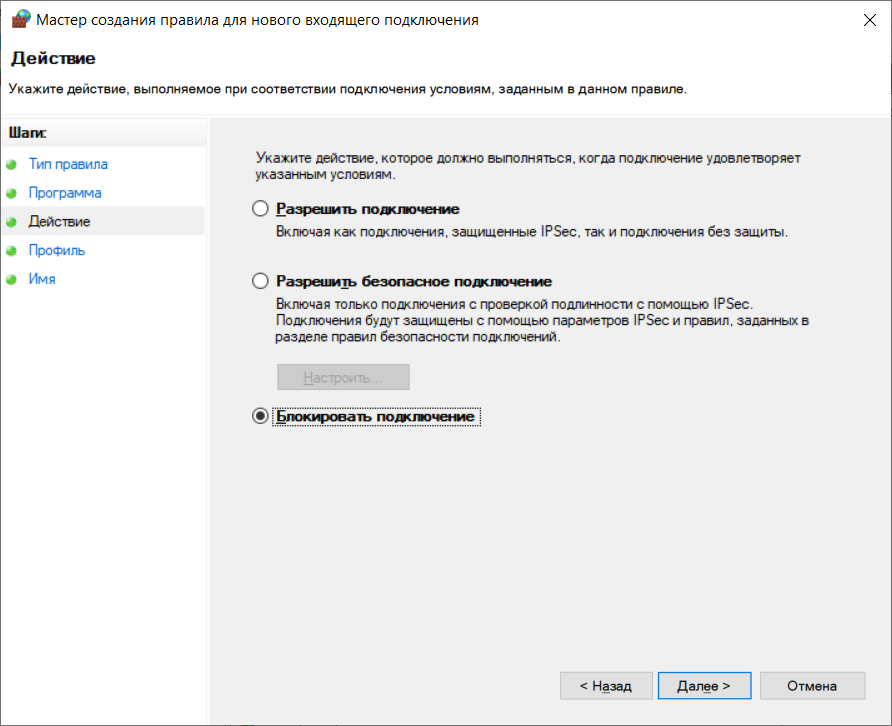


Рисунок 7 – Выбор действия

Далее указывается профиль правила (рис. 8).

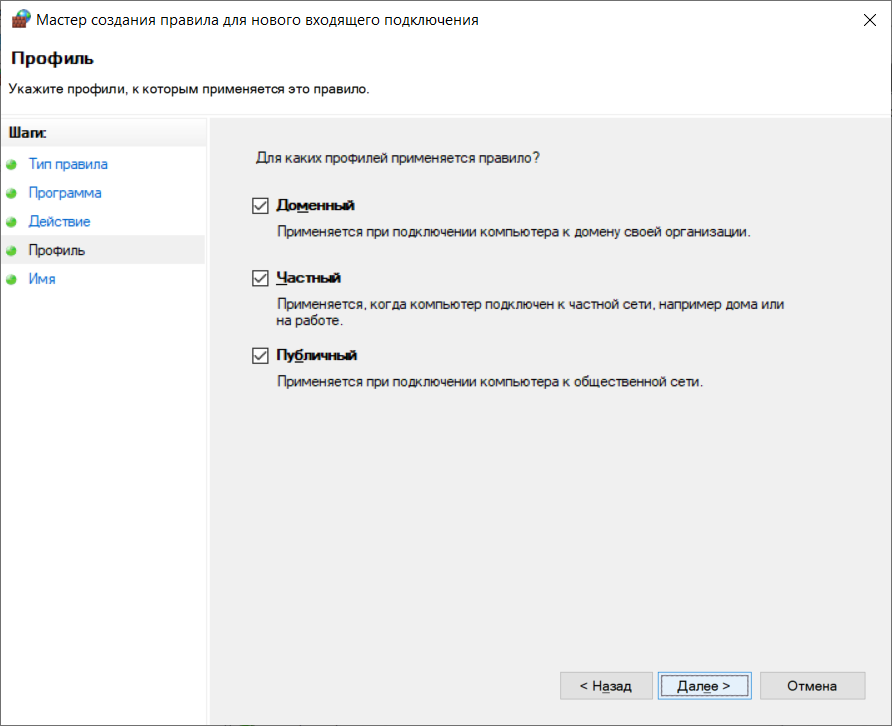


Рисунок 8 – Профиль

В следующем окне указывается имя правила (рис. 9).

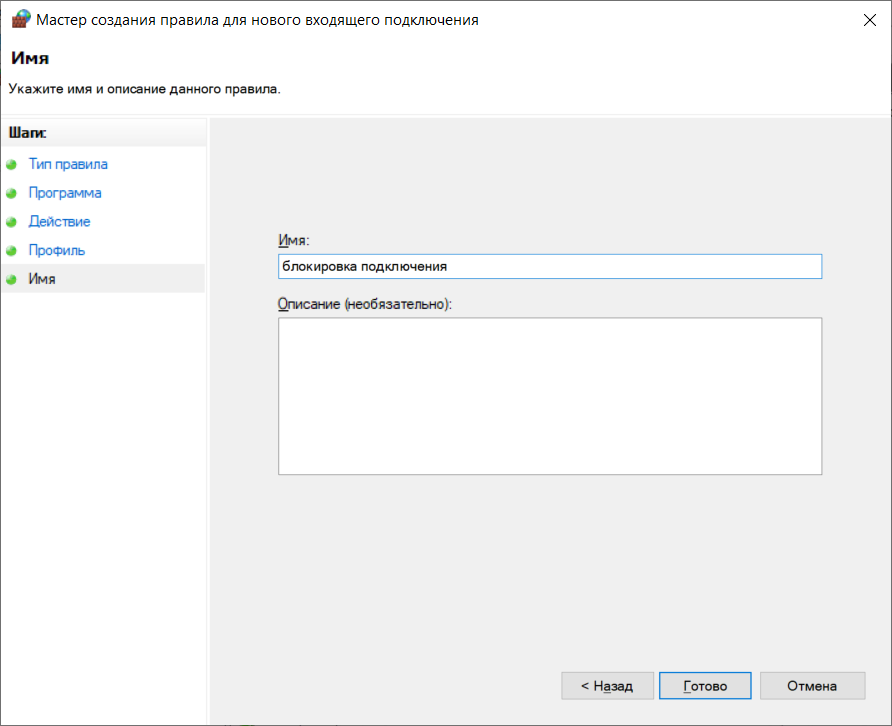


Рисунок 9 – Окно ввода имени

В общем списке появилось созданное правило. Правила можно отключать, копировать, удалять с помощью кнопок на правой панели (рис. 10).



Рисунок 10 – Созданное правило

* 1. Для 1 программы (по выбору) на разрешение подключения;

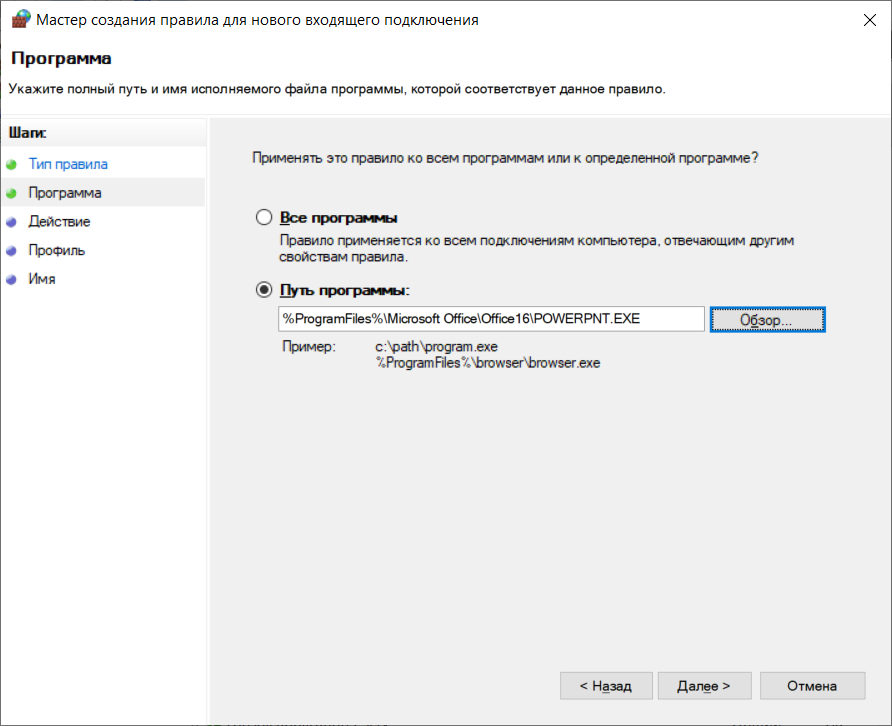


Рисунок 11 – Настройка пути программы

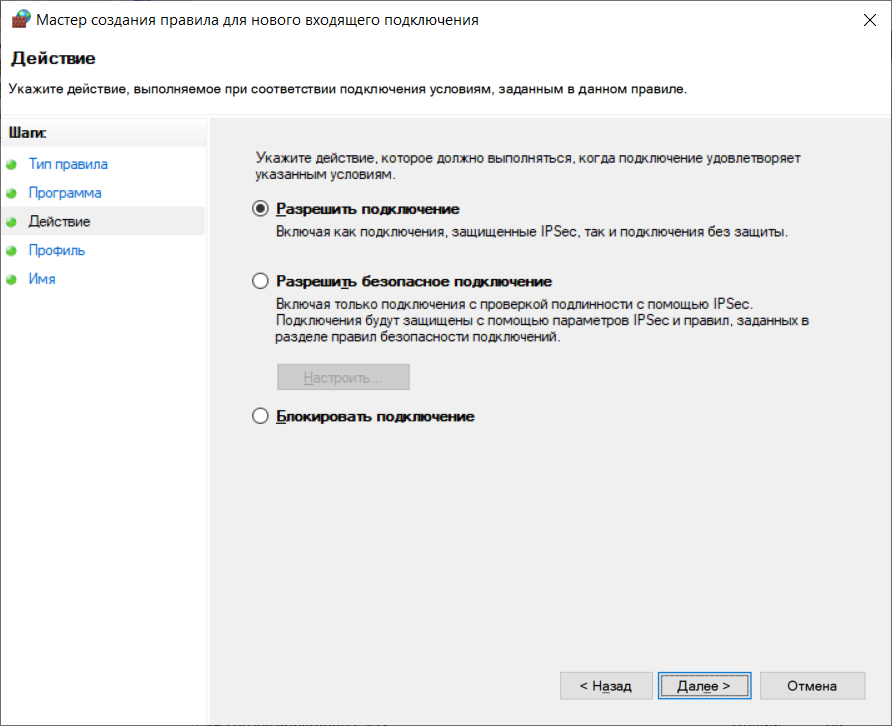


Рисунок 12 – Выбор действия

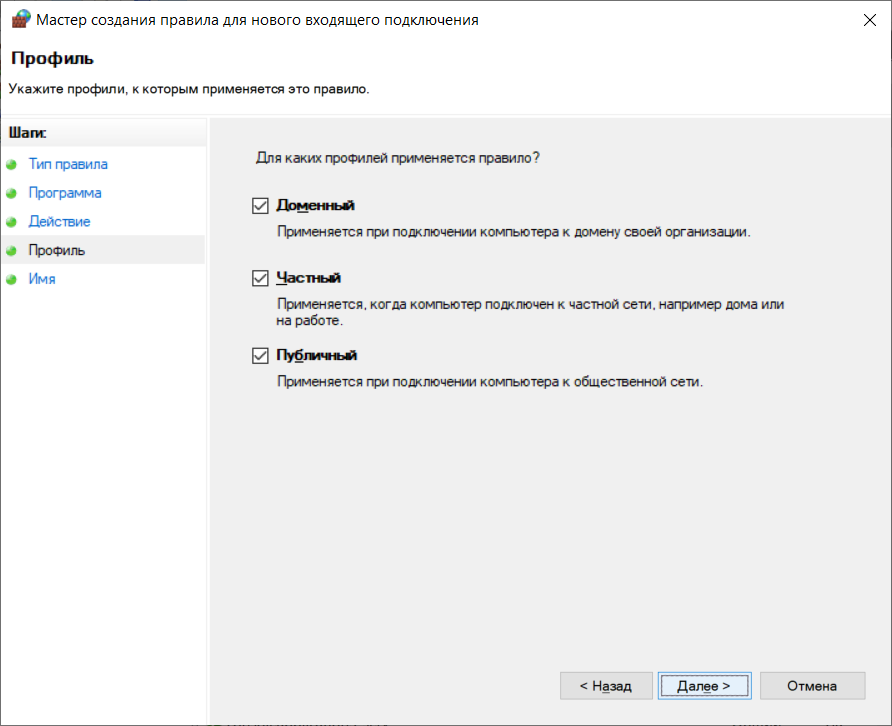


Рисунок 13 – Профиль правила

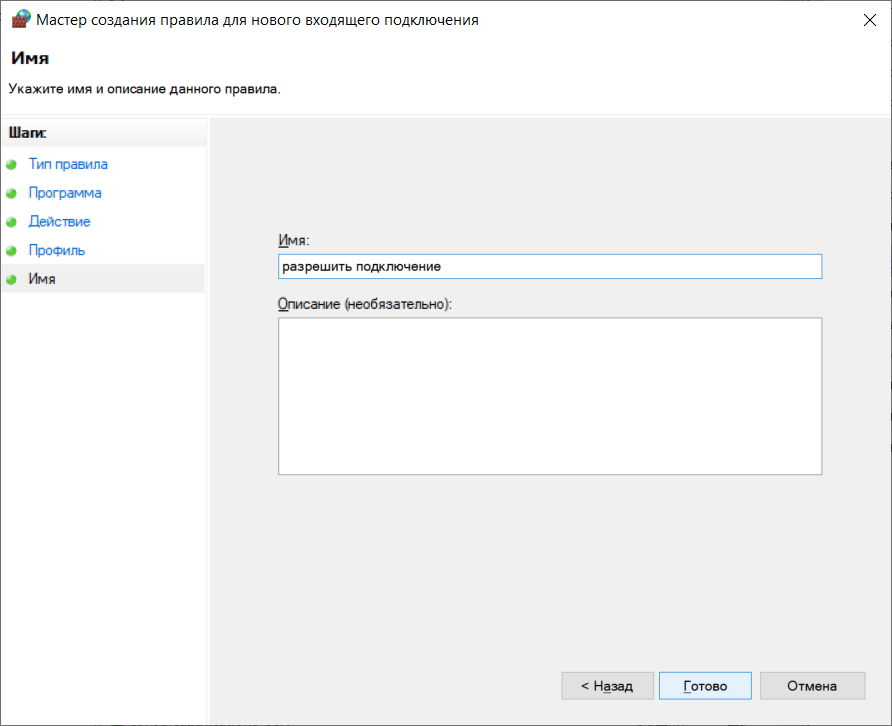


Рисунок 14 – Окно ввода имени

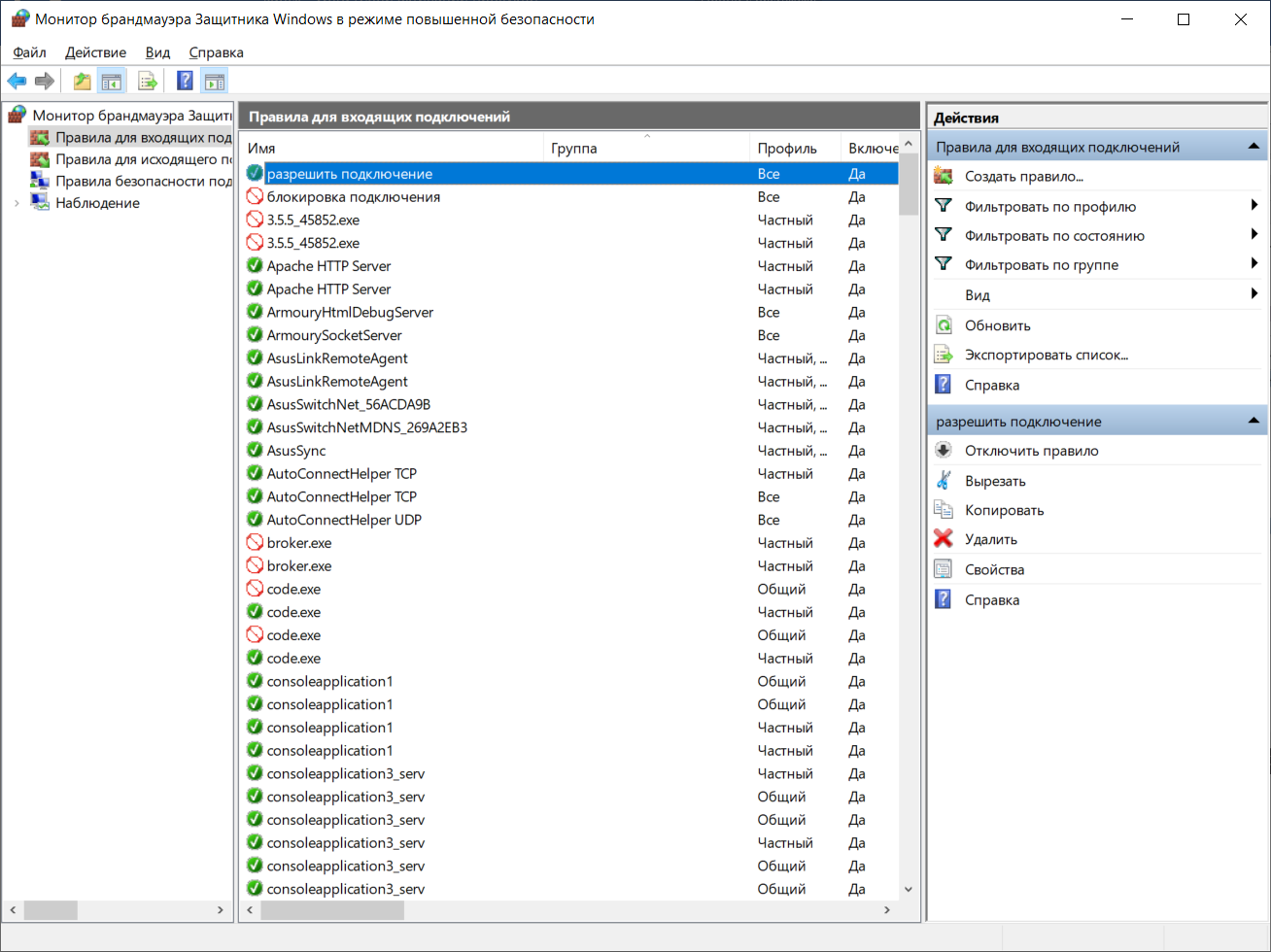


Рисунок 15 – Созданные правила

1. Создать правила для исходящих подключений (с помещением в электронный конспект копий экрана с пояснениями действий):

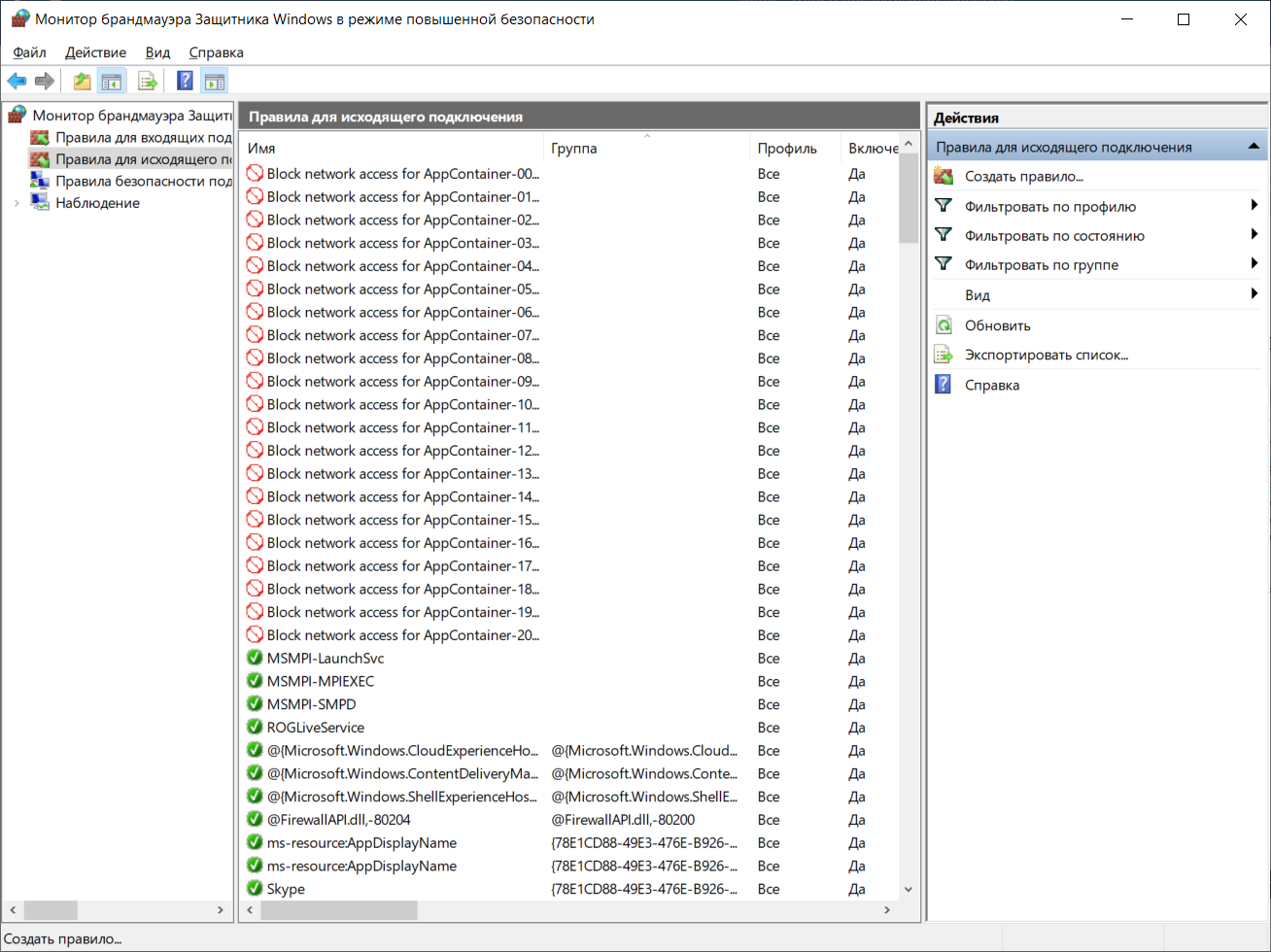


Рисунок 16 – Создание правила

* 1. Для 1 программы (по выбору) на блокировку подключения;

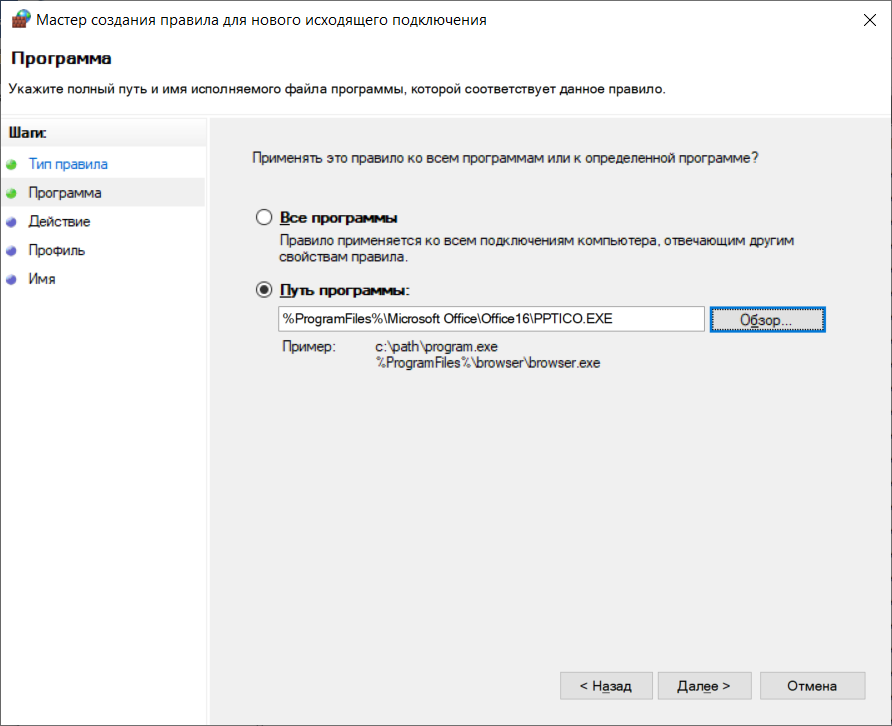


Рисунок 17 – Настройка пути программы

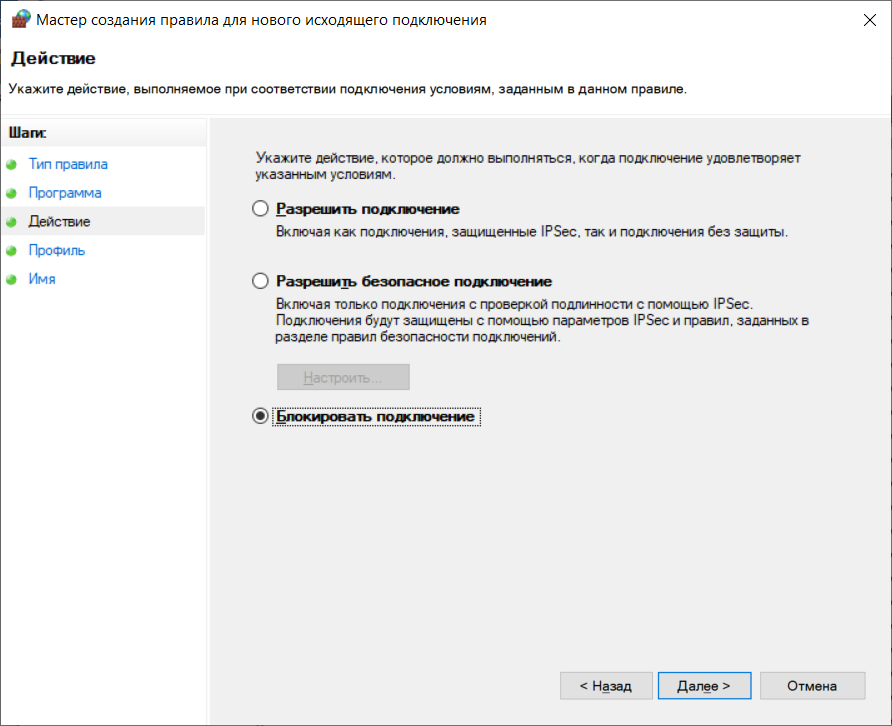


Рисунок 18 – Выбор действия

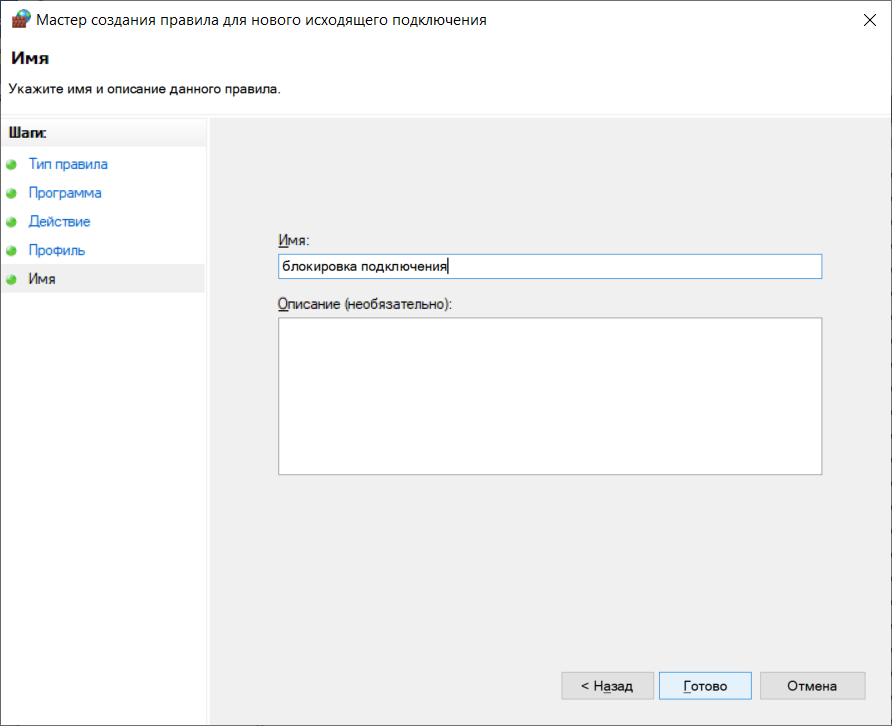


Рисунок 19 – Окно ввода имени

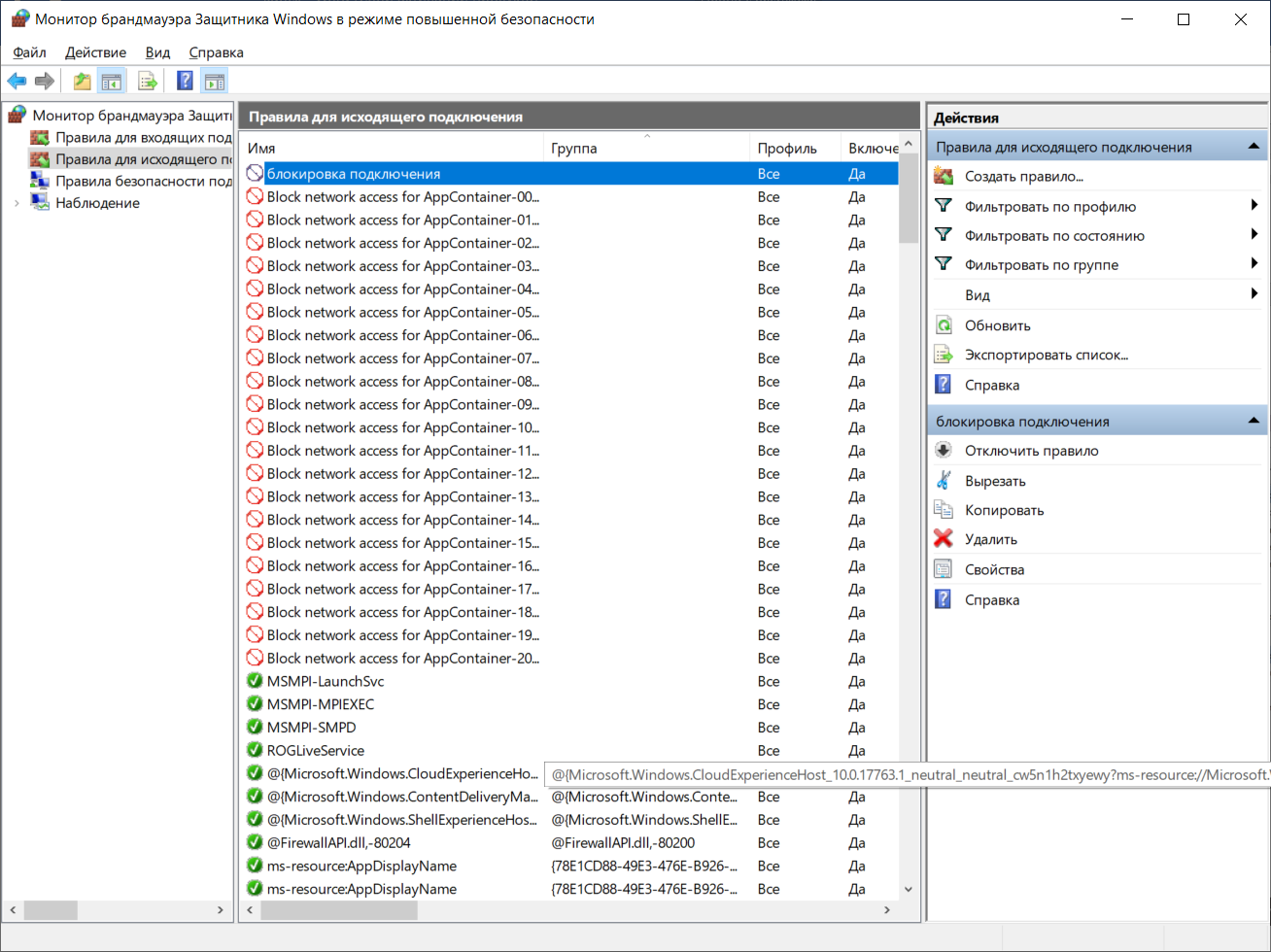
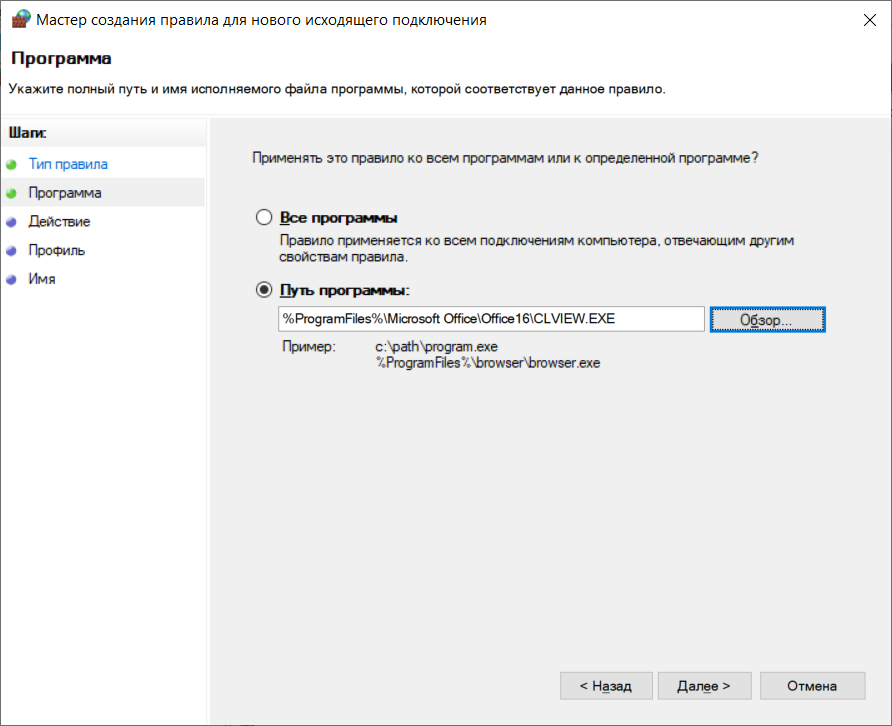
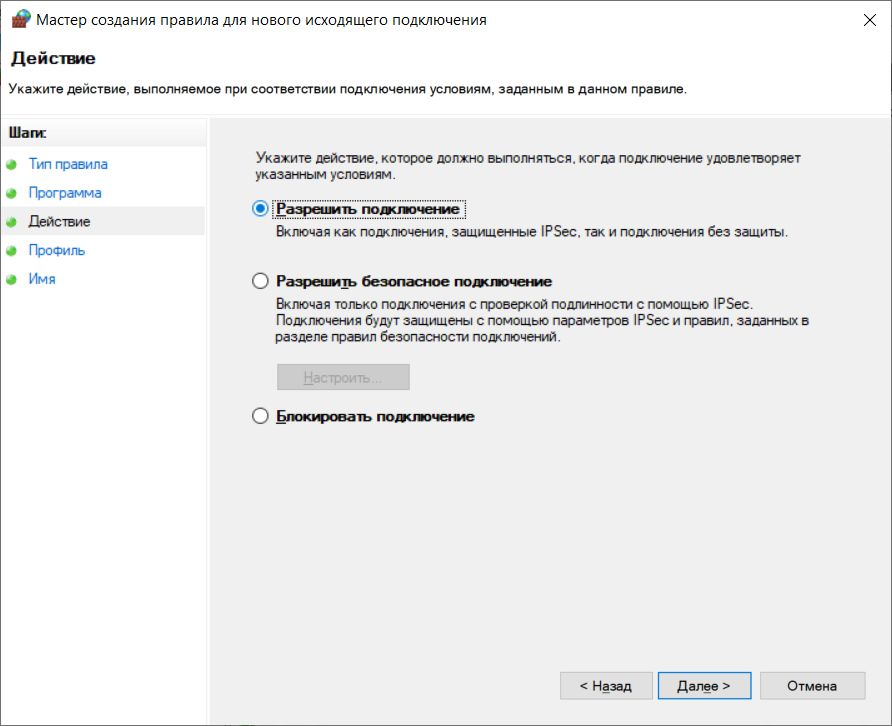
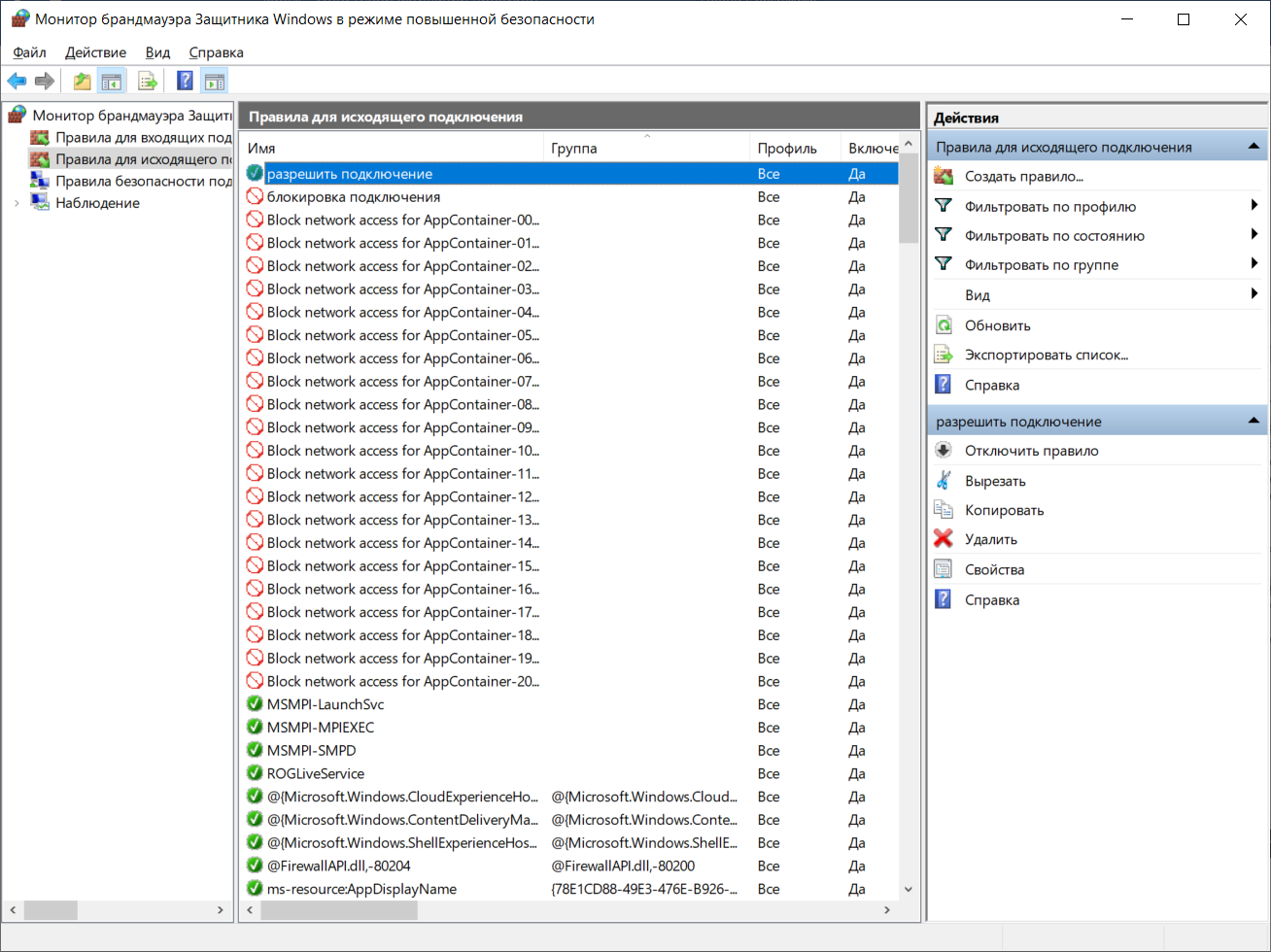


Рисунок 20 – Созданное правило

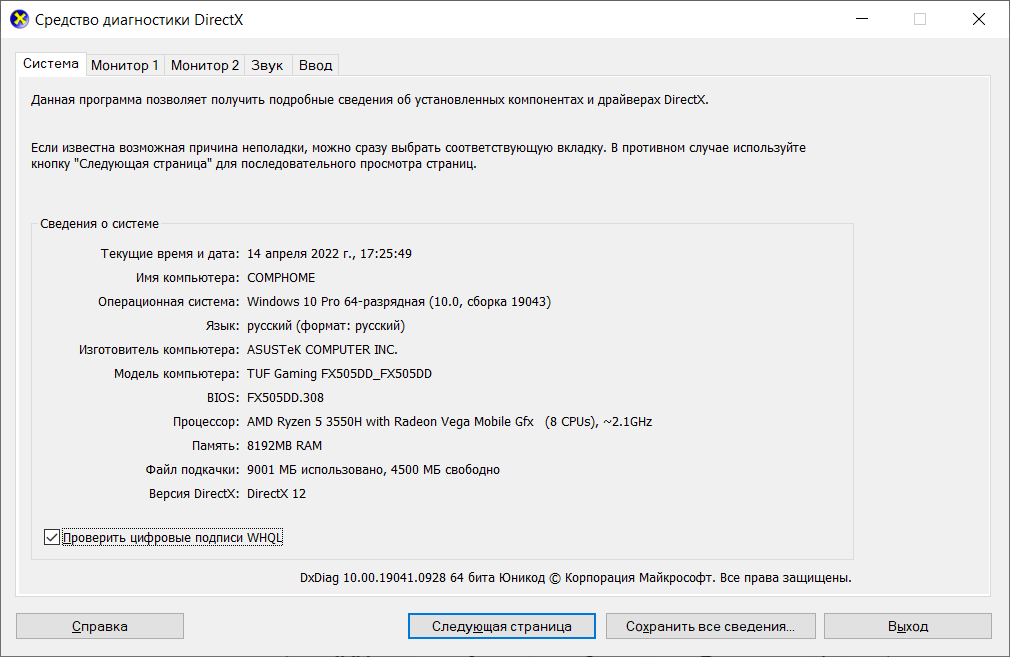
* 1. Для 1 программы (по выбору) на разрешение подключения;







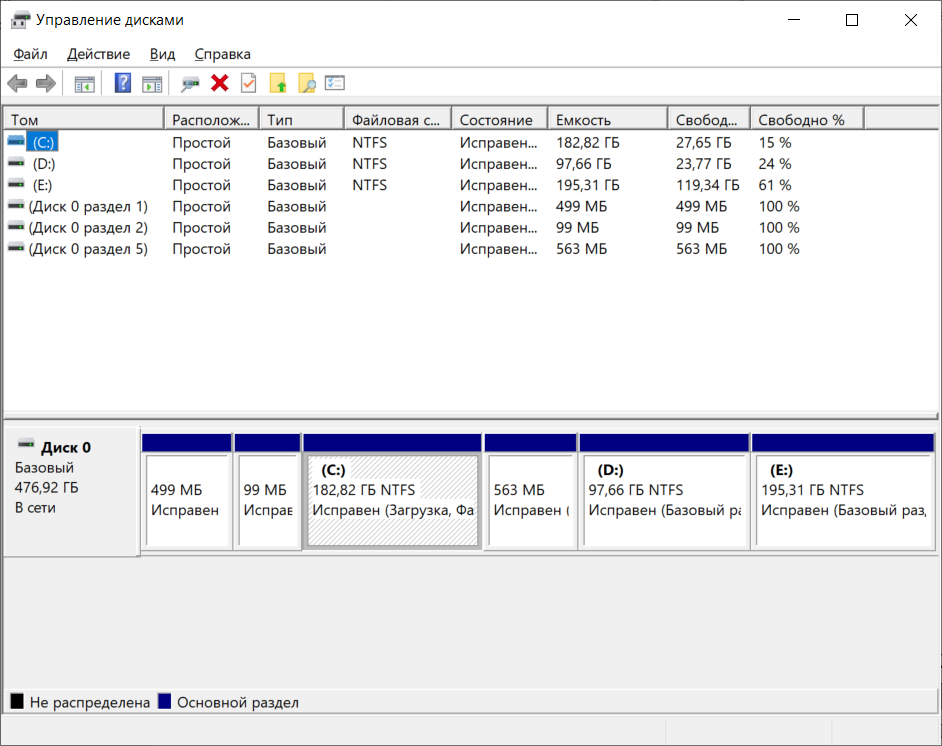
1. Вернуть настройки Брандмауэра в исходное состояние до начала выполнения практического задания.
2. Опробовать действие нескольких команд (с помещением в электронный конспект копий экрана с пояснениями действий).



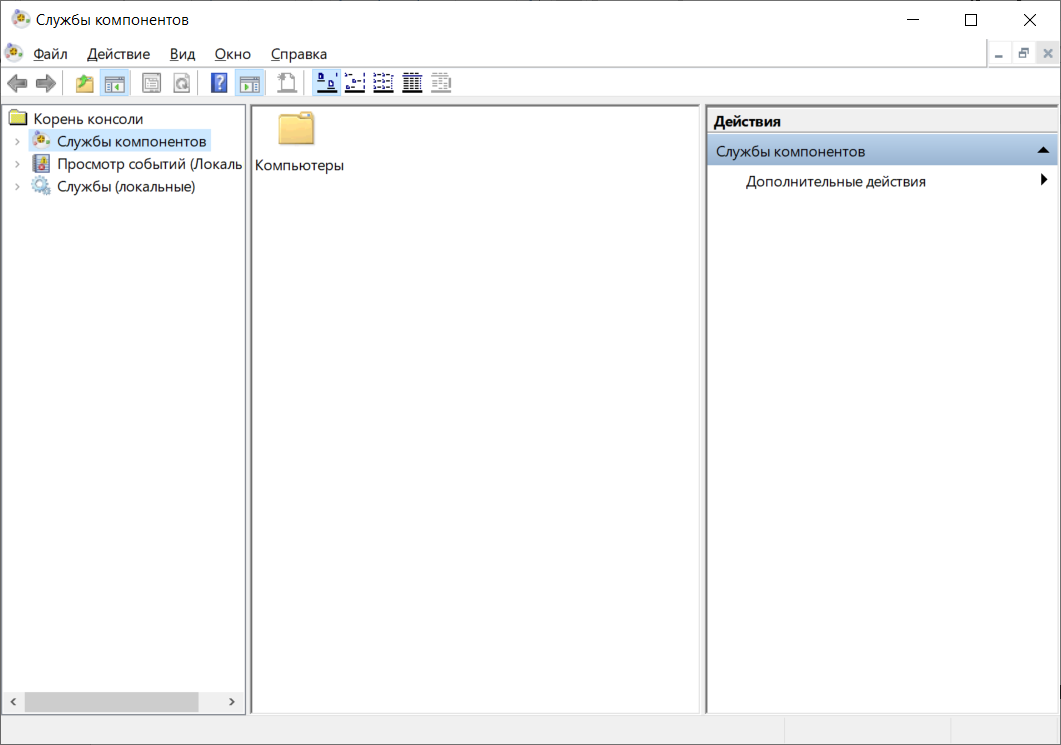
Служба диагностики DirectX-dxdiag



Калькулятор-calc



Управление дисками-diskmgmt.msc



Службы компонентов-dcomcnfg

**Вывод:** Я овладела навыками настройки и использования Брандмауэра Windows. Создала правила для входящих и исходящих подключений на разрешение и блокировку подключения.

# **Практическое занятие №5**

**Тема «Криптографическая защита информации»**

**Цель работы:** Овладение основными криптографическими алгоритмами симметричного шифрования .

**Криптография** - наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним) и аутентичности (целостности и подлинности авторства) информации.

**Сообщение:** Гринцевич Юлия Сергеевна

**Ключ:** 5

**Шифр Цезаря:** Зхнтыйжнь Грнд Цйхзййжте

Шифр Цезаря — это вид шифра подстановки, в котором каждый символ в открытом тексте заменяется символом находящимся на некотором постоянном числе позиций левее или правее него в алфавите.

**Шифр Трисемуса:** Йцдуьлждэ Фрдщ Члцйллжув

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **з** | **а** | **щ** | **и** | **т** |
| б | в | г | д | е |
| ё | ж | й | к | л |
| м | н | о | п | р |
| с | у | ф | х | ц |
| ч | ш | ъ | ы | ь |
| э | ю | я |  |  |

**Ключевое слово:** Защита

Таблица Трисемуса заполняется с помощью ключевого слова, повторяющиеся буквы которого отбрасываются. Затем таблица дополняется не вошедшими в нее буквами алфавита по порядку как в системе Цезаря с ключевым словом. Таким образом, ключом в таблицах Трисемуса является ключевое слово и размер таблицы.

**Шифр Плейфейра:** СВ ГС ФЖ ГЩ ЪЬ НА ИЦ ЁП БЖ ЁБ ИЛ

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

ГР ИН ЦЕ ВИ ЧЮ ЛИ ЯС ЕР ГЕ ЕВ НА

СВ ГС ФЖ ГЩ ЪЬ НА ИЦ ЁП БЖ ЁБ ИЛ

1. Если символы биграммы исходного текста встречаются в одной строке, то эти символы замещаются на символы, расположенные в ближайших столбцах справа от соответствующих символов. Если символ является последним в строке, то он заменяется на первый символ этой же строки.

2. Если символы биграммы исходного текста встречаются в одном столбце, то они преобразуются в символы того же столбца, находящимися непосредственно под ними. Если символ является нижним в столбце, то он заменяется на первый символ этого же столбца.

3. Если символы биграммы исходного текста находятся в разных столбцах и разных строках, то они заменяются на символы, находящиеся в тех же строках, но соответствующие другим углам прямоугольника.

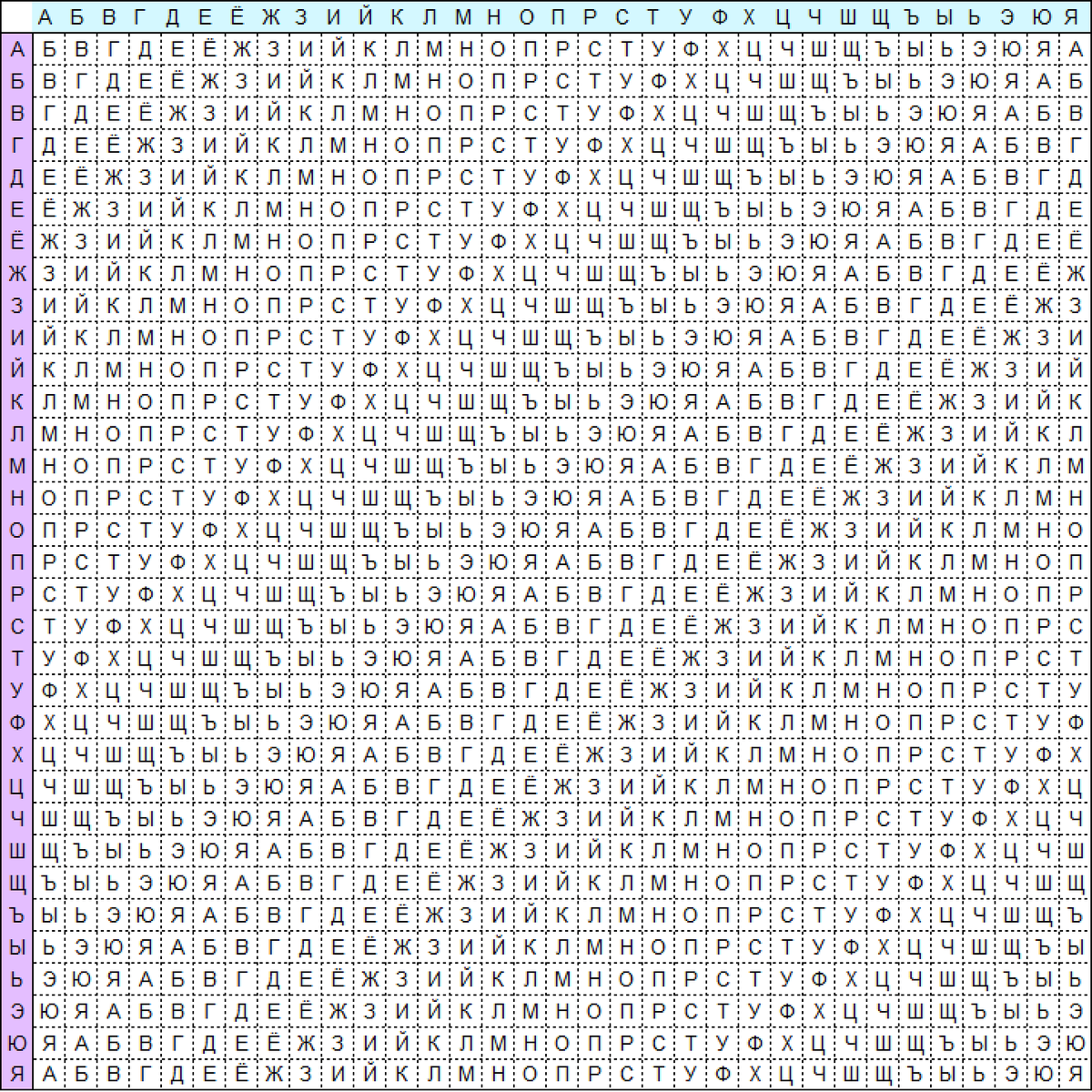
**Шифр Виженера:** ЛСГЧЙЁКЙС ЗЯЙЗ ТЯЪЦЁЁГЗЙ

Шифр Виженера — метод полиалфавитного шифрования буквенного текста с использованием ключевого слова.

Г Р И Н Ц Е В И Ч Ю Л И Я С Е Р Г Е В Н А

З А Щ И Т А З А Щ И Т А З А Щ И Т А З А Щ И

Л С Г Ч Й Ё К Й С З Я Й З Т Я Ъ Ц Ё Ё Г З Й



|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 5 | **тяеонаыбиьсрль\_т** | Расшифровать с помощью **Магического квадрата**   |  |  |  |  | | --- | --- | --- | --- | | 9 | 16 | 2 | 7 | | 6 | 3 | 13 | 12 | | 15 | 10 | 8 | 1 | | 4 | 5 | 11 | 14 |  |  |  |  |  | | --- | --- | --- | --- | | Т | Я | Е | О | | Н | А | Ы | Б | | И | Ь | С | Р | | Л | Ь |  | Т | |

ОТВЕТ : РЕАЛЬНОСТЬ БЫТИЯ

# **Практическое занятие №6**

**Тема «Криптографическая защита информации»**

**Цель** **работы**: Овладение основными криптографическими алгоритмами асимметричного шифрования.

**Задание 1.** Рассказать процесс работы алгоритма RSA.

**RSA (аббревиатура от фамилий Rivest, Shamir и Adleman)** – криптографический алгоритм с открытым ключом. Основывающийся на вычислительной сложности задачи факторизации больших целых чисел. Криптосистема RSA стала первой системой, пригодной и для шифрования, и для цифровой подписи.

**Алгоритм состоит из следующих этапов:**

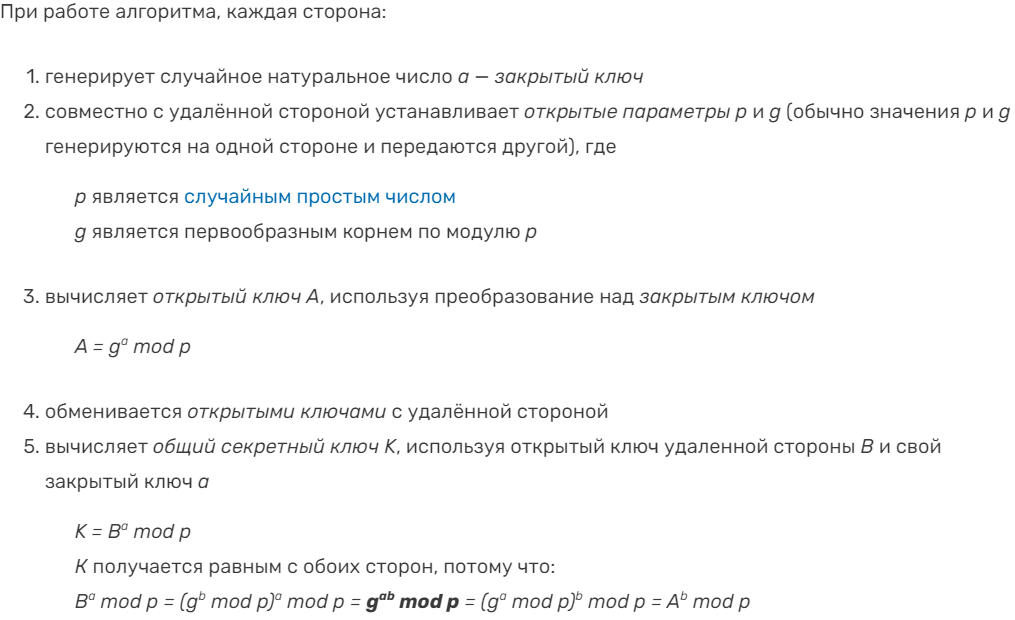
1.Генерация ключей (выбрать два простых различных числа, вычислить модуль (произведение), вычислить функцию Эйлера, выбрать открытую экспоненту, вычислить секретную экспоненту, опубликовать открытый ключ, сохранить закрытый ключ)

2.Шифрование (выбрать текст для зашифровки, вычислить шифротекст)

3.Расшифрование (вычислирть исходное сообщение)

**Задание 2. Рассказать процесс работы алгоритма Диффи-Хеллмана.**

Алгори́тм Ди́ффи — Хе́ллмана (англ. Diffie-Hellman, DH) — алгоритм, позволяющий двум сторонам получить общий секретный ключ, используя незащищенный канал связи. Этот ключ может быть использован для шифрования дальнейшего обмена с помощью алгоритма симметричного шифрования.



Алгоритм Диффи-Хелмана, обеспечивая конфиденциальность передачи ключа, не может гарантировать того, что он прислан именно тем партнером, который предполагается. Для решения этой проблемы был предложен протокол STS (station-to-station). Этот протокол для идентификации отправителя использует технику электронной подписи. Подпись шифруется общим секретным ключом, после того как он сформирован. Подпись включает в себя идентификаторы как *P1*, так и *P2*.

1. Два участника обмена договариваются о двух числах. Один выбирает большое простое число, а другой – целое число, меньшее числа первого участника. Переговоры они могут вести открыто, и это никак не отразится на безопасности.

2.Каждый из двух участников, независимо друг от друга, генерирует другое число, которое они будут хранить в тайне. Эти числа выполняют роль секретного ключа. Далее в вычислениях используются секретный ключ и два предыдущих целых числа. Результат вычислений посылается участнику обмена, и он играет роль открытого ключа.

3.Участники обмена обмениваются открытыми ключами. Далее они, используя собственный секретный ключ и открытый ключ партнера, конфиденциально вычисляют ключ сессии. Каждый партер вычисляет один и тот же ключ сессии.

**Задание 3**. Рассказать процесс работы алгоритма Эль-Гамаля.

1. Генерируется случайное простое число ~p длины ~n [битов](https://ru.wikipedia.org/wiki/%D0%91%D0%B8%D1%82).
2. Выбирается случайный примитивный элемент ~g.
3. Выбирается случайное целое число ~x такое, что ~1 < x < p-1.
4. Вычисляется ~y = g^x\,\bmod\,p.
5. Открытым ключом является тройка \left( p,g,y \right), закрытым ключом — число ~x.

**Шифрование**

Сообщение ~M шифруется следующим образом:

Выбирается сессионный [ключ](https://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D1%8E%D1%87_(%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F)) — случайное целое число ~k такое, что ~1 < k < p - 1

Вычисляются числа a = g^k\,\bmod\,p и b = y^k M\,\bmod\,p.

Пара чисел \left( a, b \right) является [шифротекстом](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D1%82%D0%B5%D0%BA%D1%81%D1%82).

Нетрудно видеть, что длина шифротекста в схеме Эль-Гамаля длиннее исходного сообщения M вдвое.

**Расшифрование**

Зная закрытый ключ ~x, исходное сообщение можно вычислить из шифротекста \left( a, b \right) по формуле:

M = b(a^x)^{-1}\,\bmod\,p.

# **Практическое занятие №7**

**Тема «Криптографическая защита информации»**

Цель: Овладение основными криптографическими алгоритмами асимметричного шифрования .

**1.Электронная цифровая подпись** – реквизит электронного документа, предназначенный для защиты данного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа ЭЦП и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе (Федеральный закон "Об электронной цифровой подписи").

При создании цифровой подписи по классической схеме отправитель:

* применяет к исходному сообщению **T** хеш-функцию **h(T)** и получает хеш-образ r сообщения;
* вычисляет цифровую подпись **s по хеш-образу r с использованием своего закрытого ключа**;
* посылает сообщение **T** вместе с цифровой подписью s получателю.

Получатель, отделив цифровую подпись от сообщения, выполняет следующие действия:

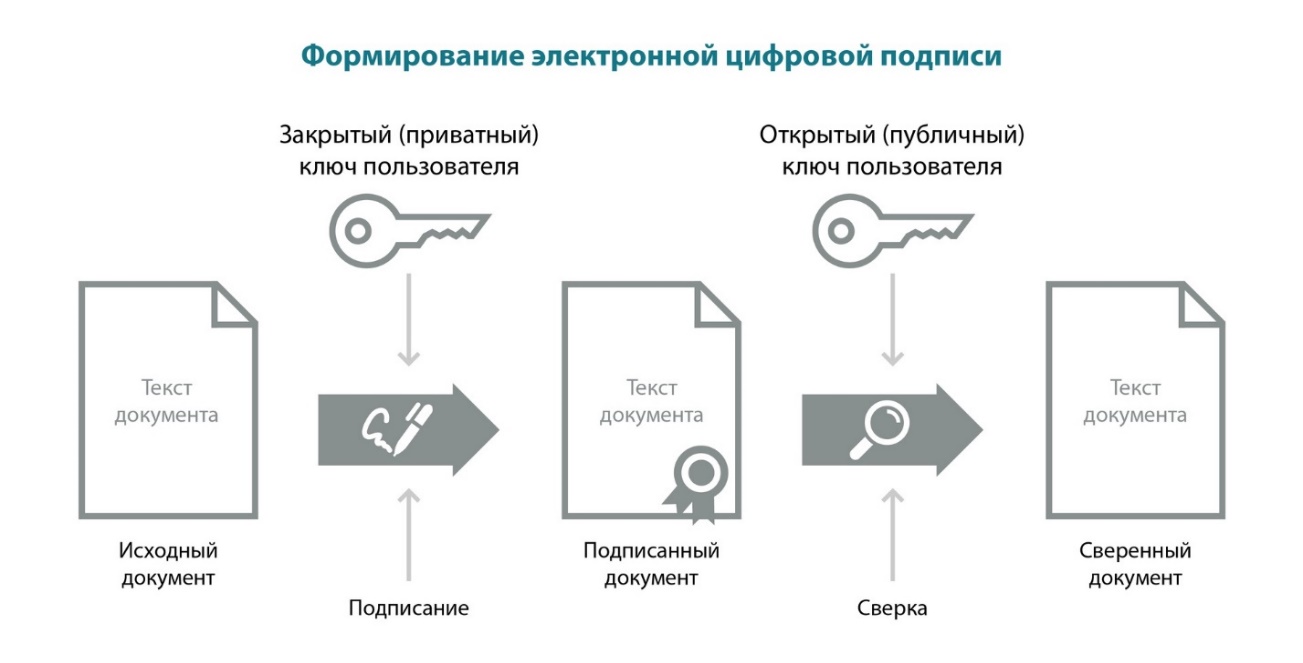
* применяет к полученному сообщению **T** хеш-функцию **h(T)** и получает хеш-образ **r** сообщения;
* расшифровывает хеш-образ **r’** из цифровой подписи s с использованием открытого ключа отправителя;
* проверяет соответствие хеш-образов r и r’ и если они совпадают, то отправитель действительно является тем, за кого себя выдает, и сообщение при передаче не подверглось искажению.

Как видно из этой схемы, порядок использования ключей обратный тому, который используется при передаче секретных сообщений. **Вначале отправитель использует свой закрытый ключ, а затем получатель применяет открытый ключ отправителя.**

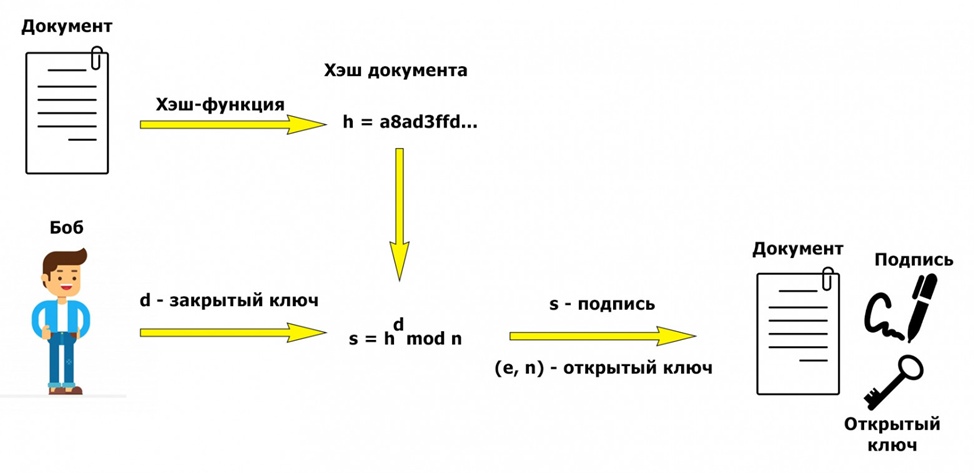
**Разновидности ЭЦП**

Кроме классической схемы ЭЦП различают еще несколько специальных:

* схема "конфиденциальной" (неотвергаемой) подписи – подпись не может быть проверена без участия сгенерировавшего ее лица;
* схема подписи "вслепую" ("затемненной" подписи) - отправитель не знает подписанного им сообщения;
* схема "мультиподписи" - вместо одного отправителя сообщение подписывает группа из нескольких участников;
* схема "групповой" подписи - получатель может проверить, что подписанное сообщение пришло от члена некоторой группы отправителей, но не знает, кем именно из членов группы оно подписано. В тоже время, в случае необходимости, отправитель может быть определен;

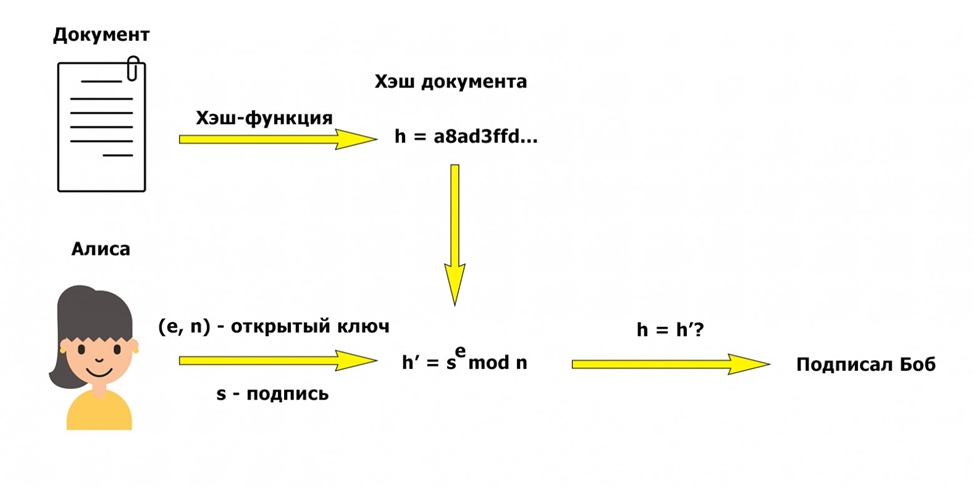


**Подпись:**



получаешь хэш документа ,хэш + формула s по ключам = подпись

**Расшифровка:**



# **Практическое занятие №8**

**Тема «Криптографическая защита информации»**

**Цель** **работы**: получение основных сведений из курса теории чисел

**Вариант 6**

1-3. *а* = 5336161097, *b* = 196210799. .

Найти остаток от деления  на 19.

**Задание 1.** Найти канонические разложения чисел

*а* = 5336161097, *b* = 196210799

5336161097

67546343

855017

10823

137

1

| 79

| 79

| 79

| 79

| 137

| 1

196210799

2483681

31439

211

1

| 79

| 79

| 149

| 211

| 1

**Итог**: *а* = 5336161097=(79^4)\*137, *b* = 196210799=(79^2)\*149\*211

**Задание 2.** Найти НОД (5336161097,196210799) пользуясь

а) алгоритмом Евклида,

5336161097=196210799\*27+38469524

196210799=38469524\*5+3863179

38469524=3863179\*9+3700913

3863179=3700913+162266

3700913=162266\*22+131061

162266=131061+31205

131061=31205\*4+6241

31205=6241\*5

Найти НОД (5336161097,196210799)=6241

б) разложением чисел на простые множители.

Разложим числа на простые множители и подчеркнем общие множители чисел:

5336161097 = 79 · 79 · 79 · 79 · 137

196210799 = 79 · 79 · 149 · 211

Общие множители чисел: 79; 79

Чтобы найти НОД чисел, необходимо перемножить их общие множители:

НОД (5336161097; 196210799) = 79 · 79 = 6241

**Задание 3**. С помощью расширенного алгоритма Евклида найти целые числа u,v, удовлетворяющие соотношению Безу:  для целых чисел *а* = 5 336 161 097, *b* = 196 210 799.

Имея НОД наших чисел НОД (5336161097;196210799)=6241 найдем соотношение Безу:

5336161097=196210799\*27+38469524

38469524=5336161097+196210799\*(-27)

196210799=38469524\*5+3863179

3863179=196210799+38469524\*(-5)

38469524=3863179\*9+3700913

3700913=38469524+3863179\*(-9)

3863179=3700913+162266

162266=3863179+3700913\*(-1)

3700913=162266\*22+131061

131061=3700913+162266\*(-22)

162266=131061+31205

31205=162266+131061\*(-1)

131061=31205\*4+6241

6241=131061+31205\*(-4)

6241=131061+31205\*(-4)= 131061-(162266-131061)\*4=

=131061\*5-162266\*4= (3700913+162266\*(-22))\*5-162266\*4 =

= 3700913\*5-162266\*114= 3700913\*5-(3863179+3700913\*(-1))\*114 =

= 3700913\*119-3863179\*114= (38469524+3863179\*(-9))\*119-3863179\*114=

=38469524\*119-3863179\*1185= 38469524\*119-(196210799+38469524\*(-5))\*1185=

=38469524\*6044-196210799\*1185=(5336161097+196210799\*(-27)) \*6044-196210799\*1185=

=5336161097\*6044-196210799\*164373

AU=5336161097\*6044

BV=196210799\*(-164373)

**ЗАДАНИЕ №4:** Найти остаток от деления  на 19.

1998 делится на 19 с остатком 3. 1998^2 делится на 19 с остатком 9. Далее достаточно на 1998 умножить только остаток и делать выводы. 1998^3 делится на 19 с остатком 8, … 5… 15 … 7 … 2 … 6 … 18 … 16 … 10 … 11 … 14 … 4 … 12 … 17 … 13 … 1, 1998^19 делится на 19 с остатком 3. Получили один из предыдущих остатков, значит «зациклились». Число 1998^19 дает тот же остаток деления на 19, что и 1998. Значит, длина цикла равна 18. 2001=18\*111+3 Число  дает тот же остаток от деления на 19, что и 1998^3, то есть 8.

# **Практическое занятие №9**

**Тема «**Авторское право и смежные права**»**

**Цель:** Изучить основные положения авторского права и смежных прав.

1. **На какие объекты распространяется авторское право?**

**Авторское** **право**-**это** вид интеллектуальной собственности, дающий ее владельцу исключительное **право** делать копии творческого произведения, как правило, в течение ограниченного времени.

Авторское право распространяется на такие объекты как

-Произведения (литературные, научные, драматические, музыкальные и т.д.)

-Производные произведения (переводы, обработки, аннотации, сборники произведений)

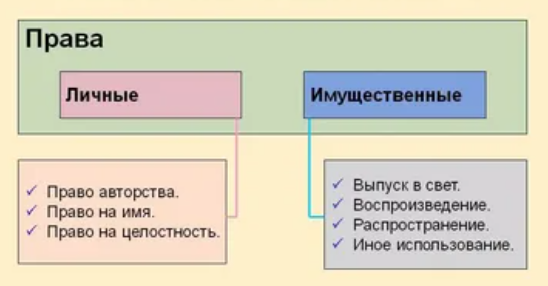
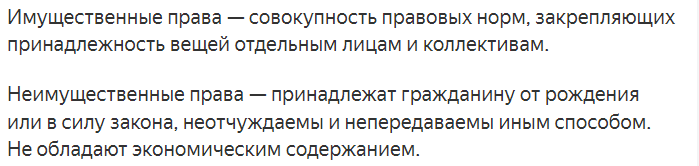
-Компьютерные программы (прикладные программы, ОС, базы данных и т.д.)

1. **Что относится к личным неимущественным правам?**

*Личные неимущественные права:*

* признаваться автором произведения (право авторства);
* использовать или разрешать использовать произведение под подлинным именем автора, псевдонимом либо без обозначения имени, т.е. анонимно (право на имя);
* обнародовать или разрешать обнародовать произведение в любой форме (право на обнародование), включая право на отзыв;
* право на защиту произведения, включая его название, от всякого рода искажении или любого иного посягательства, способных нанести ущерб чести и достоинству автора (право на защиту репутации автора)(На целостность)

Принадлежат автору независимо от его имущественных прав и сохраняются за ним даже после уступки исключительных прав на использование произведения.



1. **Что относится к личным имущественным правам?**

*Имущественные права: исключительное право осуществлять или разрешать осуществлять следующие действия:*

* воспроизведение произведения;
* распространение оригинала или экземпляров произведения посредством продажи, или иной передачи права собственности;
* прокат оригиналов или экземпляров компьютерных программ, баз данных, аудиовизуальных произведений, нотных текстов музыкальных произведений и произведений, воплощенных в фонограммах;
* импорт экземпляров произведения;
* публичный показ оригинала или экземпляра произведения;
* публичное исполнение произведения;
* передачу произведения в эфир;
* иное сообщение произведения для всеобщего сведения;
* перевод произведения на другой язык;
* переделку или иную переработку произведения.

1. Каковы особенности авторского права на составные произведения?

* Автору сборника и других составных произведений (составителю) принадлежит авторское право на осуществленные им подбор и распоряжение материалов как результат творческого труда (составительство).
* Составитель пользуется авторским правом при условии соблюдения им прав авторов каждого из произведений, включенных в составное.
* Авторы произведений, включенных в составное произведение, вправе использовать свои произведения независимо от составного произведения, если иное не предусмотрено авторским договором.
* Авторское право составителя не препятствует другим лицам осуществлять самостоятельный подбор и расположение тех же материалов для создания своих составных произведений.
* Лицу, выпускающему в свет энциклопедии, энциклопедические словари, периодические и продолжающиеся сборники научных трудов, газеты, журналы и другие периодические издания, принадлежат исключительные права на использование таких изданий в целом. Это лицо вправе при любом использовании таких изданий указывать свое наименование или требовать такого указания.
* Авторы произведений, включенных в такие издания, сохраняют исключительные права на использование своих произведений независимо от издания в целом, если иное не предусмотрено авторским договором.

1. Каков срок действия авторского права?

Право авторства, право на имя и право на защиту репутации автора охраняются бессрочно. Имущественные права действуют в течение всей жизни автора (соавторов) и 50 лет после его (последнего соавтора) смерти.

Общественное достояние по истечении срока действия имущественных прав на объекты авторского права или смежных прав означает переход этих объектов в общественное достояние и может свободно использоваться любым физическим или юридическим лицом без выплаты вознаграждения.

Переход авторского права по наследству, кроме прав авторства, на имя и на защиту репутации автора без ограничения срока.

1. **Кто является субъектом авторского права?**

Субъектом авторского права, как правило, является гражданин, творческим трудом которого создано произведение науки, литературы или искусства. Им может быть и гражданин, не достигший восемнадцатилетнего возраста и душевнобольной. Так, авторские права детей, представленные на смотры или выставки детской или юношеской самодеятельности и т.д. защищаются авторским правом.

1. **Что такое авторский договор?**

Договор, который разрешает использование произведения определенным способом и в установленных договором пределах только лицу, которому эти права передаются, и дает такому лицу право запрещать подобное использование произведения другим лицам.

1. **Наиболее распространенные виды авторских договоров?**

-изобретательский,

-постановочный,

-сценарный,

-художественного заказа,

-об использовании в промышленности неопубликованного произведения декоративно-прикладного искусства.

1. **Основные составляющие авторского договора?**

Авторский договор должен предусматривать

-способы использования произведения (конкретные права, передаваемые по данному договору);

-срок, на который передается право, и территорию, на которую распространяется действие этого права на указанный срок;

-размер вознаграждения и (или) порядок определения размера вознаграждения за каждый способ использования произведения, порядок и сроки его выплаты

-территория, на которой может осуществляться использование;

# **Практическое занятие №10**

**«Составление и оформление заявок на объекты промышленной собственности»**

**Цель:** овладеть навыками составления и оформления заявок на объекты промышленной собственности.

**Ответы на вопросы**

1. **Основные составляющие описания изобретения.**

* область техники, к которой относится изобретение;
* уровень техники;
* сущность изобретения;
* перечень фигур чертежей, если они прилагаются с кратким указанием на то, что изображено на каждой из них. Если представлены иные материалы, поясняющие сущность изобретения, то перечисляют их;
* сведения, подтверждающие возможность осуществления изобретения.

Свидетельство - это выдаваемый патентным органом от имени государства документ, который удостоверяет авторство, приоритет на объект промышленной собственности и исключительное право на его использование.

1. **Правила оформления описания изобретения.**

* названия разделов в тексте описания не указываются;
* не допускается замена раздела «Описание» в целом или его части отсылкой к источнику, в котором находятся необходимые сведения. При этом оценка новизны и изобретательского уровня осуществляется в сравнении с уровнем техники для определения, которого проводится информационный поиск;
* источники с общедоступной информацией об изобретении раскрытые автором прямо или косвенно не включаются, если раскрытие осуществлено не позднее 12 месяцев до даты подачи заявки в патентный орган.

1. **Какие основные пункты должна содержать заявка на изобретение?**

* все части, узлы и детали, составляющие данную конструкцию и показанные на чертеже, пояснены их названия, связи и взаимное расположение;
* действие (работа) устройства или способ его использования со ссылкой на цифровые обозначения, ранее упомянутых частей, узлов, деталей;
* примеры описания этого устройства, если они имеются с характеристикой тех или иных преимуществ;
* сведение подтверждающие возможность описания изобретения, относящегося к способу включают указания на последовательность действий;
* если в формуле изобретения в качестве отличительных признаков приведены параметры режима;
* при описании способа, характеризующегося использованием неизвестных средств, указываются эти средства, и подтверждается их известность до даты Приоритета.

1. **Основные документы, необходимые для подачи заявки на изобретения.**

* документ, подтверждающий уплату патентной пошлины (отмеченная банком копия платежного поручения или квитанция банка), или документ, подтверждающий основания для освобождения от ее уплаты или уплаты в меньшем размере;
* доверенность, при подаче заявки через патентного поверенного;
* заверенная копия первой заявки, в случае подачи заявки в соответствии с Парижской конвенцией по охране промышленной собственности (конвенционная заявка).

1. **Отличия заявок на охранные документы различных объектов промышленной собственности.**

* заявление о выдаче патента с указанием автора (соавторов) промышленного образца и лица (лиц), на имя которого (которых) испрашивается патент, а также их местожительства и местонахождения;
* комплект изображений изделия (макета, рисунка), дающих полное и детальное представление о внешнем виде изделия;
* описание промышленного образца, включающее совокупность его существенных признаков;
* чертеж общего вида изделия, эргономическую схему, конфекционную карту, если они необходимы для раскрытия сущности промышленного образца.

1. **На какие ОПС(**объектов промышленной собственности**) выдаются патенты?**

* на полезную модель;
* на промышленный образец;
* на сорт растений;
* изобретение.

1. **На какие ОПС выдаются свидетельства?**

* свидетельство выдается на товарный знак;
* на географические указание на 10 лет с продлением;
* на регистрацию топологии интегральной микросхемы.

**Товарным знаком и знаком обслуживания** (далее — товарный знак) признается обозначение, способствующее отличию товаров или услуг одного лица от однородных товаров или услуг других лиц.

**Топология интегральной микросхемы** - зафиксированное на материальном носителе пространственно-геометрическое расположение совокупности элементов интегральной микросхемы и связей между ними.

**Географическое указание (ГУ)**- обозначение, идентифицирующее происходящий с территории географического объекта товар, определенное качество, репутация или другие характеристики которого в значительной степени связаны с его географическим происхождением (характеристики товара).

# **Практическое занятие №12**

**Тема «**MenuTracker**» —** Меню кафе

Цель: освоить навыки проведения патентного поиска по заданной тематике.

**Теоретическое введение**

Целью патентных исследований является определение уровня техники, который используется для проверки соответствия заявленного изобретения условиям патентоспособности «новизна» и «изобретательский уровень».

Патентное исследование проводится на основании формулы изобретения с учетом описания и чертежей, если они имеются, а также с учетом изменений формулы изобретения, принятых во внимание при рассмотрении заявки.

При определении уровня техники общедоступными считаются сведения, содержащиеся в источниках информации, с которыми любое лицо может ознакомиться сами либо о содержании которых ему может быть законным путем сообщено.

**Задание для выполнения.**

Провести патентный поиск по теме своего курсового проекта.

Для выявления патентной чистоты разработанного объекта промышленной собственности следует использовать следующий регламент поиска:

объект – *приложение MenuTracker;*

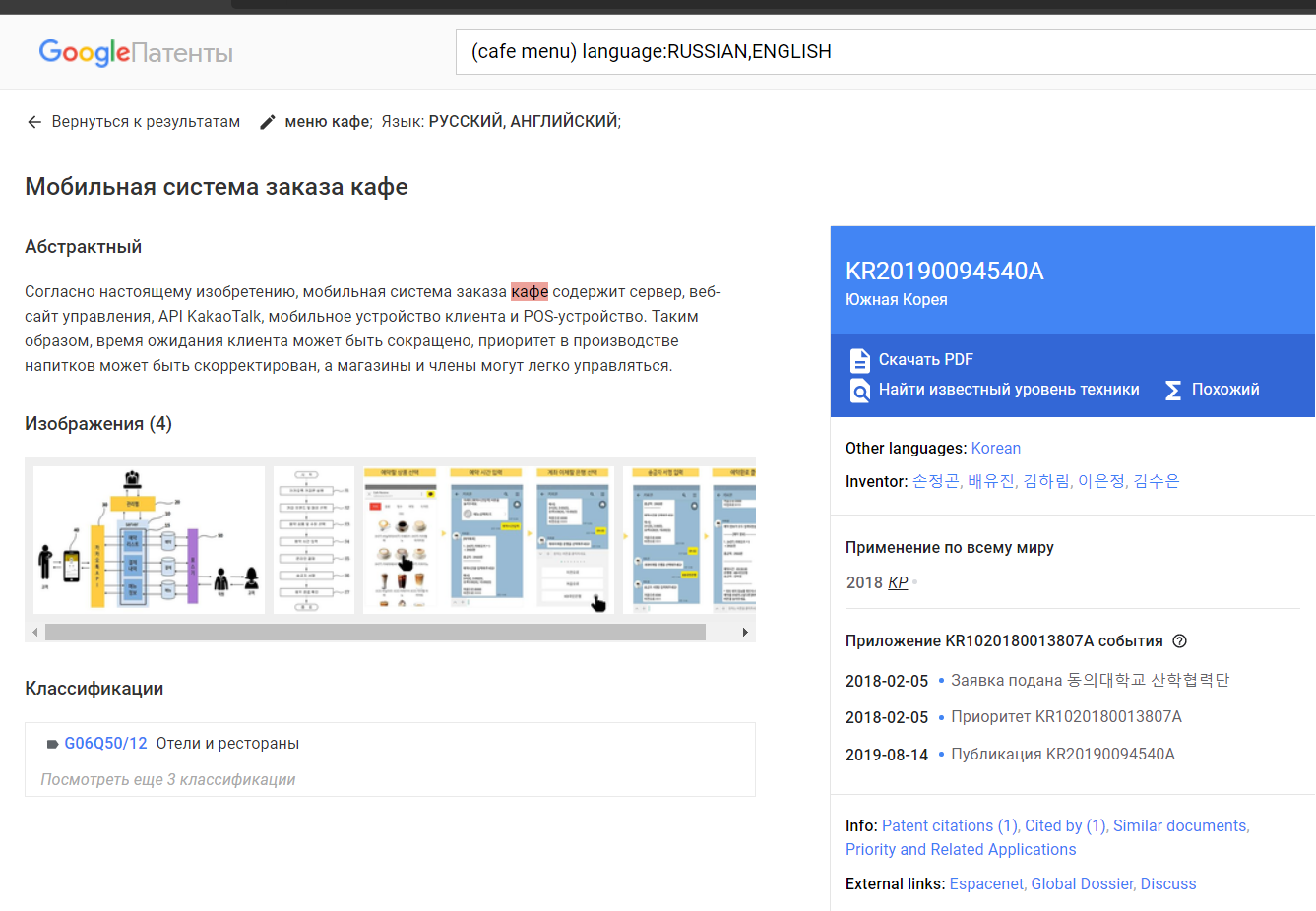
страна поиска – *Республика Беларусь*;

источники информации – *патентные*;

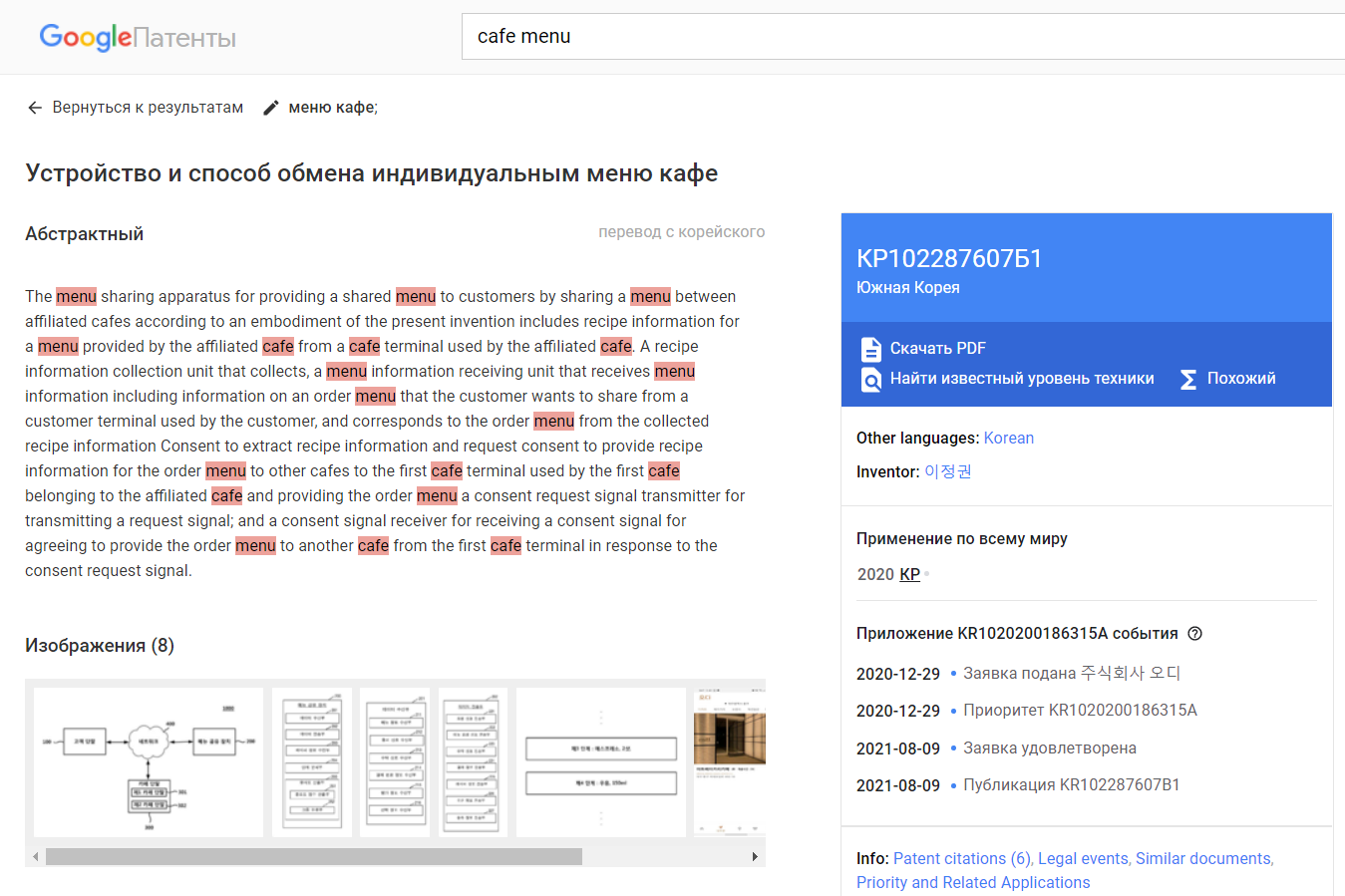
ретроспективность –*10 лет*;

**Информационная база** - *сайт национального центра интеллектуальной собственности:* *https://patents.google.com/patent*

Проведем поиск по необходимым параметрам. Результаты, схожие по своему функционалу, представлены на *рисунках* ниже.







|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Предмет поиска (объект исследования, его составные части) | Страна выдачи, вид и номер охранного документа. Классификационный индекс | Заявитель (патентообладатель), страна. Номер заявки, дата приоритета, конвенционный приоритет, дата публикации | Название изобретения (полезной модели, промышленного образца) | Сведения о действии охранного документа или причина его аннулирования (только для анализа патентной чистоты) |
| Меню кафе | KR20190094540A |  | Мобильная система заказа кафе | **Действует** |
| KR20160109378A |  | Аппарат и способ предоставления информации о кафе | **Действует** |
| КР102287607Б1 |  | Устройство и способ обмена индивидуальным меню кафе | **Действует** |

# **Практическое занятие №13**

**Тема «**Настройка антивирусов**»**

**Цель:** Овладеть навыками настройки и использования различных антивирусов.

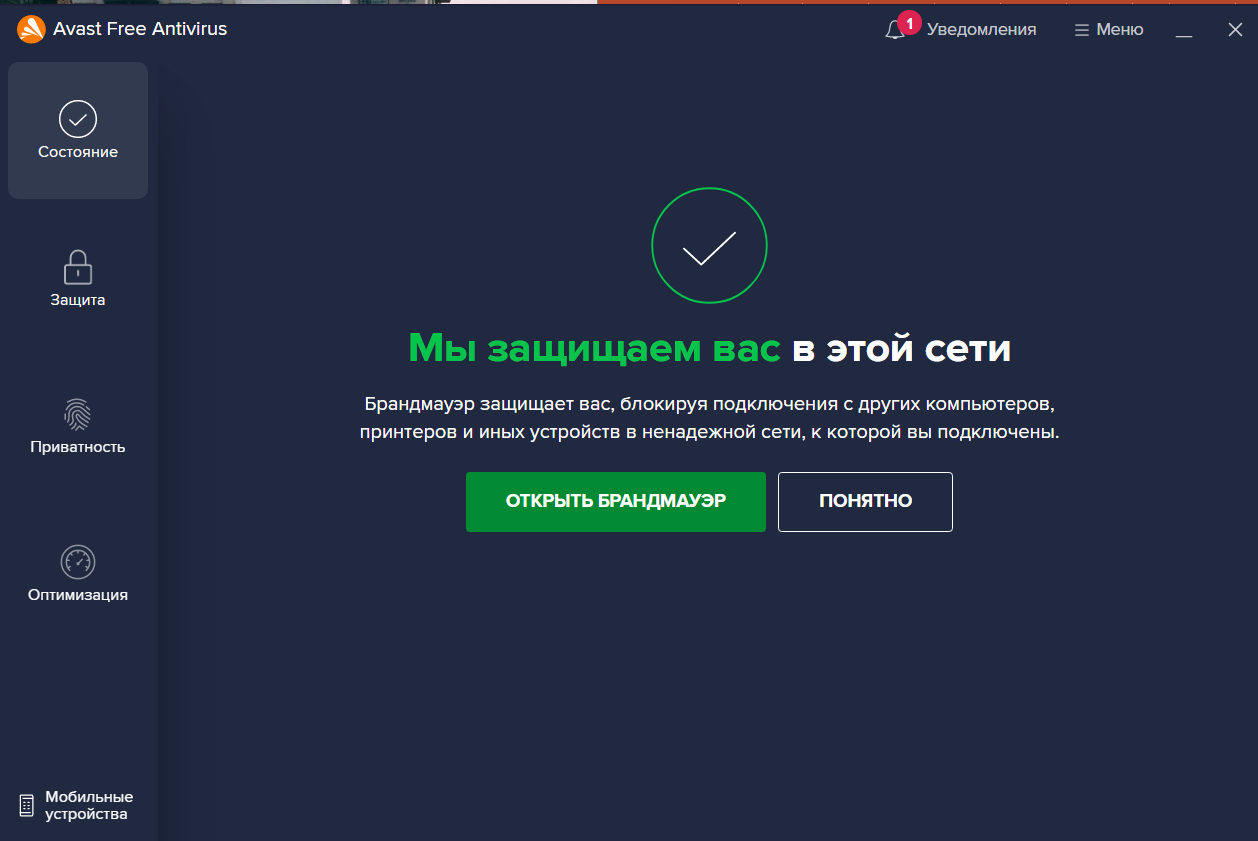
**Задание**

Установить и настроить антивирусную программу по варианту.

Обновить базу данных сигнатур вирусов.

Выполнить сканирование дисков.

Рассмотрим антивирусное программное обеспечение Avast Free Antiviru



Рис*.1* – Главный экран

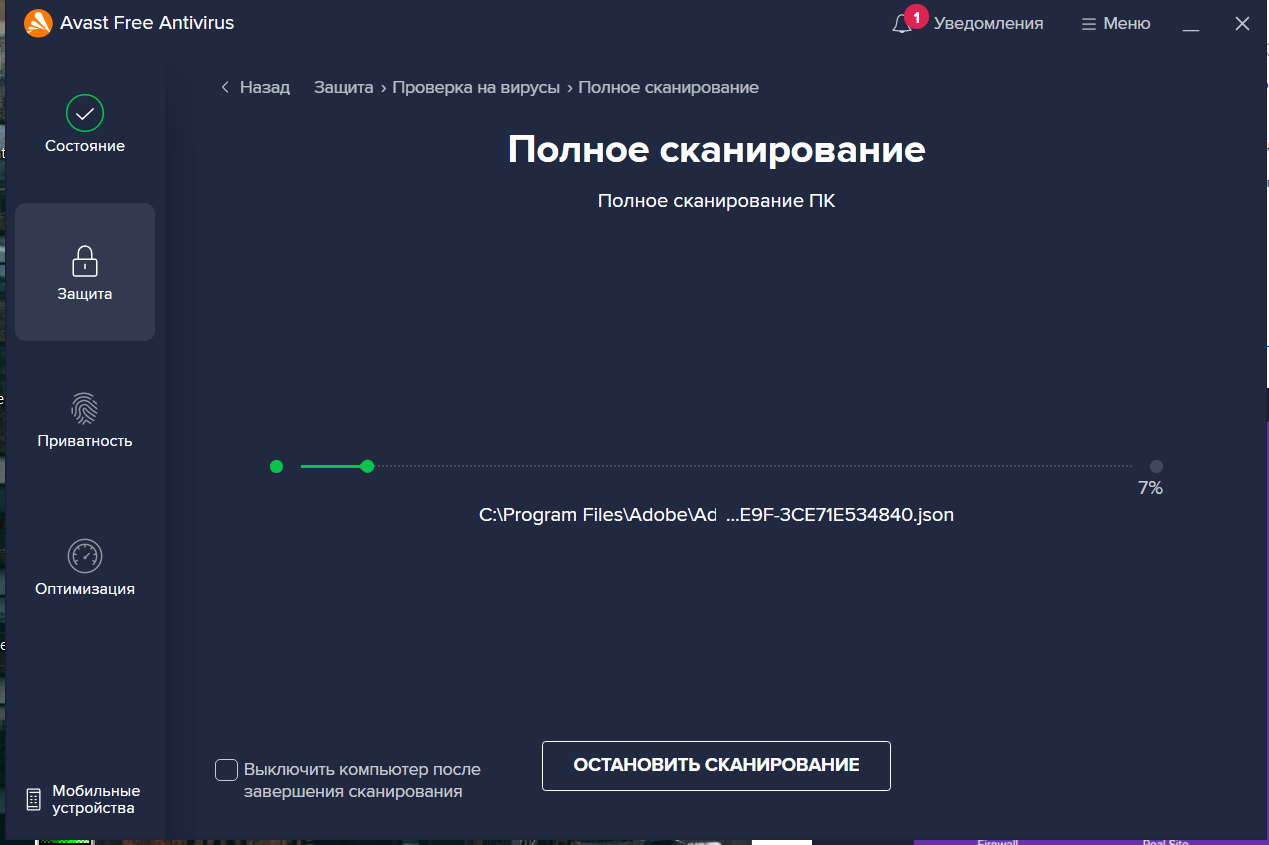


Рис.*2* – Полное сканирование ПК

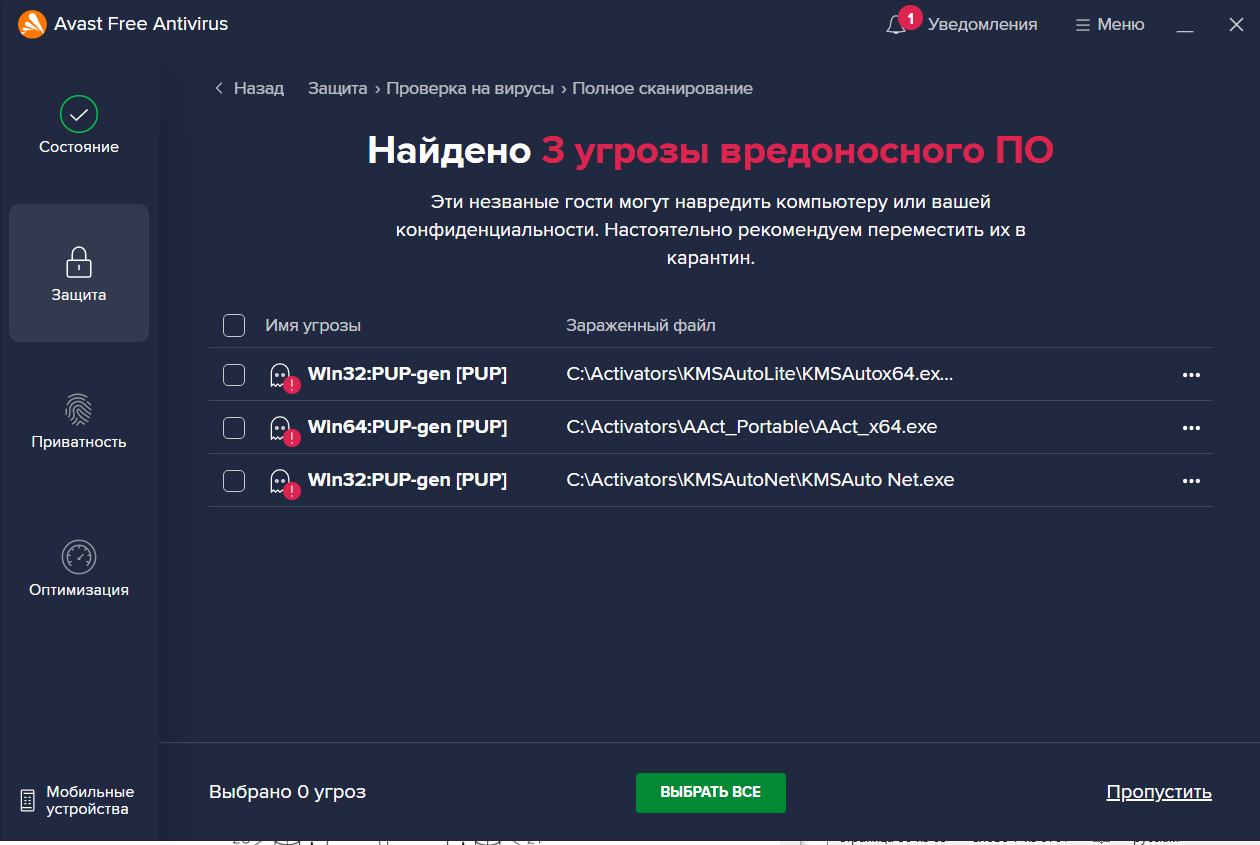


Рис.*3* – Результат полного сканирование ПК

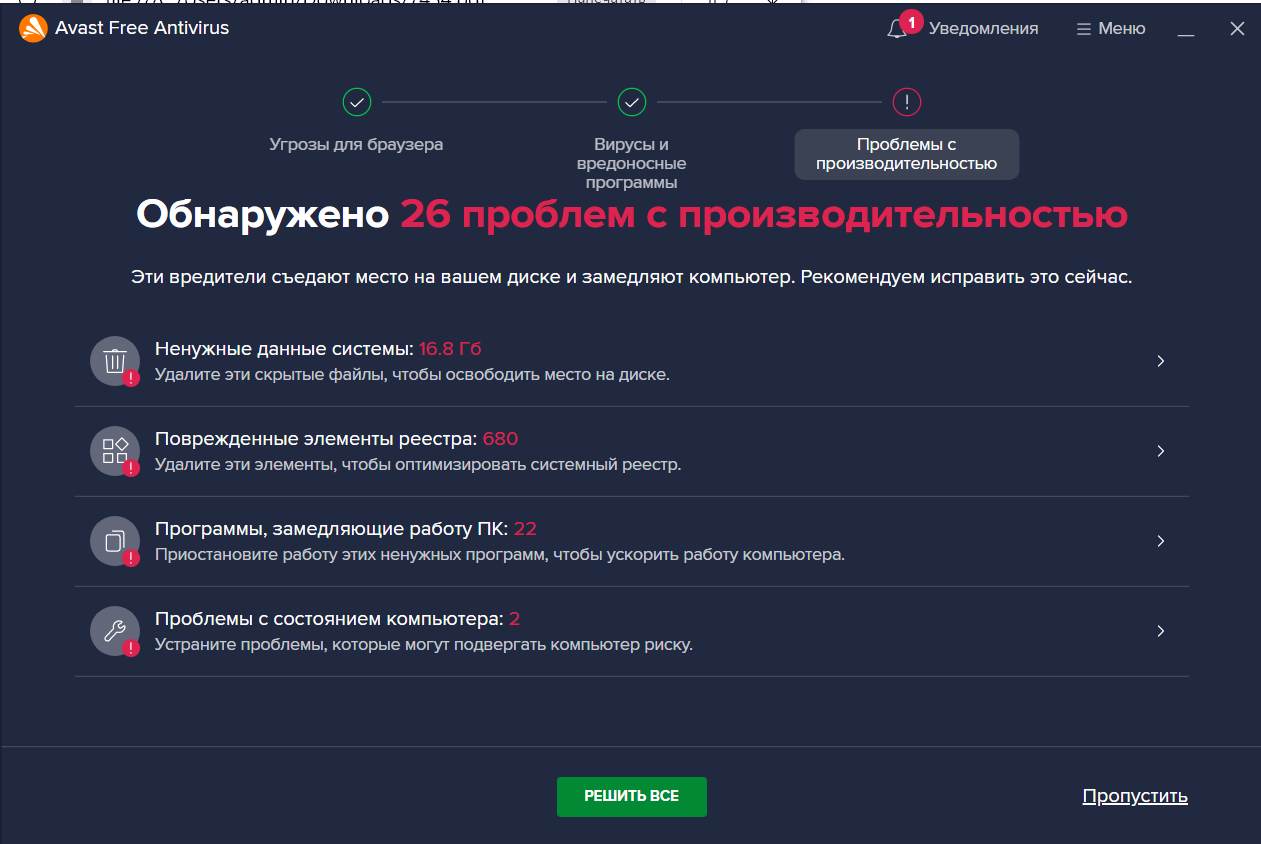


Рис.*4* – Интеллектуальное сканирование

# **Практическое занятие №14**

**Тема «Изучение стандартных средств для реализации приложений, использующих симметричное и ассиметричное шифрование с использованием библиотеки** [**System.Security.Cryptography**](https://docs.microsoft.com/ru-ru/dotnet/api/system.security.cryptography)**»**

**Цель:** Изучить модель криптографии .NET Framework, Основные классы и структуры данных, разработать приложение для шифрования файлов использующих симметричные и ассиметричные алгоритмы шифрования

**Ответить на следующие вопросы:**

1. **Какие симметричные алгоритмы шифрования Вы знаете?**

Симметричные (с секретным, единым ключом, одноключевые, single-key).

1**.Потоковые** (**шифры** Маурера и Диффи):

· с одноразовым или бесконечным ключом (infinite-key cipher);

· с конечным ключом;

· на основе генератора псевдослучайных чисел.

2. **Блочные:**

2.1. Шифры перестановки (permutation, P-блоки);

2.2. Шифры замены (substitution, S-блоки):

· моноалфавитные (Код Цезаря);

· полиалфавитные (шифр Видженера, цилиндр Джефферсона, диск Уэтстоуна, Enigma).;

Шифр Трисемуса, Плейфера, Вижинера, Магический квадрат

Симметричные алгоритмы шифрования (или криптография с секретными ключами) основаны на том, что отправитель и получатель информации используют один и тот же ключ. Этот ключ должен храниться в тайне и передаваться способом, исключающим его перехват.

В симметричном шифровании один и тот же ключ используется как для шифрования, так и для дешифрования. В этом методе исходное сообщение преобразуется в нераспознаваемое сообщение, которое невозможно идентифицировать. Это преобразованное сообщение называется зашифрованным текстом. Это делается с помощью ключа и алгоритма шифрования. На принимающей стороне зашифрованный текст преобразуется обратно в исходное сообщение с использованием того же ключа и алгоритма дешифрования.

Поскольку обе стороны используют один и тот же ключ, симметричное шифрование намного быстрее. С другой стороны, ключ должен быть доступен для расшифровки сообщения. Поэтому для передачи ключа требуется защищенный канал. В целом, симметричное шифрование является простым методом и не требует много времени для завершения. RC4, AES, DES, 3DES - это некоторые распространенные алгоритмы симметричного шифрования.

1. **Какие ассиметричные алгоритмы шифрования Вы знаете?**

Асимметричные (с открытым ключом, public-key):

· Диффи-Хеллман DH (Diffie, Hellman);

· Райвест-Шамир-Адлeман RSA (Rivest, Shamir, Adleman);

· Эль-Гамаль (ElGamal).

В асимметричных алгоритмах шифрования (или криптографии с открытым ключом) для зашифровывания информации используют один ключ (открытый), а для расшифровывания - другой (секретный). Эти ключи различны и не могут быть получены один из другого.

Асимметричное шифрование использует два ключа для шифрования и дешифрования. Эти два ключа называются закрытым ключом и открытым ключом. Он использует открытый ключ для шифрования и закрытый ключ для расшифровки. Открытый ключ доступен для стороны, которая хочет отправить сообщение. Закрытый ключ принадлежит владельцу сообщения. Сообщение, которое зашифровано открытым ключом и алгоритмом шифрования, может быть дешифровано с использованием алгоритма дешифрования и соответствующего закрытого ключа соответствующего открытого ключа.

1. **Основное назначение библиотеки System.Security.Cryptography?**

Пространство имен, предоставляет криптографические службы, включая безопасное кодирование и декодирование данных, а также множество других операций, таких как хэширование, генерация случайных чисел и проверка подлинности сообщений.

1. **Влияет ли размер ключа на криптостойкость алгоритма?**

Размер ключа измеряется в битах (двоичных разрядах). Чем он больше, тем, соответственно, больше времени необходимо на перебор возможных значений, но и тем продолжительнее работает алгоритм. Поэтому выбор оптимальной длины ключа — это вопрос баланса.

1. **Назовите основные классы библиотеки System.Security.Cryptography?**

Класс CSPParameters – содержит параметры, передаваемые поставщику служб шифрования (CSP), который выполняет криптографические вычисления.

Класс CspParameters представляет параметры, которые можно передавать управляемым криптографическим классам, использующим службы шифрования (CSP), с помощью интерфейса Microsoft Cryptography API (CAPI).

Класс RSACryptoServiceProvder - выполняет шифрование и дешифрование данных с помощью реализации асимметричного алгоритма RSA, предоставляемого поставщиком служб шифрования (CSP).

Структура RSAParameters - представляет стандартные параметры для алгоритма RSA (значения d, e, n, p, q и т.д.)

Класс RijndaelManaged – реализует симметричный алгоритм шифрования Rijndael. Поддерживаются ключи длиной 128, 192 и 256 бит.

**Вывод:** Изучила модель криптографии .NET Framework, Основные классы и структуры данных.