Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Основы защиты информации

(Вариант 14)

Студент: Косс В.А.

ФИТ 2 курс 9 группа

Преподаватель: Берников В.О.

Минск 2022

**Практическое занятие №1**

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

Цель: Изучить концепцию национальной безопасности РБ.

**Задание для выполнения.**

Ответить на следующие вопросы:

1. Что такое информационная безопасность?
2. Перечислить основные национальные интересы в информационной сфере?
3. Основные угрозы национальной безопасности, связанные с ИТ-сферой?
4. Назвать основные внутренние и внешние источники угроз национальной безопасности в информационной сфере?
5. Основные направления нейтрализации внутренних источников угроз и защиты от внешних угроз национальной безопасности в информационной сфере?

**Ответы на вопросы**

1. **Информационная безопасность** – состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере
2. **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;
* обеспечение надежности и устойчивости функционирования критически важных объектов информатизации;
* эффективное информационное обеспечение государственной политики.

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

* деструктивное информационное воздействие на личность, общество и государственные институты, наносящие 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;

1. **В информационной сфере внутренними источниками угроз национальной безопасности являются:**

* 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.

**В информационной сфере внешними источниками угроз национальной безопасности являются:**

* 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.

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

* совершенствование механизмов реализации прав граждан на получение, хранение, пользование и распоряжение информацией;
* гарантия обеспечения установленного законодательством порядка доступа к государственным информационным ресурсам и возможностям получения информационных услуг;
* привлечение внимания повышению качества, объема и конкурентоспособности национального контента
* совершенствование нормативной правовой базы обеспечения информационной безопасности;
* завершение формирования комплексной государственной системы обеспечения информационной безопасности;
* участие Республики Беларусь в международных договорах об использовании межгосударственных, международных глобальных информационных сетей и систем, но в то же время сохранение роли регулятора при внедрении иностранных информационных технологий;

**Вывод**: в ход практического занятия была изучена концепция национальной безопасности РБ.

**Практическое занятие №2**

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

Цель: научиться 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. 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 комплексно.

**Задание на выполнение**

Решить задачу разработки средств защиты для обеспечения максимальной эффективности объекта в условиях несанкционированного доступа в соответствии с вариантом 17.

Таблица 2.1- Данные для лабораторной работы

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № варианта | *E0* | *E* | *K* | *C* |
| 17 | 20000 | 19000 | 5 | 500 |

**Выполнение**

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:

|  |  |
| --- | --- |
| *(BYN)* | (2.1) |

Относительная эффективность:

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

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:

|  |  |
| --- | --- |
| *(BYN)* | (2.3) |

Тогда эффективность при наличии средств защиты:

|  |  |
| --- | --- |
| *(BYN)* | (2.4) |

а относительная эффективность :

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

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

|  |  |
| --- | --- |
| *(BYN)* | (2.6) |

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

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

или

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

То есть в условиях несанкционированного доступа при оптимальной стоимости установки самих средств защиты ущерб стремится к минимуму, эффективность и относительная эффективность стремятся к максимуму.

**Вывод:** в ходе лабораторной работы была найдены разработки средств защиты для обеспечения максимальной эффективности объекта в условиях несанкционированного доступа.

Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Отчет по практическому заданию №3:

«Разработка политики информационной безопасности строительной организации»

(Вариант 17)

Студент: Косс В.А.

ФИТ 2 курс 9 группа

Преподаватель: Берников В.О.

Минск 2022

# **ВВЕДЕНИЕ**

Разработка политики безопасности ведется для конкретных условий функционирования информационной системы. Как правило, речь идет о политике безопасности организации, предприятия или учебного заведения. С учетом этого рассмотрим следующее определение политики безопасности.

Политика безопасности — это комплекс предупредительных мер по обеспечению информационной безопасности организации. Политика безопасности включает правила, процедуры и руководящие принципы в области безопасности, которыми руководствуется организация в своей деятельности. Кроме того, политика безопасности включает в себя требования в адрес субъектов информационных отношений, при этом в политике безопасности излагается политика ролей субъектов информационных отношений.

Основные направления разработки политики безопасности — определение объема и требуемого уровня защиты данных а также определение ролей субъектов информационных отношений. В «Оранжевой книге» политика безопасности трактуется как набор норм, правил и практических приемов, которые регулируют управление, защиту и распределение ценной информации.

Результатом разработки политики безопасности является комплексный документ, представляющий собой систематизированное изложение целей, задач, принципов и способов достижения информационной безопасности. Этот документ выступает методологической основой практических мер по обеспечению информационной безопасности. Основные положения определяют важность обеспечения информационной безопасности, общие проблемы безопасности, направления их решения, роль сотрудников, нормативно-правовые основы.

При описании области применения политики безопасности перечисляются компоненты автоматизированной системы обработки, хранения и передачи информации, подлежащие защите.

В состав автоматизированной информационной системы входят аппаратные средства, программное обеспечение, данные и персонал.

Цели, задачи, критерии оценки информационной безопасности определяются функциональным назначением организации.

Политика безопасности затрагивает всех субъектов информационных отношений в организации, поэтому на этапе разработки политики безопасности очень важно разграничить их права и обязанности, связанные с их непосредственной деятельностью.

**ОПИСАНИЕ СТРУКТУРЫ БИЗНЕС-КОМПАНИИ**

По варианту необходимо разработать политику безопасности для военкомата. Организационная структура представлена на рисунке 3.1.

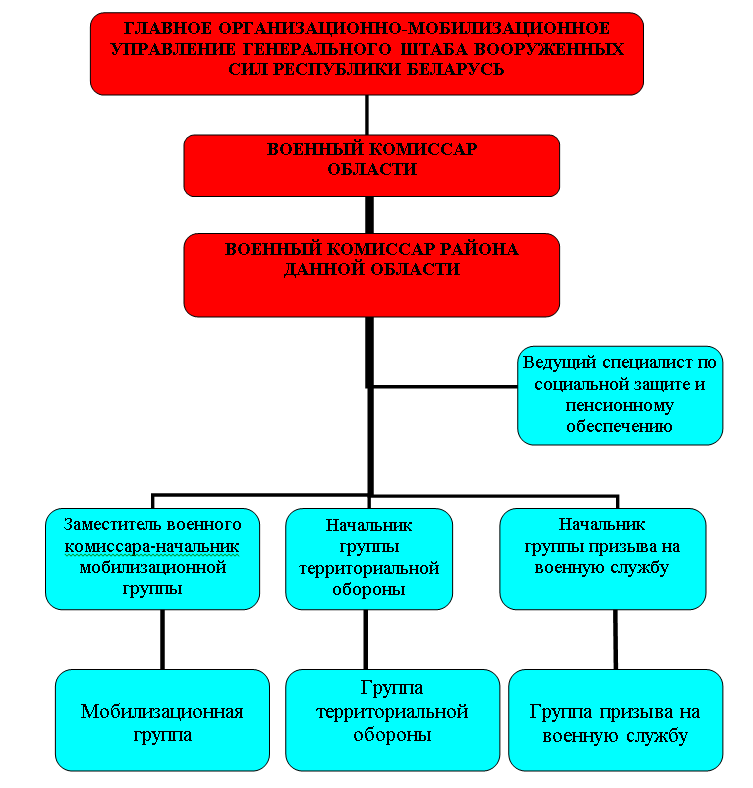


Рисунок 3.1 — Структура организации военкомата

В настоящий момент руководство служебной деятельностью военкоматов осуществляется генеральным штабом вооруженных сил Республики Беларусь через военные комиссариаты областей и районов.

Военные комиссариаты не имеют филиалов и представительств. В структуру военных комиссариатов входят командование, основные подразделения, в том числе военные комиссариаты по муниципальным образованиям, подразделения обеспечения и центры социального обеспечения.

**Военный комиссар** несет персональную ответственность за выполнение задач, стоящих перед военным комиссариатом. Разрабатывает организационную структуру. Организует работу по формированию и подготовке кадрового резерва. Определяет обязанности работников. Издает приказы в пределах своих полномочий, в необходимых случаях совместно с территориальными органами федеральных органов исполнительной власти, и распоряжения, утверждает инструкции, положения и локальные нормативные акты по вопросам деятельности военного комиссариата.

**Начальник мобилизационной группы** руководит работой отдела (отделения) планирования, предназначения, подготовки и учета мобилизационных ресурсов. Проводит работу по повышению квалификации кадров. Организует работу по реализации приказов и директив вышестоящих органов военного управления. Осуществляет контроль за выполнением требований служебных документов. Разрабатывает план проведения мобилизации людских и транспортных ресурсов военного комиссариата.

**Начальник группы территориальной обороны** занимается организацией территориальной обороны, ее руководством и ведением, планированием и руководством выполнения мероприятий по строительству и развитию территориальной обороны, координацией деятельности государственных и военных органов управления, местных исполнительных и распорядительных органов, других войск и воинских формирований по вопросам территориальной обороны. А также развитием теории территориальной обороны, разработкой нормативных правовых актов по вопросам территориальной обороны, планированием и проведением мероприятий по поддержанию боевой и мобилизационной готовности органов управления территориальной обороны и воинских частей территориальных войск.

При призыве граждан на военную службу **начальник группы призыва на военную службу** и военный комиссар района (города) обязаны принять решения о призыве на военную службу, о предоставлении отсрочки от призыва на военную службу и об освобождении от призыва на военную службу и исключении с воинского учета. В случае уклонения граждан от мероприятий по призыву, начальник группы призыва на военную службу принимают решение о направлении соответствующих материалов в территориальные органы внутренних дел по месту жительства этих граждан для решения вопроса о привлечении их к ответственности в соответствии с законодательными актами Республики Беларусь.

В соответствии с основными задачами в пределах компетенции **специалист по социальной защите и пенсионному обеспечению** организует и координирует работу управлений по труду, занятости и социальной защите, а также по назначению (перерасчету) и выплате пенсий, анализирует состояние пенсионного обеспечения и обобщает практику применения законодательства. Специалист также рассматривает запросы и предложения подведомственных органов по труду, занятости и социальной защите и других заинтересованных ведомств по пенсионным вопросам, пособиям и осуществляет надзор за соблюдением законодательства о пенсионном обеспечении.

**ОЦЕНКА РИСКОВ**

Оценка рисков как часть направления информационной безопасности (ИБ) (управления рисками) является существенным инструментом в построении защиты. Процесс оценки рисков предназначен для выявления риска для бизнеса организации и определения мер безопасности, предпринимаемых для снижения риска.

В классическом представлении риск – это вероятность реализации угрозы информационной безопасности. Оценка рисков заключается в моделировании картины наступления неблагоприятных условий посредством учета всех возможных факторов, определяющих риск. С математической точки зрения при анализе рисков такие факторы можно считать входными параметрами. При этом нужно учитывать множество источников информации и неопределенность самой информации.

На этапе оценки рисков наибольший интерес представляют непосредственно формулы и входные данные для расчета значения риска. Целью работы является вывод формулы расчета риска информационной безопасности, позволяющей получить массив актуальных рисков и оценить потери в денежном эквиваленте. На базе проведенной оценки рисков ИБ проводится разработка плана обработки рисков, на основании которого выстраивается приоритет внедрения систем и процессов ИБ в компании.

Деятельность Вооруженных Сил Республики Беларусь в информационном пространстве строится исходя из совокупности принципов: законности, приоритетности, комплексности, взаимодействия, сотрудничества и инновационности.

В информационном пространстве, которое стало частью жизни общества, разворачиваются настоящие кибервойны. В случае неспособности людей отразить атаку, могут произойти катастрофические последствия не только для одной структуры, но и в масштабах всей страны. Что же касается вооруженных сил нашей страны, в настоящий момент эта структура переживает настоящий бум модернизации. В частности в военных комиссариатах совершенствуется инфраструктура: обновляется система связи, ведь в случае направленной атаки противник может полностью дезорганизовать действия не только одного подразделения, но и, возможно, всего комиссариата. В этой связи озабоченность специалиста по информационной безопасности кажется попыткой предупредить возможные последствия, в случае несостоятельности отразить атаку.

Одним из основных источников угроз информационного характера является дестабилизация социальной и политической обстановки в местах дислокации военкоматов. Создание искусственно накаленной атмосферы, провокация конфликтов личного состава с местным населением, иногда даже беспорядки, вызванные направленным информационным воздействием, становятся серьезными угрозами стабильности ситуации в целом.

Технические угрозы информационного характера включают в себя

системы управления и сохранности конфиденциальной информации, передаваемой по каналам военной связи. Виды технических угроз деятельности Вооруженных сил могут носить различный характер: от намеренного повреждения систем и похищения информации до халатности отдельных сотрудников. Мерами защиты в этом случае станут и повышение уровня защищенности систем автоматизированного управления, тщательный отбор личного состава и его обучение требованиям, связанным с защитой информации.

Сегодня формирование единого информационного пространства Вооруженных Сил стоит в ряду актуальнейших проблем. В последние годы в Минобороны предприняты важные шаги, направленные на повышение уровня управляемости информационным обеспечением жизнедеятельности Вооруженных Сил страны. В государстве начали действовать так называемые отряды специалистов по кибербезопасности, а сейчас по большей степени внимание уделяется защите инфраструктуры вооруженных сил.

**РАЗРАБОТКА МЕР ЗАЩИТЫ**

Меры, которые могут быть применены в целях защиты информации и обеспечения безопасности в данной сфере, делятся на две группы: защита информационных систем от повреждения и информации от утечки и перехвата и защита психики личного состава от намеренного информационно-психологического воздействия. Эти меры должны приниматься в совокупности, опираясь на все новейшие научные разработки и программные продукты.

**Первая группа мер** включает в себя защиту объектов дислокации войск и расположенных в них АСУ и элементов компьютерной техники от любого намеренного выведения из строя; защита систем от удаленного проникновения , в частности с установлением программных продуктов, обеспечивающих полную защиту периметра от проникновений, например, DLP-систем и SIEM-систем; защита информации, носящей характер государственной или военной тайны, от утечек или намеренного похищения; радиоэлектронная защита. А также использование защищенных моделей компьютеров и программных средств, которые не могут быть повреждены заранее созданными проблемами в их кодах, развитие средств электронной разведки; использование социальных сетей для намеренного дезинформационного воздействия и защита систем связи.

Ко **второй группе мер** относятся предохранение психики служащих от намеренного психологического воздействия и корректировка искаженного транслирования информации.

Для разработки и реализации комплекса этих мер необходимо создание отдельных подразделений, действующих в сфере информационной безопасности.

Дополнительно следует учитывать, что меры защиты военной информации проблематично применять при формировании документации на базе научных институтов и сервисных служб.

Серьезная уязвимость систем АСУ армии возникает и из-за передачи информации закрытого характера по открытым линиям связи. Угрозы возникают и при распространении частными лицами случайно полученных ими сведений в социальных сетях. Такие риски блокируются только разъяснительной работой с населением. Комплексный подход к обеспечению информационной безопасности и личного состава должен обеспечить укрепление обороноспособности Беларуси. Опираясь на Доктрину информационной безопасности, можно разрабатывать новые комплексные способы борьбы с нарастающими угрозами

**ВЫВОДЫ**

Развитие человеческого общества неразрывно связано с процессом информатизации, под которым понимается непрерывно возобновляемый процесс создания необходимых условий для удовлетворения информационных потребностей человека. На протяжении всей истории человеческой цивилизации и даже на начальной стадии возникали потребности, связанные с получением, хранением и накоплением, первичной обработкой и переработкой, поиском, отображением, передачей и обменом информацией. Современный этап информатизации характеризуется созданием информационных систем и систем телекоммуникации с применением средств персональной электронной вычислительной техники.

Политика информационной безопасности неразрывно связана с развитием компании, ее стратегическим планированием, она определяет общие принципы и порядок обеспечения информационной безопасности на предприятии.

Эффективное обеспечение требуемого уровня информационной безопасности организации возможно только при наличии формализованного и системного подхода к выполнению мер по защите информации. Целью разработки политики информационной безопасности организации является создание единой системы взглядов и понимания целей, задач и принципов обеспечения информационной безопасности.

Определение эффективности реализации требований безопасности является одной из ключевых задач обеспечения безопасности активов на всех этапах жизненного цикла объектов информационных технологий. Ее решение связано с разработкой соответствующих методик, методов и средств оценки эффективности защиты активов, которая затруднена рядом объективных факторов, обусловленных сложностью и динамичностью процессов и информационных потоков, стремительным развитием информационных технологий, хаотичностью возникновения новых видов угроз, приводящих к появлению новых уязвимостей аппаратных и программных средств как в самом объекте информационных технологий, так и в средствах обеспечения безопасности.

Адекватный уровень ИБ в современной организации может быть обеспечен только на основе комплексного подхода, реализация которого начинается с разработки и внедрения эффективных ПБ. Эффективные ПБ определяют необходимый и достаточный набор требований безопасности, позволяющих уменьшить риски ИБ до приемлемой величины. Они оказывают минимальное влияние на производительность труда, учитывают особенности бизнес-процессов организации, поддерживаются руководством, позитивно воспринимаются и исполняются сотрудниками организации. Для того чтобы ПБ оставалась эффективной, необходимо осуществлять непрерывный контроль ее исполнения, повышать осведомленность сотрудников организации в вопросах ИБ и обучать их выполнению правил, предписываемых ПБ. Регулярный пересмотр и корректировка правил ПБ необходимы для поддержания ее в актуальном состоянии.

Разработка и внедрение ПБ в организации — процесс коллективного творчества, в котором должны участвовать представители всех подразделений, затрагиваемых производимыми изменениями. Координатором этого процесса является специалист, на которого руководство организации возлагает ответственность за обеспечение ИБ.

**Практическое занятие №4**

**Тема «Криптографическая защита информации»**

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 (рис. 1).

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.

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.

**Задание к выполнению**

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

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

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

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

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

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

3. Вернуть настройки Брандмауэра в исходное состояние до начала выполнения практического задания.

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

**Выполнение**

Для создания правила по ограничению доступа программ к сети необходимо открыть Панель управления – Брандмауэр Защитника Windows (рис. 4.1 и рис 4.2).

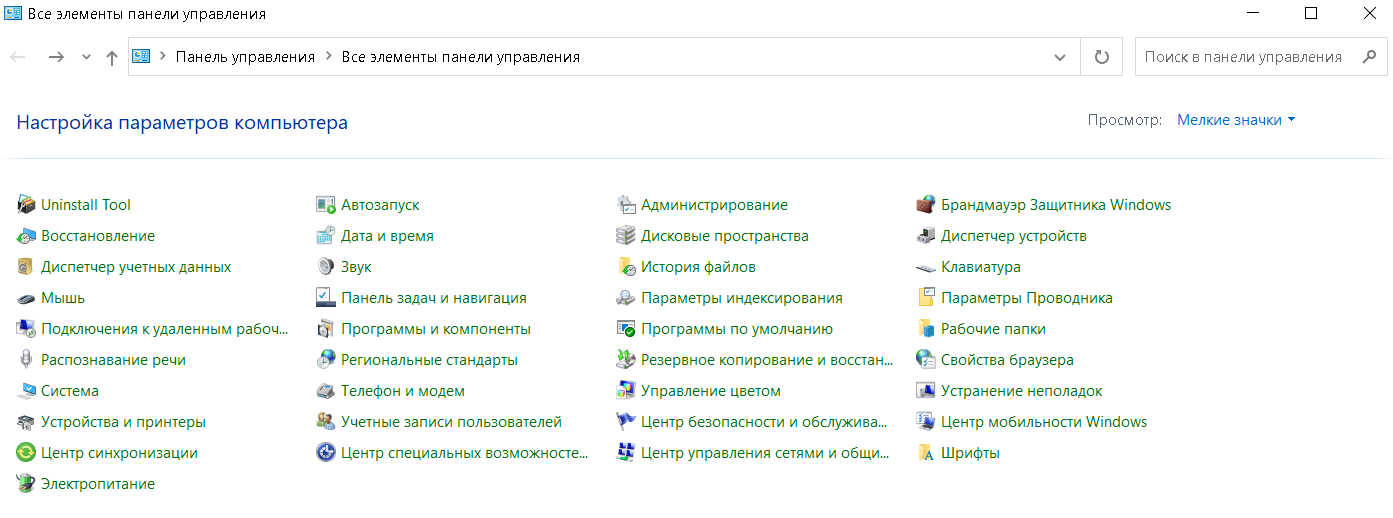


Рис. 4.1. Панель управления

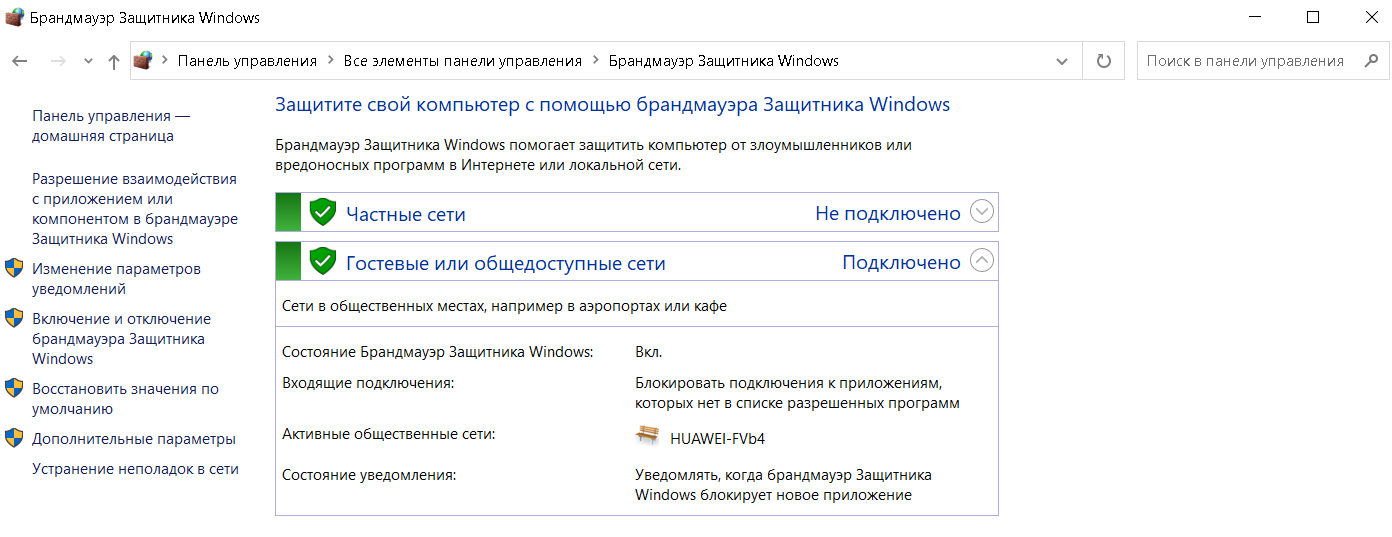


Рис. 4.2. Брандмауэр Защитника Windows

Первым этапом необходимо включить брандмауэр. В окне «Брандмауэр Защитника Windows» слева выбираем «Включение брандмауэра Windows» (рис. 4.3).

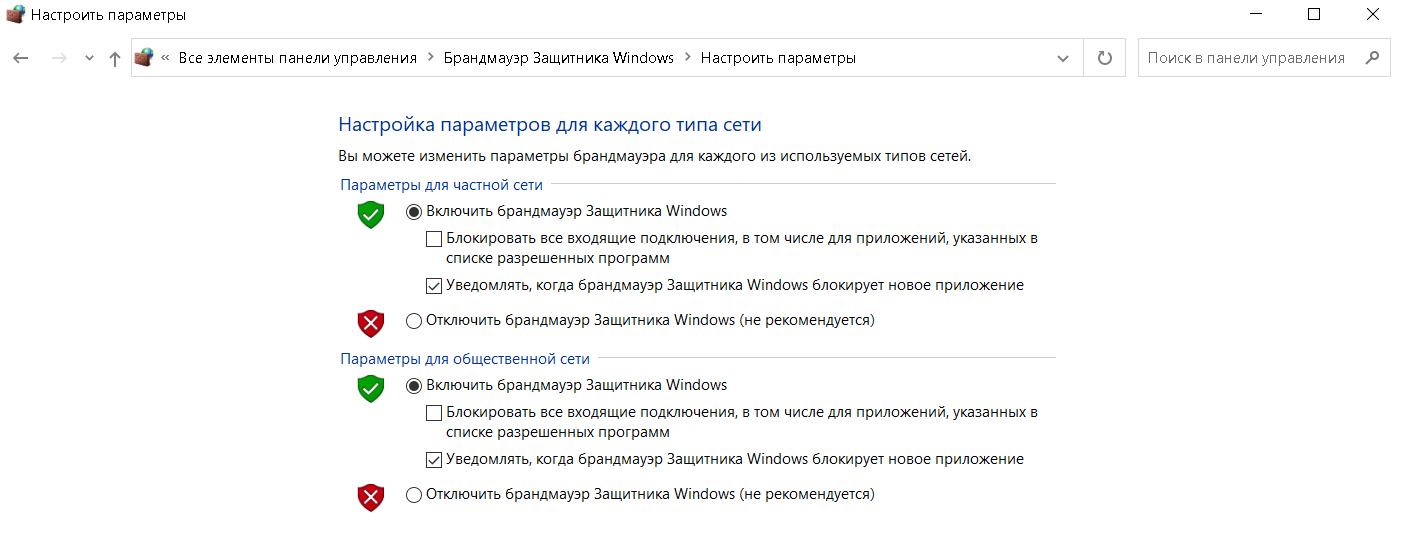


Рис. 4.3. Включение Брандмауэра

Вторым этапом является настройка правил для входящих и исходящих подключений. Для этого во вкладке «Дополнительные параметры». В открывшемся окне (рис. 4.4) выбираем в левой панели правила для входящих или исходящих подключений, затем нажимаем «Создать правило» в правой панели*.*

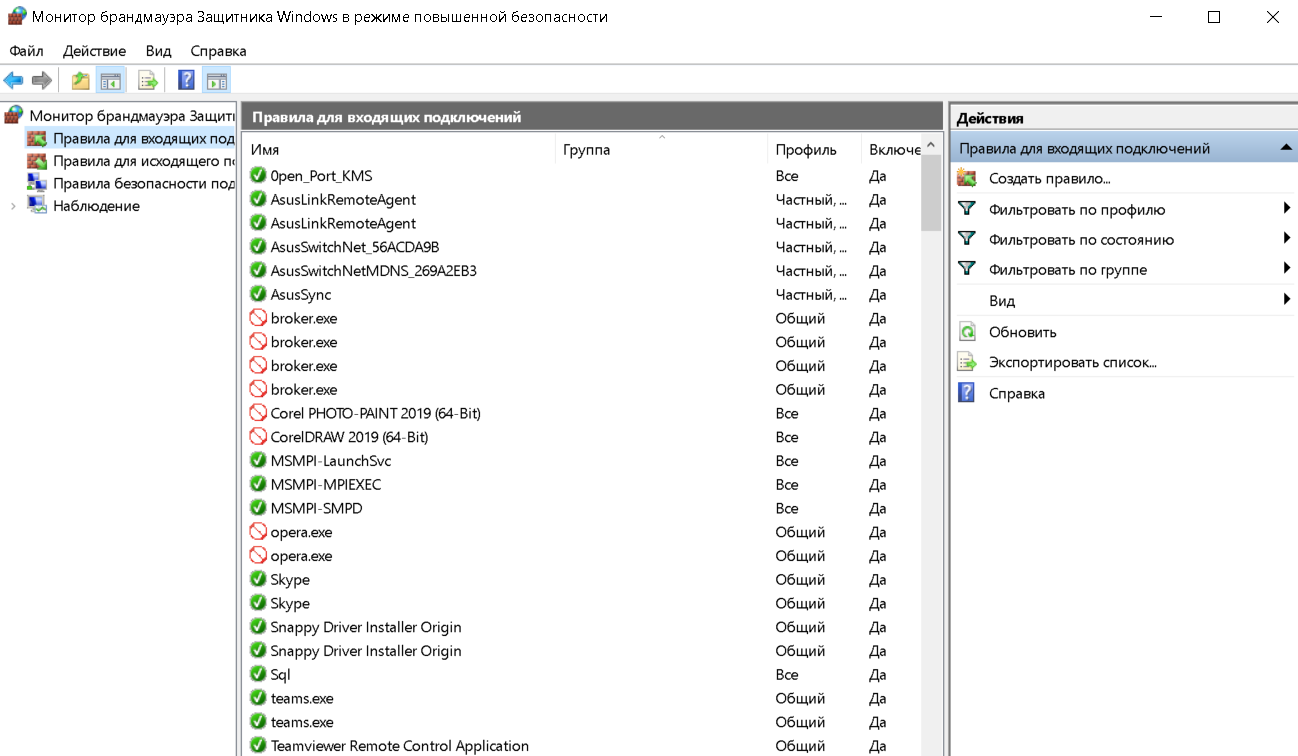


Рис. 4.4. Монитор Брандмауэра

В открывшемся мастере создания правила выбираем «Для программы» (рис. 4.5), далее прописываем путь программы (рис. 4.6) через папку, в которой она установлена, после чего выбираем блокировку или разрешение подключения (рис. 4.7).

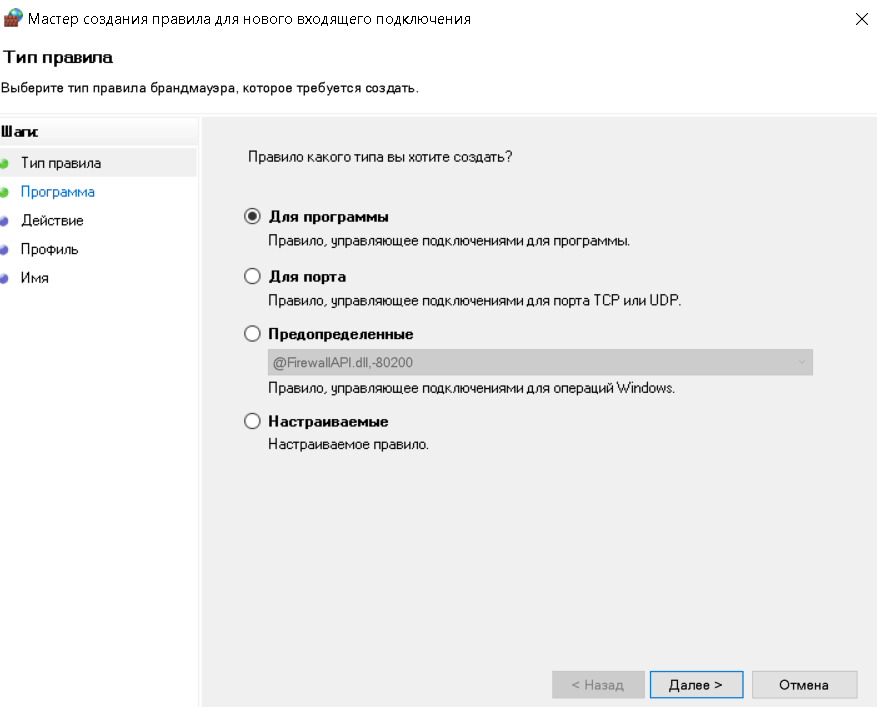


Рис. 4.5. Установка типа правила

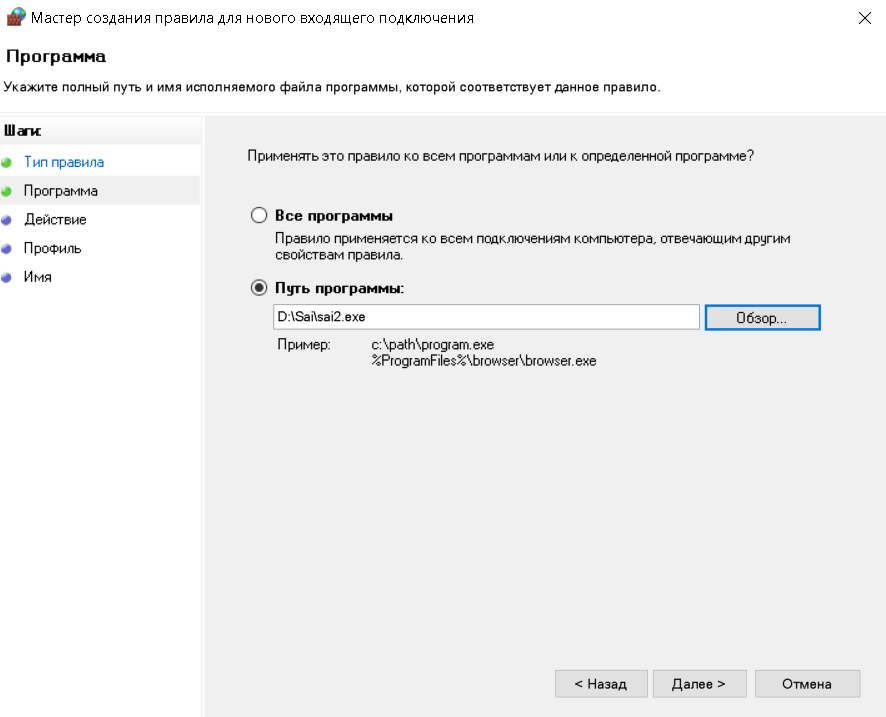


Рис. 4.6. Выбор пути к программе

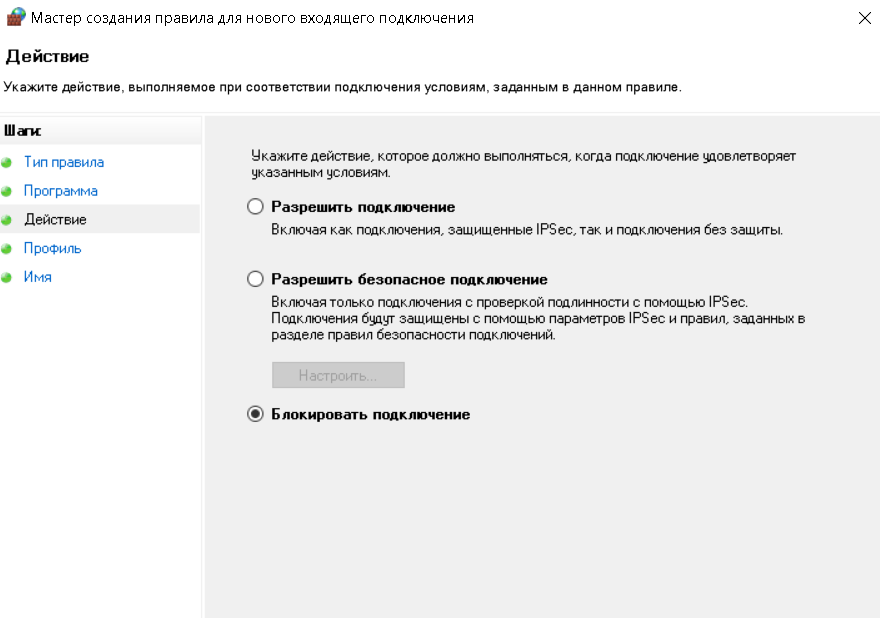
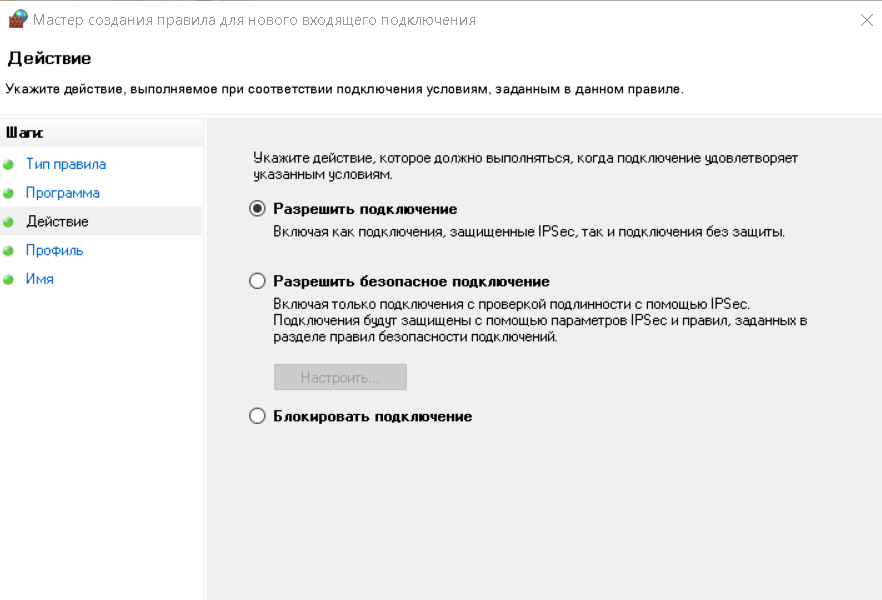


Рис. 4.7. Установка типа подключения

Затем выбираем профиль, к которому будет применено правило (рис. 4.8), и указываем имя правила (рис. 4.9).

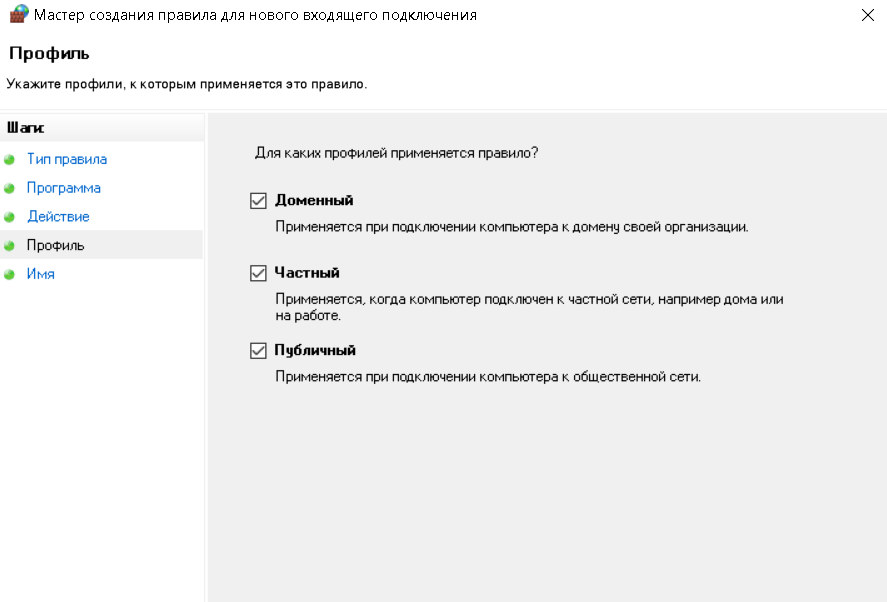


Рис. 4.8. Выбор профиля

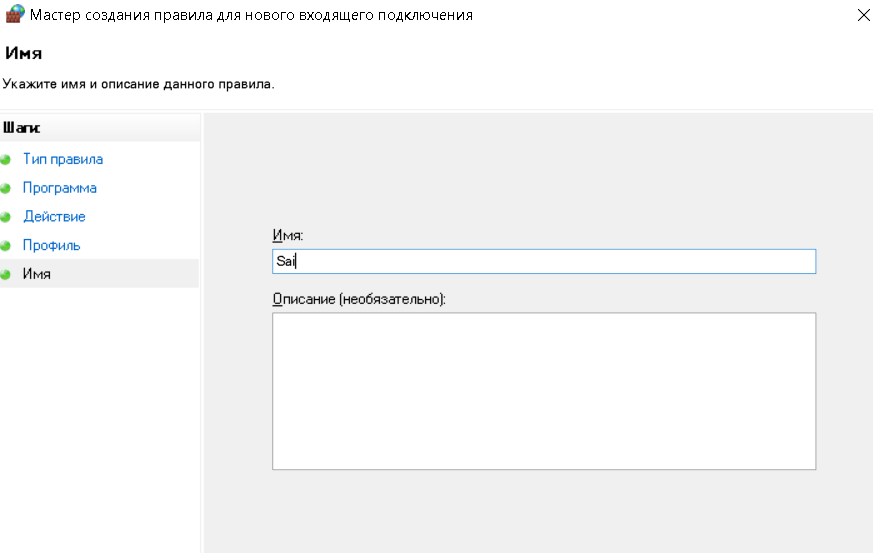
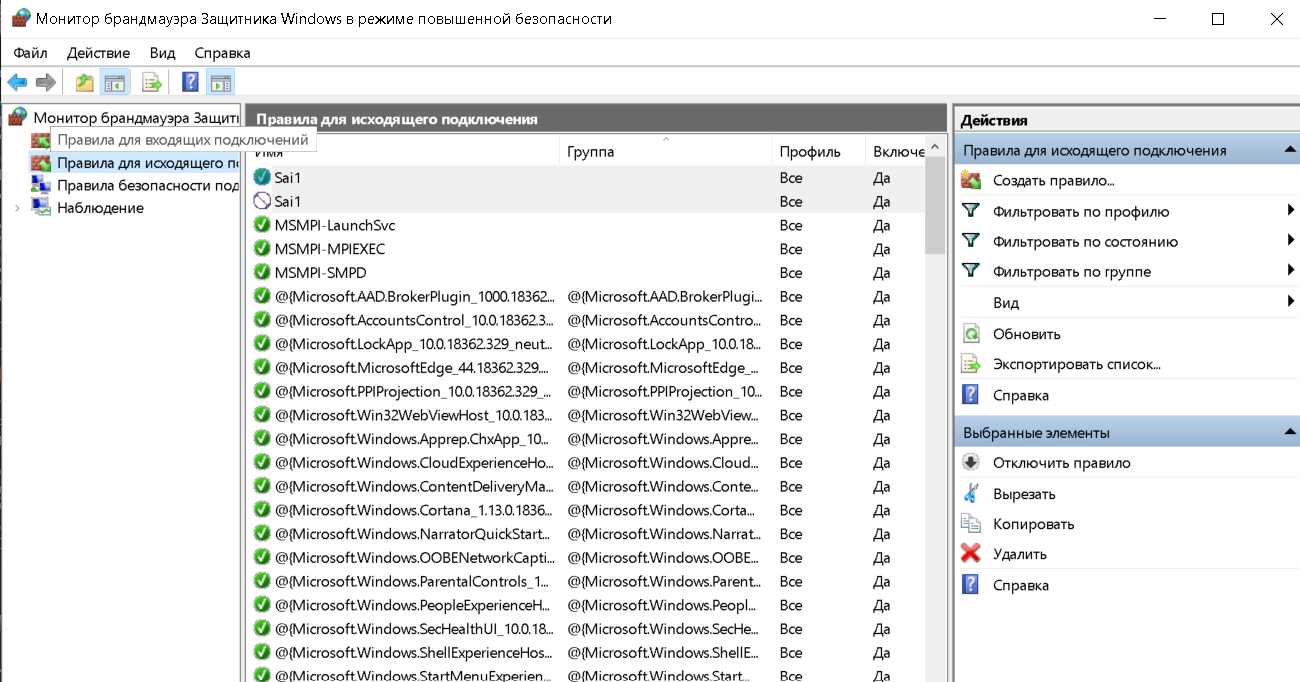
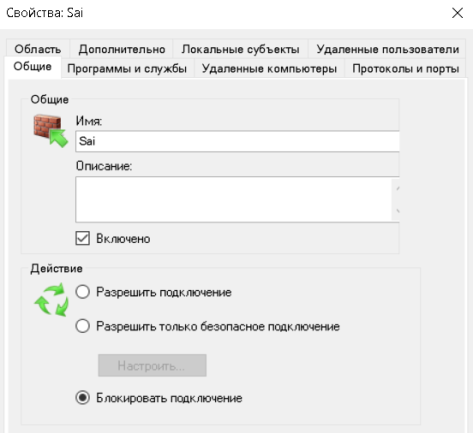
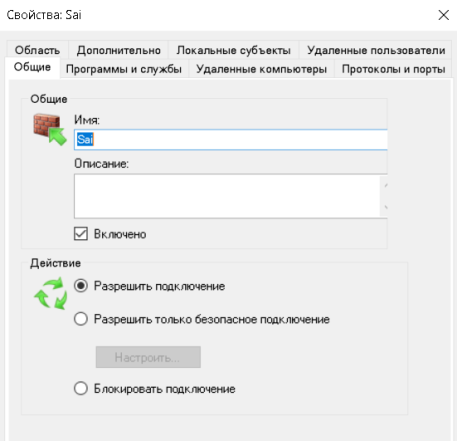


Рис.4.9. Задание имени правила

В общем списке появились созданные правила (рис. 4.10).

Рис. 4.10. Общий список с добавленными правилами

При двойном нажатии на правило отображаются его свойства. Созданные правила показаны на рисунке 4.11.



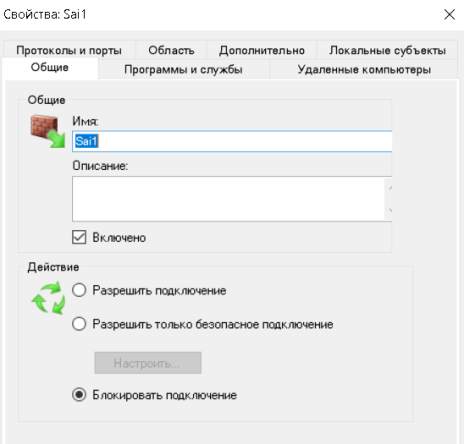
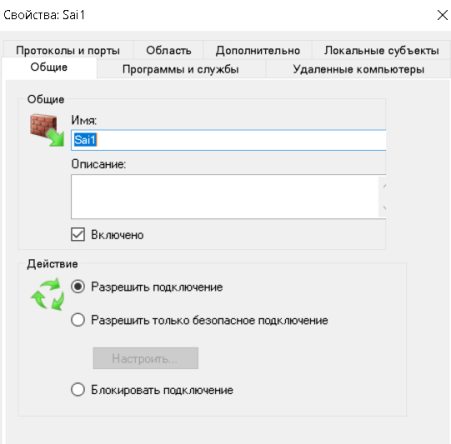


Рис. 4.11. Добавленные правила

Для возвращения настроек Брандмауэра в исходное состояние удаляем созданные правила с помощью соответствующей кнопки на правой панели (рис. 4.12).

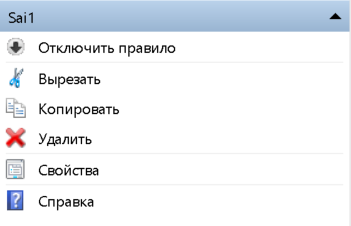


Рис. 4.12. Правая панель управления

Чтобы опробовать действие нескольких команд, нажимаем Win+R. В открывшемся окне для примера были введены команды calc (рис. 4.13), cmd (рис. 4.14), dcomcnfg (рис. 4.15), sfquirt (рис. 4.16), mstsc (рис. 4.17).

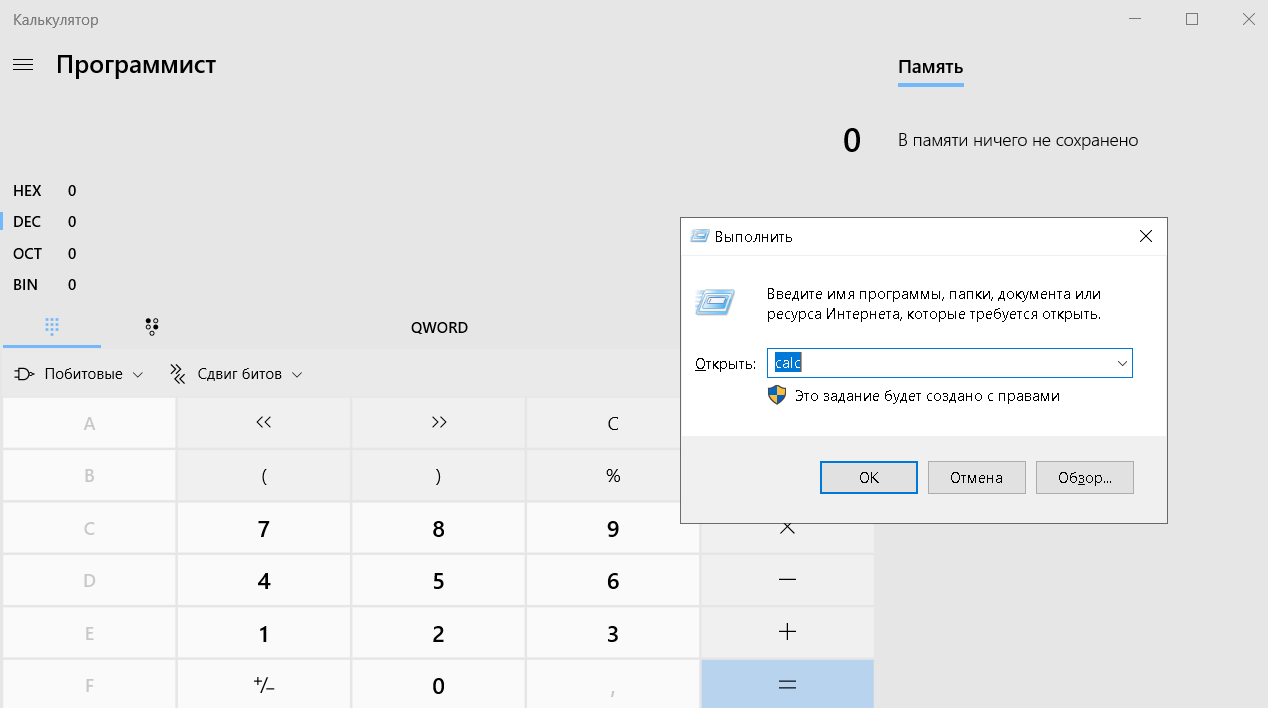


Рис. 4.13. Результат выполнения команды calc

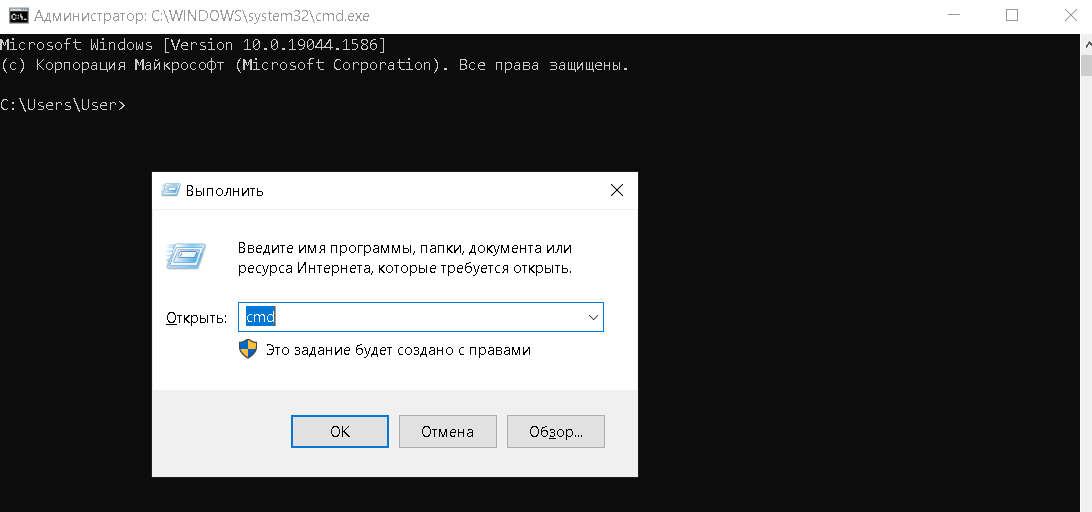


Рис. 4.14. Результат ввода команды cmd

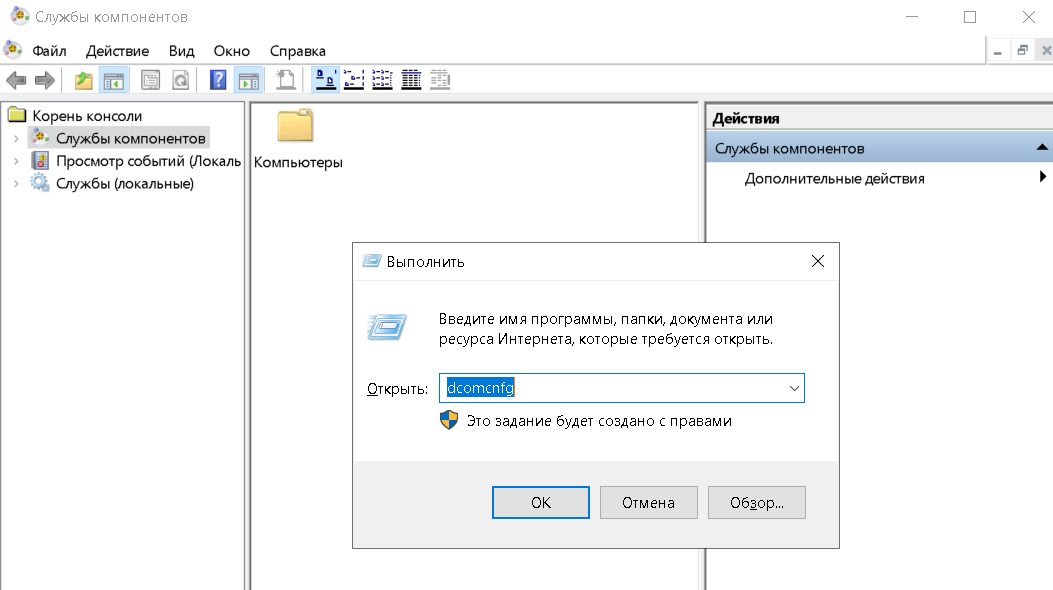


Рис. 4.15. Результат ввода команды dcomcnfg

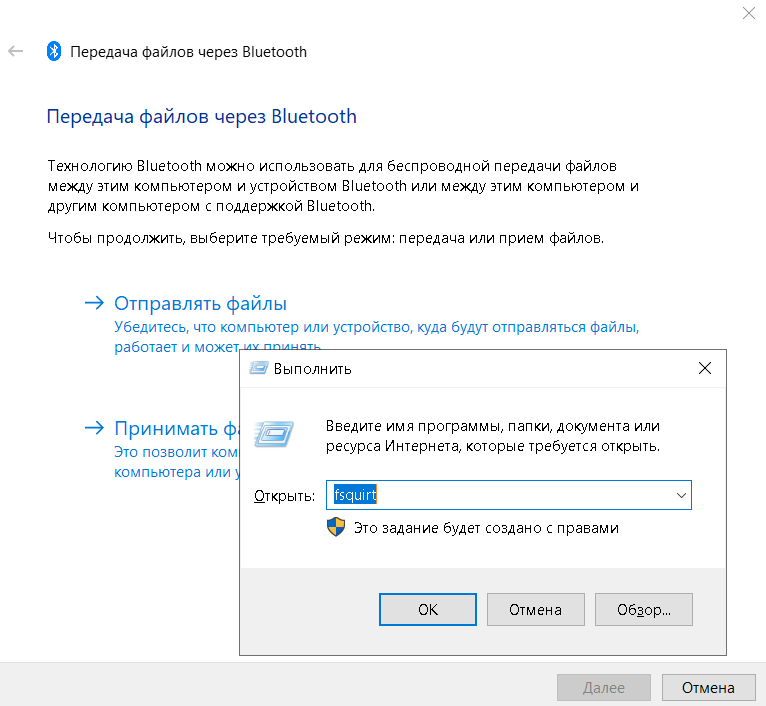


Рис. 4.16. Результат ввода команды fsquirt

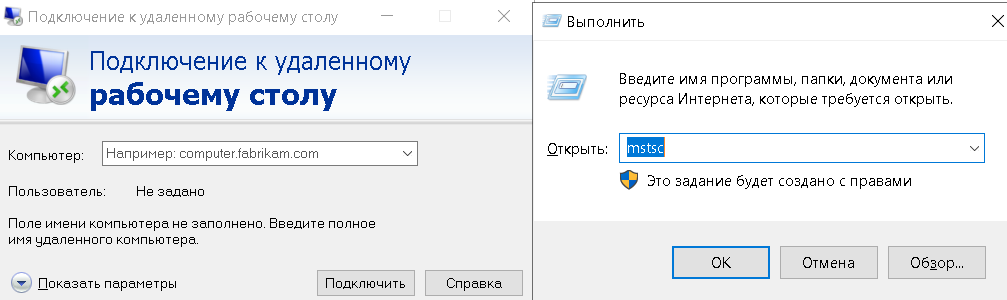


Рис. 4.17. Результат ввода команды mstsc

**Вывод:** я научилась работать с Брандмауэром защитника Windows, а также создавать новые правила для входящих и исходящих подключений. Также попробовала действие некоторых команд.

**Практическое занятие №5**

**Тема «Криптографическая защита информации»**

Цель: Овладение основными криптографическими алгоритмами симметричного шифрования.

**Теоретическое введение**

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

Изначально криптография изучала методы шифрования информации – обратимого преобразования открытого (исходного) текста на основе секретного алгоритма и/или ключа в шифрованный текст (шифротекст). Традиционная криптография образует раздел симметричных криптосистем, в которых зашифрование и расшифрование проводится с использованием одного и того же секретного ключа.

Классификация алгоритмов шифрования

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

1.1. Потоковые:

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

· с конечным ключом;

· на основе генератора псевдослучайных чисел.

1.2. Блочные:

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

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

· моноалфавитные;

· полиалфавитные;

2. Асимметричные (с открытым ключом, public-key):

· Диффи-Хеллман DH (Diffie, Hellman);

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

· Эль-Гамаль (ElGamal).

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.

**Задание к выполнению**

1. Зашифровать сообщение с использованием шифра Цезаря, Трисемуса, Плейфейра и Вижинера и полученного секретного ключа (по номеру варианта и ключевому слову «Защита»). В качестве сообщения использовать свою Фамилию Имя Отчество.

**Выполнение**

ФИО: Косс Валерия Александровна

**a) Шифр Цезаря**

Номер варианта 17, значит ключ для шифрования будет равен 17.

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

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

КОСС = Ы Я Щ Щ

ВАЛЕРИЯ = Р О Ь Ф А Ш Н

АЛЕКСАНДРОВНА = О Ь Ф Ы Щ О Ю У А Я Р Ю О

**b) Шифр Трисемуса**

З А Щ И Т Б В Г

Д Е Ж Й К Л М Н

О П Р С У Ф Х Ц

Ч Ш Ъ Ы Ь Э Ю Я

КОСС = У Ч Ы Ы

ВАЛЕРИЯ = М Е Ф П Ъ Й Г

АЛЕКСАНДРОВНА = Е Ф П У Ы Е Ц О Ъ Ч М Ц Е

**c) Шифр Плейфейра**

Вспомогательный символ Ъ

Делим исходный текст на биграммы: ко-съ-съ, ва-ле-ри-яъ, ал-ек-са-нд-ро-вн-аъ

З А Щ И Т Б В Г

Д Е Ж Й К Л М Н

О П Р С У Ф Х Ц

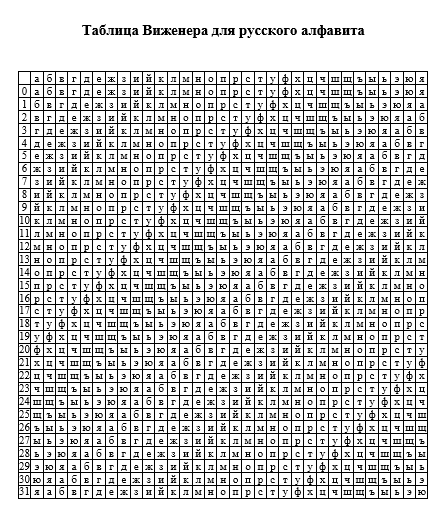
Ч Ш Ъ Ы Ь Э Ю Я

КОСС = Д Ы Р Ы Р Ы

ВАЛЕРИЯ = Г Щ М Ж С Щ Ч Ы

АЛЕКСАНДРОВНА = Б Е Ж Л П И Д Е С П Г М Щ М

**d) Шифр Вижинера**



З А Щ И Т Б В Г

Д Е Ж Й К Л М Н

О П Р С У Ф Х Ц

Ч Ш Ъ Ы Ь Э Ю Я

КОСС = С О К Щ

ВАЛЕРИЯ = Й А Д Н В И Ж

АЛЕКСАНДРОВНА = З А Ю Т Г А Ф Д Й Ц Ф Н З

1. Расшифровать следующее сообщение:

|  |  |  |
| --- | --- | --- |
| 17. | **И\_ЛБКЧУОПЧТУ\_ОЬР** | Расшифровать с помощью Двойной перестановки по ключу.  **Ключ 1 ЛЕТО**  **Ключ2 4213** |

**Выполнение**

*0 1 2 3 4*

*1* И К П \_

*2* \_ Ч Ч О

*3* Л У Т Ь

*4* Б О У Р

*0 2 1 4 3*

*1* К И \_ П

*2* Ч \_ О Ч

*3* У Л Ь Т

*4* О Б Р У

*0 2 1 4 3*

*4* О Б Р У

*2* Ч \_ О Ч

*1* К И \_ П

*3* У Л Ь Т

ОБРУЧ ОЧКИ ПУЛЬТ

**Вывод:** в ходе лабораторной работы были изучены основные криптографические алгоритма мы симметричного шифрования.

**Практическое занятие №6**

**Тема «Криптографическая защита информации»**

Цель: Овладение основными криптографическими алгоритмами асимметричного шифрования.

**Задание №1**

Рассказать процесс работы алгоритма RSA.

|  |  |  |
| --- | --- | --- |
| Этап | Описание операции | Результат операции |
| Генерация ключей | Выбрать два простых различных числа | p=3557,  q=2579 |
| Вычислить модуль (произведение) | n = p \cdot q = 3557 \cdot 2579 = 9173503 |
| Вычислить функцию Эйлера | \varphi(n) = (p-1) (q-1) = 9167368 |
| Выбрать открытую экспоненту | e = 3 |
| Вычислить секретную экспоненту | d = e^{-1} \mod \varphi(n)  d = 6111579 |
| Опубликовать открытый ключ | \{e, n\} = \{3,9173503 \} |
| Сохранить закрытый ключ | \{d, n\} = \{6111579, 9173503 \} |
| Шифрование | Выбрать текст для зашифровки | m = 111111 |
| Вычислить шифротекст | \begin{align} c &= E(m) \\  &= m^e \mod n \\  &= 111111^3   \mod 9173503 \\  &= 4051753 \end{align} |
| Расшифрование | Вычислить исходное сообщение | \begin{align} m &= D(c) = \\   &= c^d \mod n \\   &= 4051753^{6111579} \mod 9173503 \\   &= 111111 \end{align} |

**Задание №2**

Рассказать процесс работы алгоритма Диффи-Хеллмана.

На практике **обмен ключами** по алгоритму Диффи‑Хеллмана происходит по следующей схеме.

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.
4. Ключ сессии может использоваться как секретный ключ для другого алгоритма шифрования, например DES. Никакое третье лицо, контролирующее обмен, не сможет вычислить ключ сессии, не зная один из секретных ключей.

**Задание №3**

Рассказать процесс работы алгоритма Эль-Гамаля.

## **Генерация ключей**

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:

1. 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
2. Вычисляются числа a = g^k\,\bmod\,p и b = y^k M\,\bmod\,p.
3. 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" \o "Шифротекст).

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.

При этом нетрудно проверить, что

~(a^x)^{-1}\equiv g^{-kx}\pmod{p}

и поэтому

~b(a^x)^{-1}\equiv (y^kM)g^{-xk}\equiv (g^{xk}M) g^{-xk}\equiv M \pmod{p}.

Для практических вычислений больше подходит следующая формула:

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

**Задание №4\***

Используя существующие криптографические библиотеки, создать приложение и проанализировать работу вышеперечисленных алгоритмов.

**Выводы:** были изучены основные криптографические алгоритмы асимметричного шифрования, а также была проанализирована их работа на практике.

**Практическое занятие №7**

**Тема «Криптографическая защита информации»**

Цель: **изучить и закрепить умение реализации ЭЦП на примере RSA.**

**Задание**

Объяснить последовательность выполнения процедур генерации и проверки ЭЦП.

Описать последовательность действий участников протокола при отправке и проверке ЭЦП.

Описать схему протокола ЭЦП на основе алгоритма RSA.

Записать результаты выполнения задания и код полученной программы.

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.

Схема протокола ЭЦП на основе алгоритма RSA:

Во-первых, вырабатываются ключи. То есть выбираются два простых числа, находится модуль, функция Эйлера от модуля, выбирается открытая и закрытая экспонента (выполняет отправитель А). Далее отправитель А выполняет оправку сообщения и электронной подписи.



Рисунок 1− Отправка сообщения методом RSA

Получив сообщение отправитель В проверяет электронную подпись.



Рисунок 2− Проверка сообщения методом RSA

**Контрольные вопросы:**

1. Дайте определение понятию "электронная цифровая подпись".

**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").

2. Объясните какой порядок использования ключей (открытый; закрытый) при отправке и проверке ЭЦП.

Вначале отправитель использует свой закрытый ключ, а затем получатель применяет открытый ключ отправителя.

3. Перечислите специальные схемы ЭЦП.

* 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;

**Практическое занятие №8**

**Тема «Криптографическая защита информации»**

**Вариант 1**

Цель: получение основных сведений из курса теории чисел

**Задание**

1. Найти канонические разложения чисел *а* = 101398751 и  *b =*326147777.

2. Найти НОД  = НОД (101398751, 326147777) пользуясь a) алгоритмом Евклида, б) разложением чисел на простые множители.

3. С помощью расширенного алгоритма Евклида найти целые *u*, *v*, удовлетворяющие соотношению Безу: *au* + *bv* = НОД  = НОД (101398751, 326147777).

4. Найти остаток от деления на 29.

**Задание 1.** Найти канонические разложения чисел

**Решение.**

Следовательно, 101398751 = 311∙571∙571, 326147777 = 571∙607∙941.

**Задание 2а.** Найти НОД (101398751, 326147777) пользуясь а) алгоритмом Евклида, б) разложением чисел на простые множители.

**Решение.** Применим алгоритм Евклида.

326147777 : 101398751 = 3 (остаток 21951524),

101398751 : 21951524 = 4 (остаток 13592655),

21951524 : 13592655 = 1 (остаток 8358869),

13592655 : 8358869 = 1 (остаток 5233786),

8358869 : 5233786 = 1 (остаток 3125083),

5233786 : 3125083 = 1 (остаток 2108703),

3125083 : 2108703 = 1 (остаток 1016380),

2108703 : 1016380 = 2 (остаток 75943),

1016380 : 75943 = 13 (остаток 29121),

75943 : 29121 = 2 (остаток 17701),

29121 : 17701 = 1 (остаток 11420),

17701 : 11420 = 1 (остаток 6281),

11420 : 6281 = 1 (остаток 5139),

6281 : 5139 = 1 (остаток 1142),

5139 : 1142 = 4 (остаток 571),

1142 : 571 = 2 (остаток 0).

Следовательно, НОД (101398751, 326147777) = 571.

**Задание 2б.** Найдём НОД (*a, b*), воспользовавшись разложением на простые множители чисел *a* и *b*, полученным в решении предыдущего задания: 101398751 = 311∙571∙571, 326147777 = 571∙607∙941. Следовательно, наибольшим общим делителем будет: НОД (101398751;326147777) = 517.

**Задание 3.** С помощью расширенного алгоритма Евклида найти целые числа *u*,*v*, удовлетворяющие соотношению Безу: для целых чисел *а* = 101398751 и  *b =*326147777.

**Решение.** Построим таблицу для данных

*v u r q*

*1 0* 326147777 -

0 1 101398751 3

1 -3 21951524 4

-4 13 8358869 1

5 -16 8358869 1

-9 29 5233786 1

14 -45 3125083 1

-23 74 2108703 1

37 -119 1016380 2

-97 312 75943 13

1298 -4175 29121 2

-2693 6882 17701 1

3991 -12837 11420 1 1

-6684 21477 6281 1

10675 -34336 5139 1

-17359 55835 1142 4

80111 -257676 571 2

НОД (101398751;326147777) = 571 = -257676*a* + 80111*b*.

**Задание 4.**

Найти остаток от деления на 29.

**Практическое занятие №9**

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

Цель: Изучить основные положения авторского права и смежных прав.

**Задание для выполнения.**

Ответить на следующие вопросы:

1. На какие объекты распространяется авторское право?
2. Что относится к личным неимущественным правам?
3. Что относится к личным имущественным правам?
4. Каковы особенности авторского права на составные произведения?
5. Каков срок действия авторского права?
6. Кто является субъектом авторского права?
7. Что такое авторский договор?
8. Наиболее распространенные виды авторских договоров?
9. Основные составляющие авторского договора?

**Ответы на вопросы**

1. **Авторское право** **распространяется как на обнародованные, так и на необнародованные произведения**, существующие в какой-либо объективной форме.

Произведения

* литературные (включая компьютерные программы и базы данных);
* научные (статьи, монографии, отчеты);
* драматические и музыкально-драматические, сценарные;
* хореографические и пантомимы;
* музыкальные с текстом или без текста;
* аудиовизуальные;
* живописи, графики, скульптуры и другие изобразительного искусства;
* декоративно-прикладного искусства;
* архитектуры, градостроительства и садово-паркового искусства;
* фотографические;
* карты, планы, эскизы и иные, относящиеся к архитектуре, географии, топографии, другим наукам и технике;
* другие произведения.

Производные произведении

* переводы, обработки, инсценировки, музыкальные аранжировки, обзоры, аннотации, рефераты;
* сборники произведений: энциклопедии, антологии, атласы и другие составные произведения как результат творческого труда.

Компьютерные программы (все виды программ)

* прикладные программы и операционные системы на любом языке и в любой форме, включая исходный текст и объектный код.
* Базы данных или компиляции иных материалов в любой форме, представляющие собой по подбору и расположению материалов результат интеллектуального творчества.

Авторские нрава распространяются на:

* произведения, обнародованные (либо необнародованные, но находящиеся в какой-либо объективной форме) на территории РБ, независимо от гражданства авторов и их правопреемников;
* произведения авторов-граждан РБ (и их правопреемников), обнародованные (либо необнародованные, но находящиеся в какой-либо объективной форме) за пределами РБ;
* произведения авторов- фаж дан других государств (и их правопреемников), обнародованные (либо необнародованные, но находящиеся в какой-либо объективной форме) за пределами РБ - в соответствии с международными договорами РБ.

1. **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).
* Принадлежат автору независимо от его имущественных прав и сохраняются за ним даже после уступки исключительных прав на использование произведения.

1. **Личные 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. **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. **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.

Автор вправе указать лицо, на которое он возлагает охрану своих личных неимущественных прав после своей смерти и осуществляет свои полномочия пожизненно. При отсутствии указаний охрана осуществляется его наследниками или специально уполномоченным государственным органом РБ при отсутствии наследников.

1. **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.

Но недееспособные, став субъектами авторского права, не имею; права самостоятельно совершать какие-либо сделки, связанные с использованием авторского права. Несовершеннолетние в возрасте от 14 до 18 лет могут самостоятельно осуществлять авторские права на свои произведения.

Субъектами авторского права после смерти автора становятся наследники. Наследование авторских прав может происходить как по закону, так и по завещанию.

1. **Авторский договор** разрешает использование произведения определенным способом и в установленных договором пределах только лицу или лицам, которому эти нрава передаются, и дает такому лицу право запрещать подобное использование произведения другим лицам.

Выступая в качестве особого вида гражданско-правового договора, авторский договор, в свою очередь, подразделяется на ряд разновидностей, каждая из которых имеет свои особенности.

1. **Распространенные виды авторских договоров**

Наиболее распространенным видом авторского договора является **издательский договор**. В рамках данного договора осуществляется издание и переиздание любых произведений, которые могут быть зафиксированы на бумаге, т.е. произведений литературы (научных, художественных, учебных и т.п.), драматических, сценарных, музыкальных произведений, произведений изобразительного искусства и т.д. Издательский договор наиболее полно урегулирован действующим законодательством и исследован юридической наукой.

**Постановочный договор** заключается тогда, когда основным способом использования произведения является его публичное исполнение. Его предметом могут быть драматические произведения, музыка или либретто оперы, балета, оперетты, музыка к драматическому спектаклю и т.п., которые используются театрально-зрелищными организациями (театрами, филармониями, цирками, концертными организациями и т.д.) путем постановки на сцене. В настоящее время постановочный договор должен заключаться пользователями в отношении как необнародованных, так и обнародованных произведений.

**Сценарный договор** - это договор, который регламентирует отношения, связанные с использованием текста, по которому снимается кинофильм, телефильм, делается радио- или телепередача, проводится массово-зрелищное мероприятие и т.д. Сценарный договор близок к постановочному договору, из рамок которого он постепенно выделился в самостоятельный вид. Их основное различие заключается в том, что литературный сценарий в отличие, например, от драматического произведения используется не в своем неизменном виде, а служит основой для создания более приближенного к нуждам кинематографа, телевидения или радио режиссерского сценария, по которому, собственно, и ставится фильм или делается передача. В этом смысле сценарный договор предполагает, что произведение (сценарий) может быть использовано в измененном виде.

**Договор о депонировании рукописи** регулирует условия и порядок обнародования и последующего использования произведения, которое помещается на хранение в специальный информационный орган. Обычно путем депонирования используются научные произведения, представляющие интерес лишь для ограниченного круга специалистов, но запросам которых им предоставляются копии депонированных произведений или их отдельных частей.

**Договор художественного заказа** опосредует отношения, связанные с созданием произведений изобразительного искусства в целях их публичной демонстрации. Его предметом являются разнообразные произведения изобразительного искусства, которые изготавливаются авторами по заказам организаций и частных лиц и переходят в собственность последних. Владельцы произведений (материальных носителей) вправе распоряжаться ими по своему усмотрению, но при условии уважения авторских прав создателей авторских произведений.

**Договор об использовании в промышленности произведений декоративно-прикладного искусства** имеет своей задачей урегулирование вопросов, возникающих в связи с тиражированием в промышленности оригинальных произведений декоративно-прикладного искусства. Он заключается лишь с внештатными художниками предприятий, произведения которых принимаются к использованию. Авторы получают вознаграждение как за сам факт создания произведения, принятого к использованию, так и за последующее тиражирование в зависимости от объема использования.

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**, а также **другие условия**, которые стороны сочтут необходимыми.

**Практическое занятие №10**

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

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

**Задание для выполнения.**

Ответить на следующие вопросы:

1. Основные составляющие описания изобретения?
2. Правила оформления описания изобретения?
3. Какие основные пункты должна содержать заявка на изобретение?
4. Основные документы, необходимые для подачи заявки на изобретения?
5. ОТЛИЧИЯ заявок на охранные документы различных объектов промышленной собственности?
6. На какие ОПС выдаются патенты?
7. На какие ОПС выдаются свидетельства?

**Ответы на вопросы**

1. **Описание изобретения** начинается с названия изобретения и указания индекса или индексов рубрики действующей редакции международной патентной классификации, к которой относится заявляемое изобретение и содержит следующие разделы:

* 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. Названия разделов в тексте описания не указываются.

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.

В разделе «Уровень техники» приводятся сведения об аналогах и прототипах.

В разделе «Особенности изложения описания устройства» приводится описание устройства в статическом состоянии со ссылками на фигуры чертежей и цифровые обозначения конструктивных элементов. Цифровые обозначения соответствующих частей, узлов, деталей проставляются но мере их упоминания, в порядке их возрастания, начиная с 1. Этими же числовыми обозначениями должны быть помечены упомянутые части, узлы и детали на чертежах или других графических материалах.

При описании устройства в статическом состоянии должны быть указаны все части, узлы и детали, составляющие данную конструкцию и показанные на чертеже, пояснены их названия, связи и взаимное расположение. В этой части описания должны быть подробно изложены конструктивные, а также при необходимости технологические особенности заявленного устройства.

После описания устройства в статическом состоянии описывается действие (работа) устройства или способ его использования со ссылкой на цифровые обозначения, ранее упомянутых частей, узлов, деталей. При этом цифровые обозначения упоминаются в любом порядке, удобной для изложения данной части раздела.

После описания устройства в действии приводятся другие примеры описания этого устройства, если они имеются с характеристикой тех или иных преимуществ.

Формула изобретения печатается на отдельном листе и подписывается заявителем или уполномоченным на это лицом. Передачу таких полномочий подтверждает соответствующий документ.

Формула может быть одно и многозвенной и включать соответственно один или несколько пунктов.

Однозвенная формула применяется для характеристики одного изобретения совокупностью существенных признаков не имеющей развития или уточнения применительно к частным случаям его выполнения или использования.

Многозвенная формула применяется для характеристики одного изобретения с развитием и (или) уточнением совокупности его существенных признаков применительно к частным случаям выполняется или использования изобретение. Она имеет независимый и следующие за ним зависимые пункты.

Независимый пункт включает совокупность признаков достаточных для получения технического результата. Он состоит, как правило, из ограничительной и отличительной частей. Ограничительная часть включает существенные признаки, совпадающие с признаками прототипа, в том числе и название, отражающее назначение изобретения. Отличительная часть включает существенные признаки, которые отличают изобретение от прототипа.

При составлении пункта формулы после изложения ограничительной части вводится словосочетание «отличающееся тем, что», непосредственно после которого излагается отличительная часть.

1. **Основные пункты, которые должна содержать заявка на изобретение** есть пункты описания, уровня техники, особенностей изложения описания устройства в статическом состоянии и движении, независимый пункт и пункт формулы изложения.
2. **Основные документы, необходимые для подачи заявки на изобретения.**

Заявка подается в трех экземплярах и должна содержать:

* заявление о выдаче патента (типовой бланк);
* описание изобретения, раскрывающее его с полнотой достаточной для осуществления изобретения;
* формулу изобретения, выражающую его сущность и полностью основанную на описании;
* чертежи и иные материалы, если они необходимы для понимания сущности изобретения;
* реферат;
* доверенность в случае подачи заявки патентным поверенным;
* вместе с заявкой (и указанными выше документами) или не позднее 2-х месяцев с даты ее подачи в одном экземпляре предоставляется документ, подтверждающий уплату пошлины в установленном размере или освобождение от уплаты, либо наличие оснований для уменьшения ее размера.

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

**Подача заявки на изобретение (20 лет):**

Заявка на выдачу патента на изобретение подается автором изобретения, нанимателем, если изобретение служебное, физическим или юридическим лицом, которым автор или наниматель передает на договорной основе свое право на подачу заявки или к которому они перешли в соответствии с законодательством Республики Беларусь в наследовании. Она может быть передана через служебного поверенного, зарегистрированного в патентном органе.

Заявки, поступившие в патентный орган, назад не возвращаются.

Заявка подается в трех экземплярах и должна содержать:

* заявление о выдаче патента (типовой бланк);
* описание изобретения, раскрывающее его с полнотой достаточной для осуществления изобретения;
* формулу изобретения, выражающую его сущность и полностью основанную на описании;
* чертежи и иные материалы, если они необходимы для понимания сущности изобретения;
* реферат;
* доверенность в случае подачи заявки патентным поверенным.

Заявление о выдаче патента оформляется на русском языке. Остальные документы на белорусском, русском или другом языке.

В заявлении о выдаче патента указываются сведения о названии изобретения, заявителях и авторах, дате подачи заявки, адресе для переписки, перечня прилагаемых документов и др. Заявление представляется по установленной НЦИС форме.

Временная правовая охрана заявленному изобретению предоставляется с даты публикации заявки до даты публикации сведений о патенте. До даты публикации сведений о заявке на изобретение но не позднее даты получения решения о выдаче патента на изобретение возможно по ходатайству преобразование заявки на изобретение в заявку на полезную модель.

Заявку на полезную модель преобразовать в заявку на изобретение возможно до даты получения решения о выдаче патента на полезную модель.

**Подача заявки на полезную модель (10 лет):**

Полезной моделью признается техническое решение, относящееся к устройствам и являющееся новым и промышленно применимым. К устройствам относятся конструкции и изделия.

Заявка на полезную модель должна относиться к одной полезной модели или гpyппу полезных моделей, связанных между собой так, что они образуют единый творческий замысел (требование единства полезной модели).

Заявка на полезную модель должна содержать:

* заявление о выдаче патента с указанием автора (соавторов) полезной модели и лица (лиц), на имя которого (которых) испрашивается патент;
* описание полезной модели, раскрывающее ее с полнотой, достаточной для осуществления;
* формулу полезной модели, выражающую ее сущность и полностью основанную на описании;
* чертежи;
* реферат.

К заявке прилагаются следующие документы:

* 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).

При экспертизе заявки на полезную модель проверка соответствия заявленной полезной модели условиям патентоспособности не осуществляется.

**Подача заявки на промышленный образец (5 лет):**

Промышленный образец представляет собой художественное или художественно-конструкторское решение, определяющее внешний вид изделия.

Заявка должна относиться к одному промышленному образцу и может включать его варианты (требование единства промышленного образца).

Заявка должна содержать:

* 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. К заявке прилагаются документы:
* 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).

При экспертизе заявки на промышленный образец проверка соответствия заявленного промышленного образца условиям патентоспособности не осуществляется.

**Подача заявки на товарный знак (10 лет):**

Товарные знаки и знаки обслуживания представляют собой обозначения, которые способствуют отличию тоываров или услуг одних юридических или физических лиц от однородных товаров или услуг других юридических или физических лиц.

На каждый товарный знак или знак обслуживания должна быть оформлена отдельная заявка на специальном бланке. Заявка должна содержать сведения о заявителе. В заявке должен быть указан перечень товаров и услуг, для которых регистрируется товарный знак или знак обслуживания. В заявке может содержаться несколько классов товаров и услуг в соответствии с Международной классификацией товаров и услуг (МКТУ). К заявке прилагается графическое изображение товарного знака и описание (при необходимости) с указанием цвета или цветового сочетания, в котором испрашивается регистрация.

К заявке прилагается документ, подтверждающий уплату патентной пошлины в установленном размере.

Союзы, ассоциации и другие объединения юридических лиц могут регистрировать коллективные товарные знаки. Коллективный товарный знак и право на его использование не могут быть переданы другим лицам.

**Подача заявки на регистрацию топологии интегральной микросхемы (10 лет):**

Заявка должна содержать документы:

* заявление о выдаче свидетельства;
* депонируемые материалы, содержащие комплект одного из следующих видов материалов: фотографии фотошаблонов; сборочный Топологический чертеж; послойные топологические чертежи; фотографии каждого слоя топологии;
* образцы ИМС с данной топологией в случае использования ее до даты подачи заявки;
* реферат;
* доверенность (в случае подачи через патентного поверенного).

К заявке прилагается 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.

1. **На какие ОПС выдаются патенты**.

Патентная деятельность, полезные модели, промышленные образцы, интегральных микросхем, компьютерные программы, способы, вещества, биотехнологические продукты, применение всего вышеперечисленного.

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

Открытия, научные теории, математические методы, товарные знаки, географические указания.

**Практическое занятие №11**

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

Цель: Изучить виды, содержание и порядок проведения патентных исследований.

**Задание для выполнения.**

В результате проведения исследовательских работ по определению расстояния, было предложено создание цифровой фотокамеры, внешний вид которой представлен на рисунке 1.

|  |  |
| --- | --- |
|  | Наличие предполагаемых существенных признаков и планируемый выпуск продукции являются предпосылками для патентования разработки.  Необходимо выполнить экспертизу патентной чистоты разработанного конструктивного решения (ОПС). |
| Рисунок 1 – Способ определения расстояния до объекта посредством цифровой фотокамеры |

В качестве существенных признаков при патентовании предполагаемого изобретения, выносится конструктивный признак: в способе определения расстояния до объекта посредством цифровой фотокамеры указанная фотокамера с известным фокусным расстоянием направляется в сторону исследуемого объекта, совмещается перекрестие объектива, жестко соединенное с фотокамерой коллиматора, оптическая ось которого перпендикулярна оптической оси фотокамеры, с любым попавшим в поле зрения тест-объектом, получается первое цифровое фотографическое изображение исследуемого объекта. Далее фотокамера перемещается по горизонтали вдоль оптической оси коллиматора на заданное расстояние, вновь совмещается перекрестие объектива коллиматора с тем же тест-объектом и получается второе цифровое фотографическое изображение исследуемого объекта. На полученных изображениях формируют по окну сканирования с одинаковыми координатами и размерами по горизонтали и вертикали соответственно, осуществляют сканирование одного окна относительно другого.

*Выполнение задания*. Для выявления патентной чистоты разработанного объекта промышленной собственности следует использовать следующий регламент поиска:

* объект – *цифровая фотокамера, определяющая расстояние до объекта;*
* страна поиска – *Республика Беларусь*;
* источники информации – *патентные*;
* ретроспективность – *2014 г.*;

информационная база – *База патентов Беларуси* https://bypatents.com/4-18666-sposob-opredeleniya-rasstoyaniya-do-obekta-posredstvom-cifrovojj-fotokamery.html#about

Для проведения патентного поиска необходимо определить классификационную рубрику предполагаемого изобретения, которая в данном случае, классифицируется по разделу **«ФИЗИКА»**, класс **«G01 Измерение; испытание».**

Проведенный патентный поиск по указанному классу, выявил следующие аналогичные по конструктивному выполнению патенты и полезные модели, приведенные на рисунках 2 – 5:

|  |  |
| --- | --- |
|  |  |
| Рисунок 2 – Устройство для определения углов наклона объектов Номер патента: 485308 | Рисунок 3 – Способ определения расстояния до объекта  Номер патента: 17251 |
|  |  |
| Рисунок 4 – Способ определения дальности до объекта и его скорости посредством цифровой фотокамеры. Номер патента: 16674 | Рисунок 5 – Способ измерения дальности до объекта посредством двухволнового лазера. Номер патента: 11972 |

Все данные по обнаруженным патентам-аналогам сводятся в соответствующую таблицу.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Таблица 6 – Патентная документация | | | | |
| 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 охран-ного документа или причина его аннулирования (только для анализа патентной чистоты) |
| Приборы по измерение расстояний, горизонтов или азимутов; топография, навигация; гироскопические приборы; фотограм-метрия или видеограм-метрия | Патент СССР  № 485308  МПК G01C 9/36. | Горгураки В.Ф., Карпов Ю.В., Севериновский М.Л.  Заявка 1875652, от 26.01.1973, опубл. 25.09.1975 | «Устройство для определения углов наклона объектов» | Неизвестно |
| Патент РБ  № 17251  МПК  G01C 3/00. | Козлов В.Л.  Заявка a20111225 от 28.02.2012, опубл. 30.06.2013 | «Способ определения расстояния до объекта» | Действует |
| Патент РБ  № 16674  МПК G01C 3/00. | Козлов В.Л.  Заявка a20110382 от 28.03.2011, опубл. 30.12.2012 | «Способ определения дальности до объекта и его скорости посредствомцифровой камеры» | Действует |
| Патент РБ  № 11972  МПК G01C 3/08. | Козлов В.Л.  Заявка a20071440 от 27.11.2007, опубл. 30.06.2009 | «Способ измерения дальности до объекта посредством двухволнового лазера» | Действует |

Дальнейший анализ сущности обнаруженной патентной информации, выполняемой специалистами, позволяет определить наличие существенных отличий и возможность получения патента на изобретение или полезную модель.

**Практическое занятие №12**

**Тема «Патентный поиск»**

Цель: освоить навыки проведения патентного поиска по заданной тематике.

**Задание для выполнения.**

#### Провести патентный поиск по теме своего курсового проекта.

**Выполнение**

Поиск осуществлялся в категории «Агрегатор записей» в Google Patents.

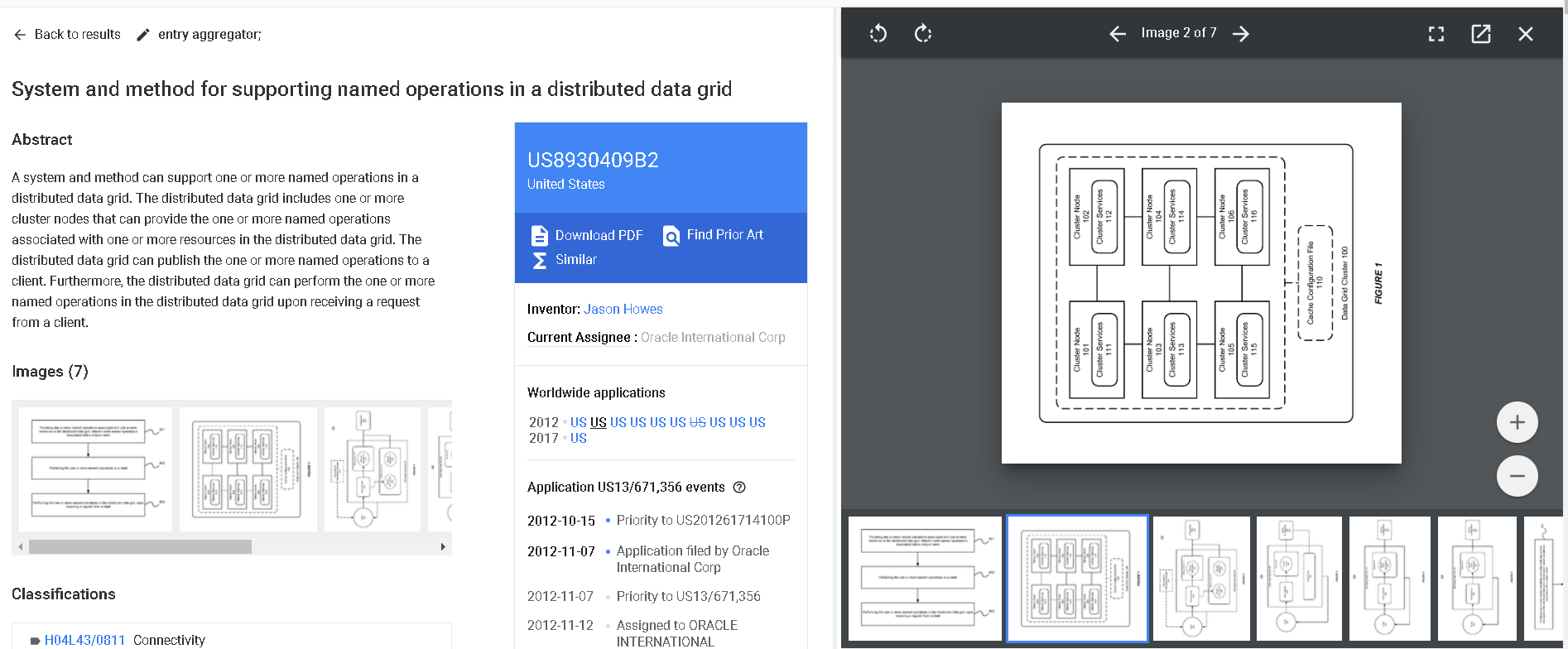


Рисунок 1.

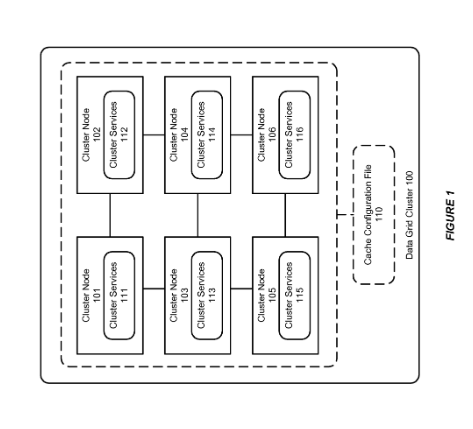


Рисунок 2.

Система и метод могут поддерживать одну или несколько именованных операций в распределенной сетке данных. Распределенная сетка данных включает один или несколько узлов кластера, которые могут предоставлять одну или несколько именованных операций, связанных с одним или несколькими ресурсами в распределенной сетке данных. Распределенная сеть данных может публиковать одну или несколько именованных операций для клиента. Кроме того, распределенная сеть данных может выполнять одну или несколько именованных операций в распределенной сети данных при получении запроса от клиента.

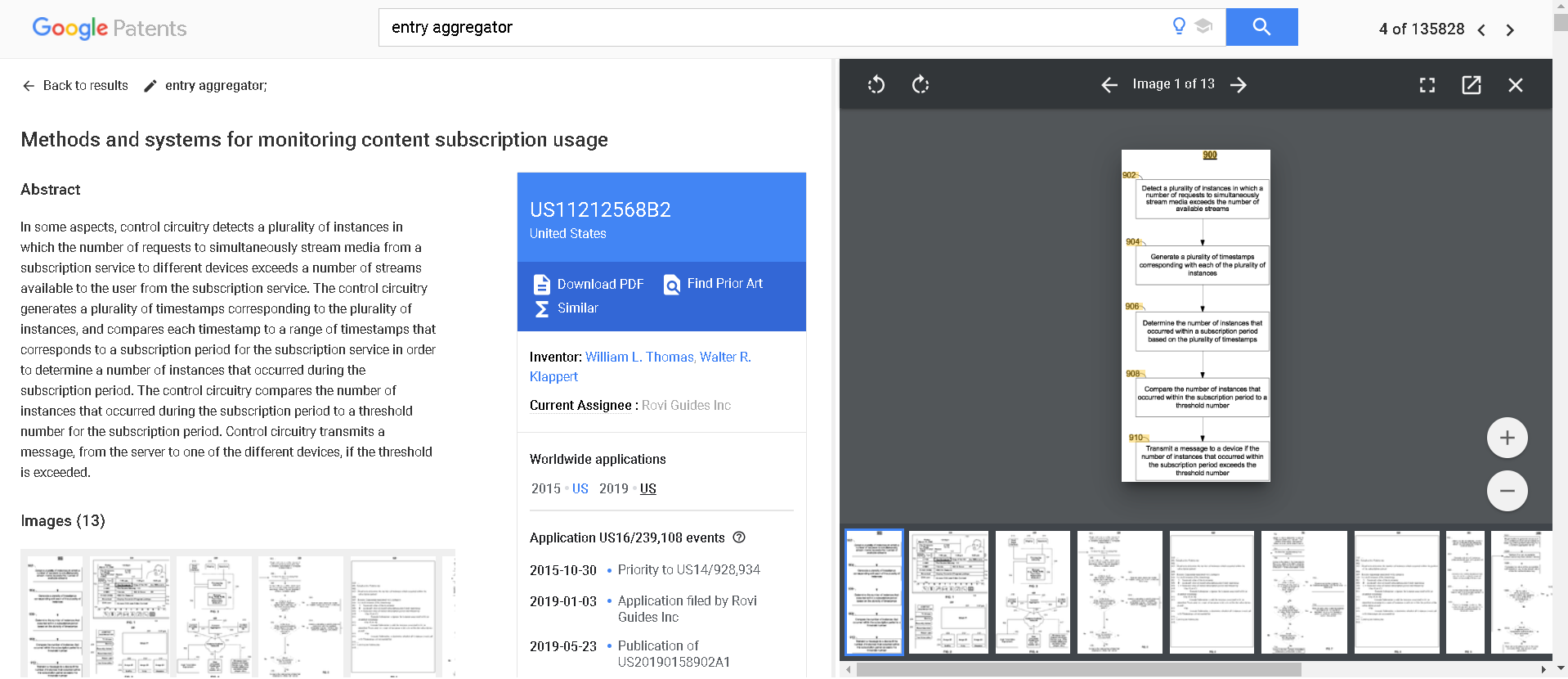


Рисунок 3.

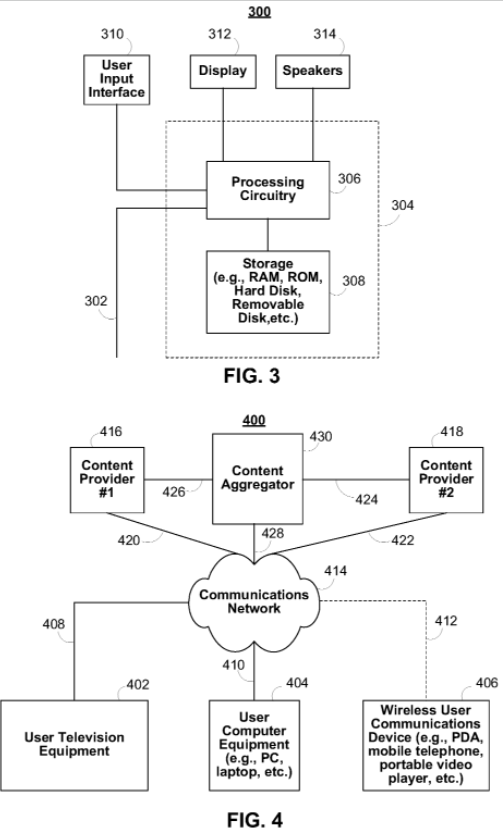


Рисунок 4.

В некоторых аспектах схема управления обнаруживает множество случаев, в которых количество запросов на одновременную потоковую передачу медиа из службы подписки на различные устройства превышает количество потоков, доступных пользователю из службы подписки. Схема управления генерирует множество временных меток, соответствующих множеству случаев, и сравнивает каждую временную метку с диапазоном временных меток, который соответствует периоду подписки для службы подписки, чтобы определить количество случаев, которые произошли в течение периода подписки. Схема управления сравнивает количество экземпляров, произошедших в течение периода подписки, с пороговым числом для периода подписки. Схема управления передает сообщение с сервера на одно из различных устройств, если пороговое значение превышено.

**Практическое занятие №13**

**Тема «Настройка антивирусов»**

Цель: Овладение навыками настройки и использования различных антивирусов.

**Задание к выполнению**

Установка антивирусной программы «Kaspersky»

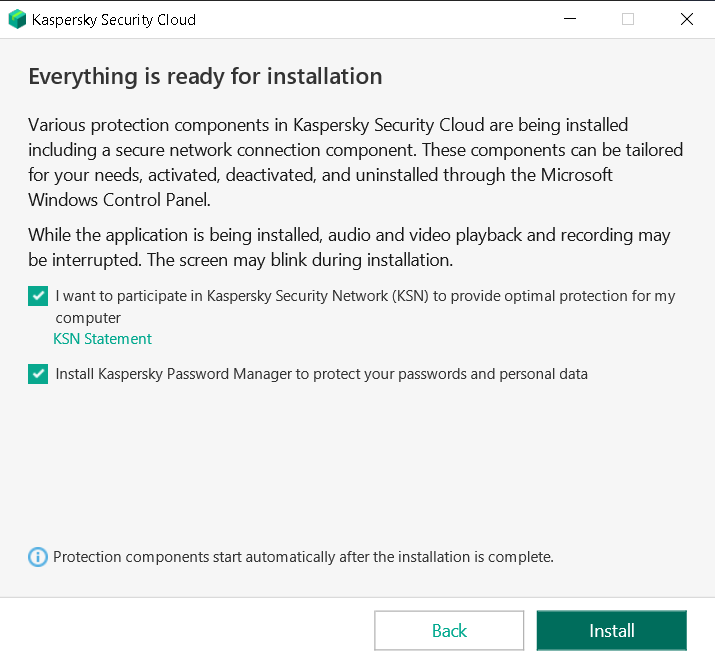


Рисунок 1.

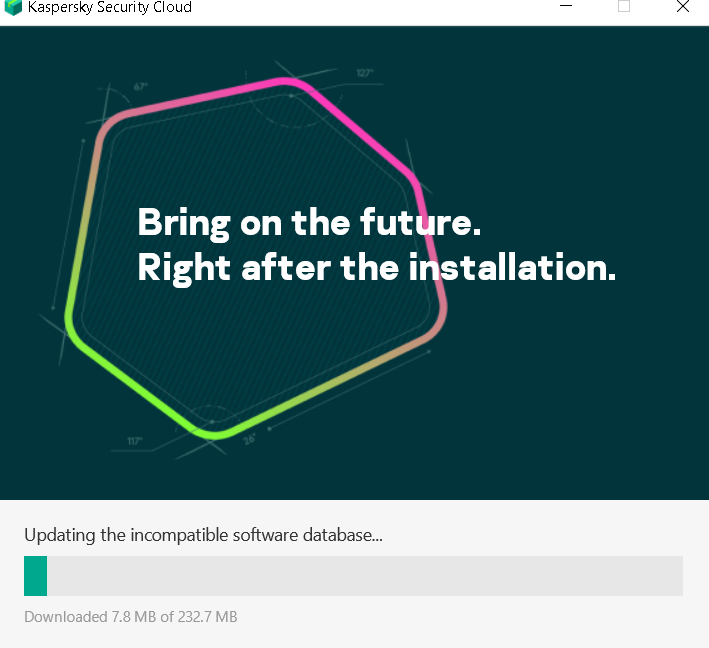


Рисунок 2.

Обновление базы данных сигнатур вирусов.

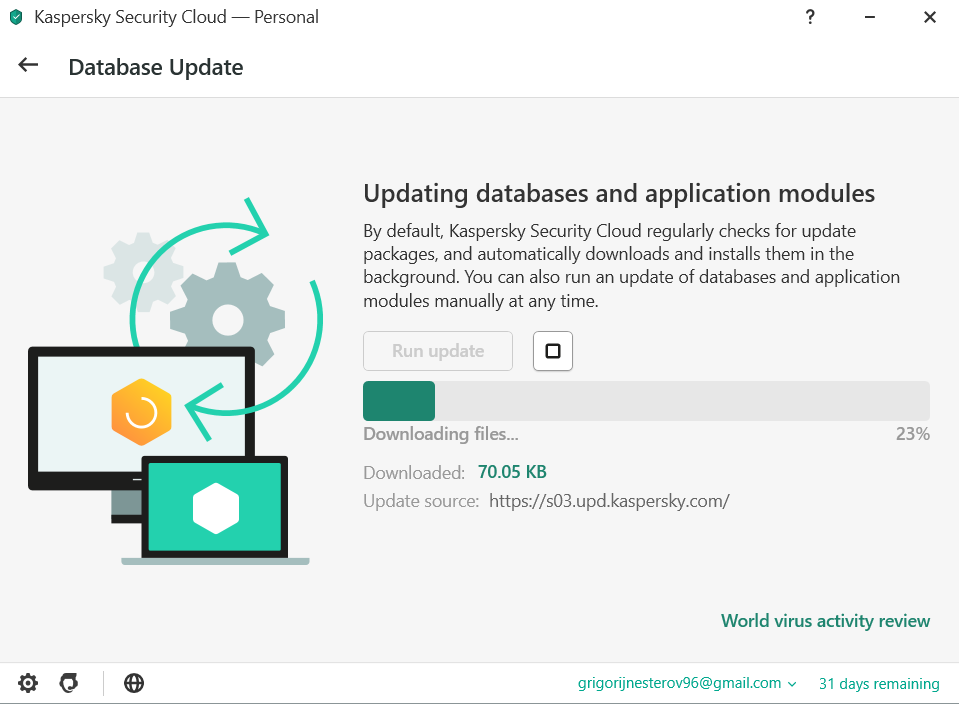


Рисунок 3.

Сканирование дисков.

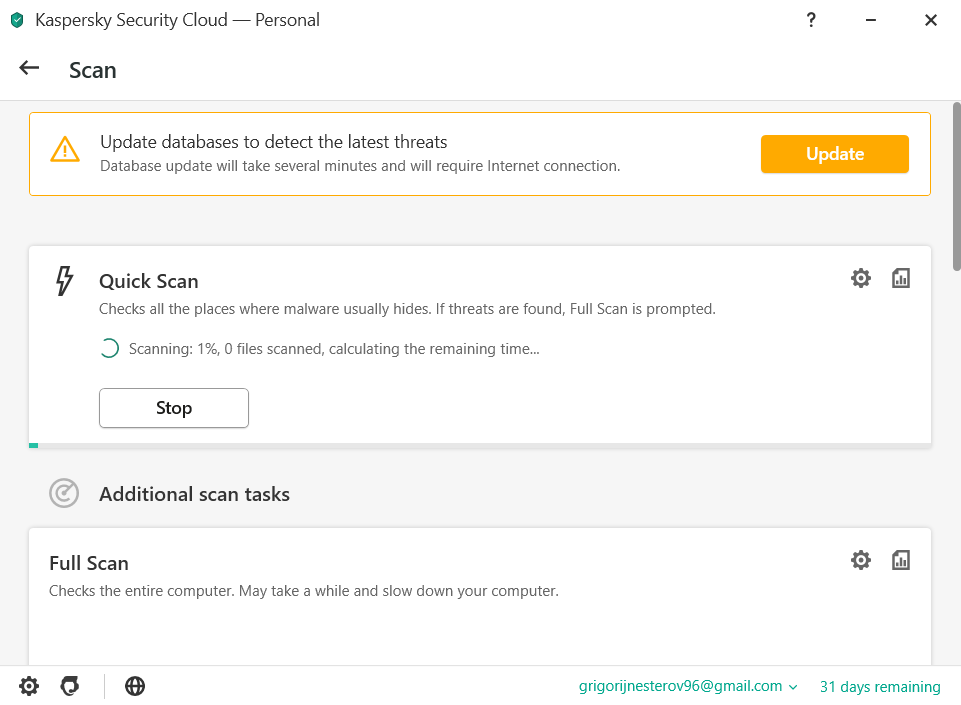


Рисунок 4.

**Практическое занятие №14**

**Тема «Изучение стандартных средств для реализации приложений, использующих симметричное и ассиметричное шифрование с использованием библиотеки 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

**Контрольные вопросы:**

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

Цезаря, Трисемуса, Плейфейра, Виженера.

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

Эль-Гамаля, RSA, Деффи-Хеллмана.

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

В .NET классы в [System.Security.Cryptography](https://docs.microsoft.com/ru-ru/dotnet/api/system.security.cryptography) пространстве имен управляют множеством сведений о криптографии.

NET Framework предоставляет реализацию многих стандартных криптографических алгоритмов. Эти алгоритмы просты в использовании и по умолчанию имеют наиболее безопасные из возможных значений свойств.

В целом открывает доступ к криптографическим сервисам. Можно шифровать и расшифровывать данные, обеспечивать их целостность и получать цифровую подпись.

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

Значения длины ключа и вектора инициализации могут использоваться для определения начальных точек и длин всех частей пакета шифрования, которые затем могут использоваться при расшифровке файла.

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

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

Класс RSACryptoServiceProvder - выполняет шифрование и дешифрование данных с помощью реализации асимметричного алгоритма RSA, предоставляемого поставщиком служб шифрования (CSP). Позволяет выполнить экспорт, импорт данных ассиметричной пары ключей.

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

Класс CryptoStream – определяет поток, который связывает потоки данных с криптографическими преобразованиями.

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