Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Электронная тетрадь**

по Основам Защиты Информации

Студент: Белявский Т.С.

ФИТ 2курс 2 группа

Преподаватель: Берников В. О.

Минск 2021

**Практическое занятие №1**

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

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

**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 интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере;

**2.** К основным национальным интересам относятся: реализация конституционных прав граждан на получение, хранение и распространение полной, достоверной и своевременной информации, формирование и развитие информационного общества, утверждение равноправного участия Республики Беларусь в мировых информационных отношениях, преобразование информационной индустрии в экспортно-ориентированный сектор экономики, реализация эффективного информационного обеспечения государственной политики, обеспечение надежности и устойчивости функционирования критически важных объектов информатизации.

**3.** К основным угрозам национальной безопасности относятся: нарушение функционирования критически важных объектов информатизации, деструктивное информационное воздействие на личность, общество и государственные институты, наносящее ущерб национальным интересам, недостаточные масштабы и уровень внедрения передовых информационно-коммуникационных технологий, снижение или потеря конкурентоспособности отечественных информационно-коммуникационных технологий, информационных ресурсов и национального контента.

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

Также внешними источниками информации являются: открытость и уязвимость информационного пространства Республики Беларусь от внешнего воздействия, доминирование ведущих зарубежных государств в мировом информационном пространстве, информационная деятельность зарубежных государств, международных и иных организаций, отдельных лиц, наносящая ущерб национальным интересам Республики Беларусь, 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.

**5.** В политической 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:** в ходе практического занятия я изучил концепцию национальной безопасности РБ и ознакомился с указами президента РБ.

**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 объектa; возрастающая.

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

**Задача:** решить задачу разработки средств защиты для обеспечения максимальной эффективности объекта в условиях несанкционированного доступа.

**Исходные данные**: E0 =20000(руб.) E =18000(руб.) K=10 C=1000(руб.).

Рассчитаем ∆E: ∆𝐸=𝐸0−𝐸=20000-18000=2000(руб.)

Находим значение относительной эффективности функционирования:



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

(руб).

Находим эффективность функционирования:

(руб).

Найдём относительную эффективность функционирования:



В том случае, если эффективность функционирования имеет стоимостное значение:

(руб).

**Вывод:** 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**

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

**Цель:** 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.

Зместитель начальника

Плановый отдел

Почтовые отделения

Пенсионный отдел

Бухгалтерия

Экономист

Специалист пенсионного отдела

Специалист почтового отделения

Бухгалтер

Начальник

Главный бухгалтер

Специалист по доставке

Оператор

Программист

Страховой агент

Отдел доставки

ИТ отдел

Отдел подписки

Страховой отдел

Инженер

Отдел эксплуатации

Рис. 3.1 – Модель структуры предприятия

Начальник осуществляет общее руководство компанией, является её официальным представителем, а также Организует техническую подготовку производства (строительства) или других видов основной деятельности предприятия. Осуществляет руководство текущим и перспективным планированием технического развития предприятия, его производственной базы. Руководит составлением технических заданий на проектирование вновь строящихся производств, сооружений, технических средств, расширение, развитие и реконструкцию действующих, на внедрение средств автоматизации, механизации. Рассматривает и согласовывает проектно-конструкторскую документацию по модернизации оборудования и рационализации рабочих мест. Осуществляет технический надзор за выполнением строительно-монтажных работ, приемку работ и законченных объектов. Разрабатывает мероприятия по повышению производительности работ и более эффективному использованию производственных мощностей. Контролирует производство продукции в соответствии с заказами. Организует и контролирует закупки сырья и материалов (план поставок), необходимый запас сырья и материалов. Организует производственный учет. Организует техническое обслуживания и ремонт оборудования. Организует ведение технической и другой предусмотренной законодательством документации (по технике безопасности, противопожарной безопасности и т.д.).

Заместитель руководителя по производству находится в подчинении руководителя предприятия, организует своевременный выпуск качественной продукции службами и подразделениями предприятия, которые находятся в его подчинении, обеспечивает внедрение в производство новейших систем и методик организации и планирования производства.

руководство исполнением отдельных указаний по производству продукции целевого назначения. Руководство, контроль и организация работы цехов, занимающихся сбором отходов цветных и черных металлов и по выпуску новых изделий. Обеспечение внедрения и соблюдения установленных технических условий и стандартов, а также применения новейших методов и средств испытаний и измерений в процессе производства продукции, обеспечение контроля над состоянием и работой средств измерений и соблюдения определенного порядка их эксплуатации и использования. Участие в разработках и осуществление мер производства конкурентоспособной продукции, регулярный анализ ее технического уровня. Участие в разработках предложений о снятии с производства продукции, которая не пользуется спросом. Внедрение работу цехов современных методов планирования и организации производства, обеспечение условий для работ с высокой производительностью, обеспечение соблюдения законов о труде, норм и правил охраны труда, промышленной санитарии и техники безопасности. Подготовка распоряжений по вопросам, которые касаются его компетенции в области производства изделий, процесса и сроков их изготовления и прочим вопросам, которые обязательны к исполнению начальником участков и цехов и начальником производства.

Главный бухгалтер подчиняется непосредственно руководителю организации. При постановке и ведении бухгалтерского учета главный бухгалтер должен следовать нормам действующего законодательства, выполнять указания и распоряжения руководителя организации, а также лица, уполномоченного на это письменным указанием руководителя. Таким письменным указанием может быть должностная инструкция главного бухгалтера.

Все множество потенциальных угроз безопасности информации делится на три класса по природе их возникновения: антропогенные, техногенные и естественные(природные).

Возникновение антропогенных угроз обусловлено деятельностью человека. Среди них можно выделить угрозы, возникающие вследствие как непреднамеренных (неумышленных) действий: угрозы, вызванные ошибками в проектировании информационной системы и ее элементов, ошибками в действиях персонала, так и угрозы, возникающие в силу умышленных действий, связанные с корыстными, идейными или иными устремлениями людей.

Возникновение техногенных угроз обусловлено воздействиями на объект угрозы объективных физических процессов техногенного характера, технического состояния окружения объекта угрозы или его самого, не обусловленных напрямую деятельностью человека. К техногенным угрозам могут быть отнесены сбои, в том числе в работе, или разрушение систем, созданных человеком.

Возникновение естественных (природных) угроз обусловлено воздействиями на объект угрозы объективных физических процессов природного характера, стихийных природных явлений, состояний физической среды, не обусловленных напрямую деятельностью человека.

К естественным (природным) угрозам относятся угрозы метеорологические, атмосферные, геофизические, геомагнитные, включая экстремальные климатические условия, метеорологические явления, стихийные бедствия. Источники угроз по отношению к инфраструктуре Главпочтамта могут быть как внешними, так и внутренними.

Источниками внутренних угроз являются: сотрудники организации, программное обеспечение, аппаратные средства.

Внутренние угрозы могут проявляться в следующих формах: ошибки пользователей и системных администраторов, нарушения сотрудниками Главпочтамта установленных регламентов сбора, обработки, передачи и уничтожения информации, ошибки в работе программного обеспечения, отказы и сбои в работе компьютерного оборудования.

К внешним источникам угроз относятся:компьютерные вирусы и вредоносные программы, организации и отдельные лица, стихийные бедствия.

По способам воздействия на объекты информационной безопасности угрозы подлежат следующей классификации:информационные,программные, физические.

К информационным угрозам относятся: несанкционированный доступ к информационным ресурсам, незаконное копирование данных в информационных системах, хищение информации из архива, отделов и баз данных, нарушение технологии обработки информации, противозаконный сбор и использование информации, использование информационного оружия.

К программным угрозам относятся: использование ошибок и «дыр» в ПО, компьютерные вирусы и вредоносные программы.

К физическим угрозам относятся: уничтожение или разрушение средств обработки информации и связи, хищение носителей информации, хищение программных или аппаратных ключей и средств криптографической защиты данных, воздействие на персонал (шантаж, нападение).

Специфические угрозы безопасности: возможность отключения электричества, что приведет к сбою незавершенных операций и потере данных. Угроза возникновения неправильной адресации пакетов. Угроза проникновения на рабочие места сотрудников людей, не являющихся работниками отделов, которые имеют туда доступ, и попадания на Главпочтамт предметов, способных нанести ущерб. Угроза доступа в эксплуатационный отдел, могут быть нарушены эксплуатационные планы. Угроза изменения базы данных людей, получающих пенсию, в следствии чего не только главпочтамту, но и обществу будет нанесен урон. Угроза доступа в ИТ-отделе.

**Разработка мер защиты**

**Целями защиты информации являются:** предотвращение утечки, хищения, утраты, искажения, подделки информации; предотвращение несанкционированных действий по уничтожению, модификации, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы.

При разработке политики безопасности можно использовать следующую модель (рис. 1), основанную на адаптации Общих Критериев (ISO 15408) и проведении анализа риска (ISO 17799).

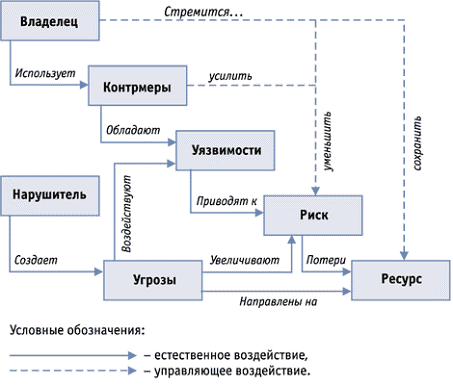


Рис. 3.2 – Модель построения корпоративной системы защиты информации.

Представленная модель – это совокупность объективных внешних и внутренних факторов и их влияние на состояние информационной безопасности на объекте и на сохранность материальных или информационных ресурсов.

Рассматриваются следующие объективные факторы: угрозы информационной безопасности, характеризующиеся вероятностью возникновения и вероятностью реализации; уязвимости информационной системы или системы контрмер (системы информационной безопасности), влияющие на вероятность реализации угрозы; риск – фактор, отражающий возможный ущерб организации в результате реализации угрозы информационной безопасности: утечки информации и ее неправомерного использования (риск в конечном итоге отражает вероятные финансовые потери – прямые или косвенные).

Для создания эффективной политики безопасности предполагается первоначально провести анализ рисков в области информационной безопасности. Затем определить оптимальный уровень риска для предприятия на основе заданного критерия. Политику безопасности и соответствующую корпоративную систему защиты информации предстоит построить таким образом, чтобы достичь заданного уровня риска.

Предлагаемая методика разработки политики информационной безопасности современного предприятия позволяет полностью проанализировать и документально оформить требования, связанные с обеспечением информационной безопасности, избежать расходов на излишние меры безопасности, возможные при субъективной оценке рисков, оказать помощь в планировании и осуществлении защиты на всех стадиях жизненного цикла информационных систем, обеспечить проведение работ в сжатые сроки, представить обоснование для выбора мер противодействия, оценить эффективность контрмер, сравнить различные варианты контрмер.

В ходе работ должны быть установлены границы исследования. Для этого необходимо выделить ресурсы информационной системы, для которых в дальнейшем будут получены оценки рисков. При этом предстоит разделить рассматриваемые ресурсы и внешние элементы, с которыми осуществляется взаимодействие. Ресурсами могут быть средства вычислительной техники, программное обеспечение, данные, а также информационные ресурсы – отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (архивах, фондах, банках данных, других информационных системах). Примерами внешних элементов являются сети связи, внешние сервисы и т.п.

При построении модели будут учитываться взаимосвязи между ресурсами. Например, выход из строя какого-либо оборудования может привести к потере данных или выходу из строя другого критически важного элемента системы. Подобные взаимосвязи определяют основу построения модели организации с точки зрения ИБ.

Эта модель, в соответствии с предлагаемой методикой, строится следующим образом: для выделенных ресурсов определяется их ценность, как с точки зрения ассоциированных с ними возможных финансовых потерь, так и с точки зрения ущерба репутации организации, дезорганизации ее деятельности, нематериального ущерба от разглашения конфиденциальной информации и т.д. Затем описываются взаимосвязи ресурсов, определяются угрозы безопасности и оцениваются вероятности их реализации.

На основе построенной модели можно обоснованно выбрать систему контрмер, снижающих риски до допустимых уровней и обладающих наибольшей ценовой эффективностью. Частью системы контрмер будут рекомендации по проведению регулярных проверок эффективности системы защиты.

Обеспечение повышенных требований к ИБ предполагает соответствующие мероприятия на всех этапах жизненного цикла информационных технологий. Планирование этих мероприятий производится по завершении этапа анализа рисков и выбора контрмер. Обязательной составной частью этих планов является периодическая проверка соответствия существующего режима ИБ политике безопасности, сертификация информационной системы (технологии) на соответствие требованиям определенного стандарта безопасности.

По завершении работ, можно будет определить меру гарантии безопасности информационной среды, основанную на оценке, с которой можно доверять информационной среде объекта. Данный подход предполагает, что большая гарантия следует из применения больших усилий при проведении оценки безопасности. Адекватность оценки основана на вовлечении в процесс оценки большего числа элементов информационной среды объекта, глубине, достигаемой за счет использования при проектировании системы обеспечения безопасности большего числа проектов и описаний деталей выполнения, строгости, которая заключается в применении большего числа инструментов поиска и методов, направленных на обнаружение менее очевидных уязвимостей или на уменьшение вероятности их наличия

**Выводы**

Важно помнить, что прежде чем внедрять какие-либо решения по защите информации необходимо разработать политику безопасности, адекватную целям и задачам современного предприятия. В частности, политика безопасности должна описывать порядок предоставления и использования прав доступа пользователей, а также требования отчетности пользователей за свои действия в вопросах безопасности. Система информационной безопасности (СИБ) окажется эффективной, если она будет надежно поддерживать выполнение правил политики безопасности, и наоборот. Этапы построения политики безопасности – это внесение в описание объекта автоматизации структуры ценности и проведение анализа риска, и определение правил для любого процесса пользования данным видом доступа к ресурсам объекта автоматизации, имеющим данную степень ценности. При этом политику безопасности желательно оформить в виде отдельного документа и утвердить руководством предприятия.

**Практическое занятие №4**

Настройка Брандмауэра Windows

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

**Теоретические сведения**

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

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

К числу таких служб и протоколов относятся:

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

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

**Задания для самостоятельного выполнения**

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. 1.1).

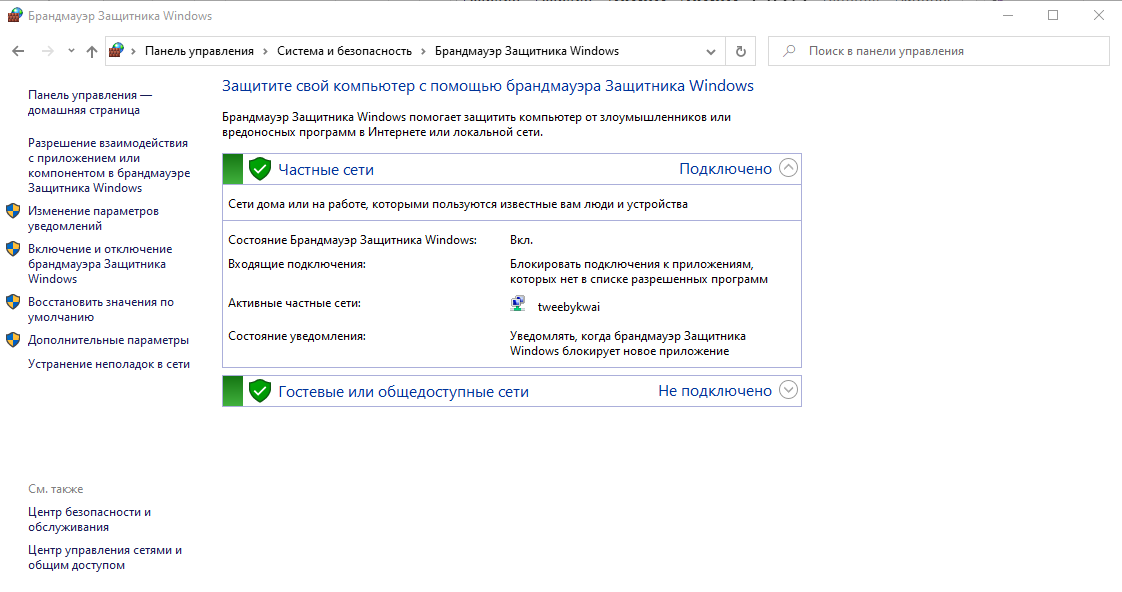


Рисунок 1.1 – Главное окно

В открывшемся окне (рис. 1.2) выбираем в левой панели правила для входящих подключений, затем во вкладке меню «Действие» выбираем «Создать правило», либо нажимаем «Создать правило» в правой панели.

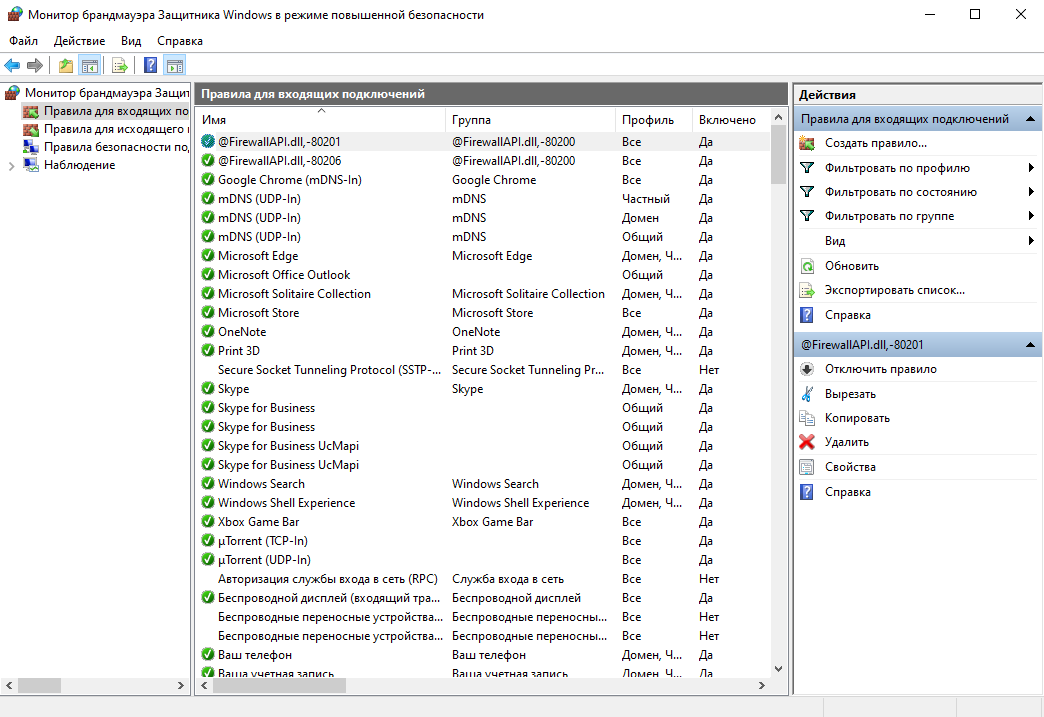


Рисунок 1.2 – Правила для входящих подключений

В открывшемся мастере создания (рис. 1.3) правила выбираем «Для программы», в случае если необходимо перекрыть доступ к сети конкретной программе, либо «Для порта» (например, если есть необходимость отключить часть возможностей программы).

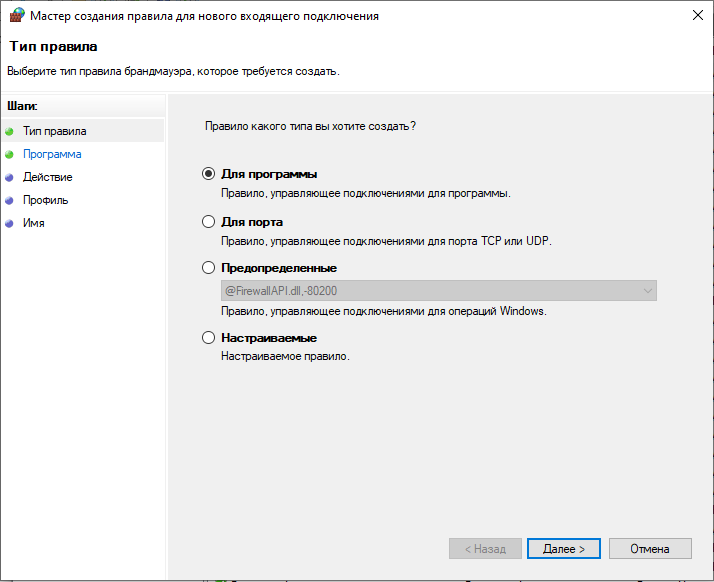


Рисунок 1.3 – Тип правила

При ограничении работы программы далее необходимо указать её путь, обязательно через папку, в которой она установлена, а не через ярлыки (рис. 1.4).

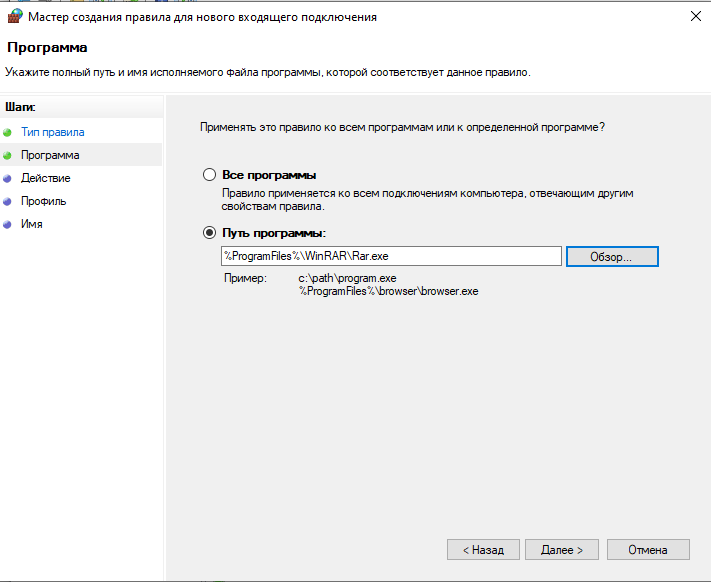


Рисунок 1.4 – Программы

Далее указывается какое именно действие вы хотите применить. В данном случае (рис. 1.5) необходимо блокировать подключение.

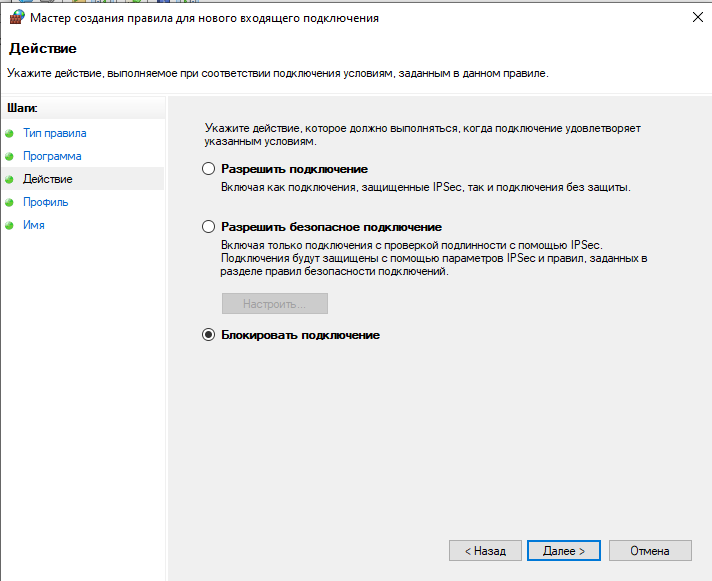


Рисунок 1.5 – Действие

Далее указывается профиль правила (рис. 1.6).

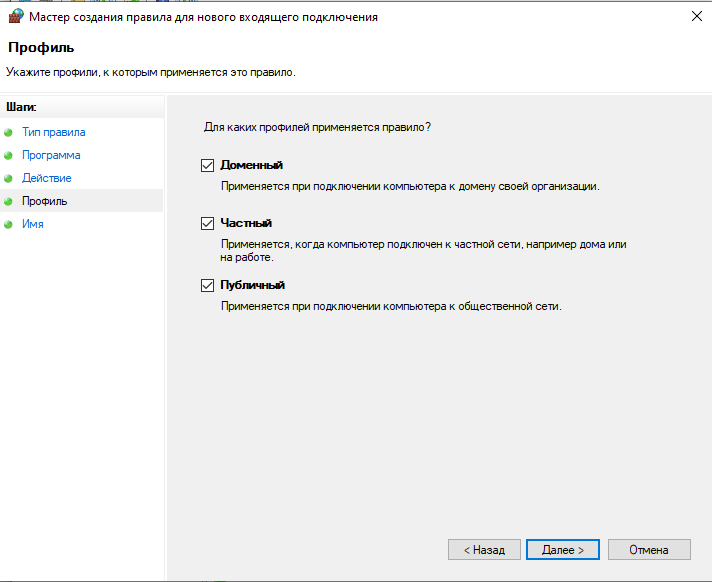


Рисунок 1.6 – Профиль

В следующем окне (рис. 1.7) указывается имя правила.

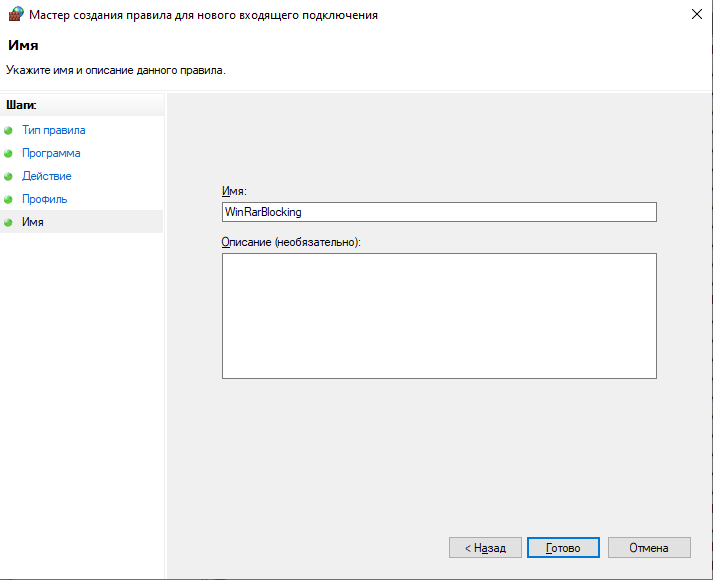


Рисунок 1.7 – Имя

В общем списке (рис. 1.8) появилось созданное правило. Правила можно отключать, копировать, удалять с помощью кнопок на правой панели.

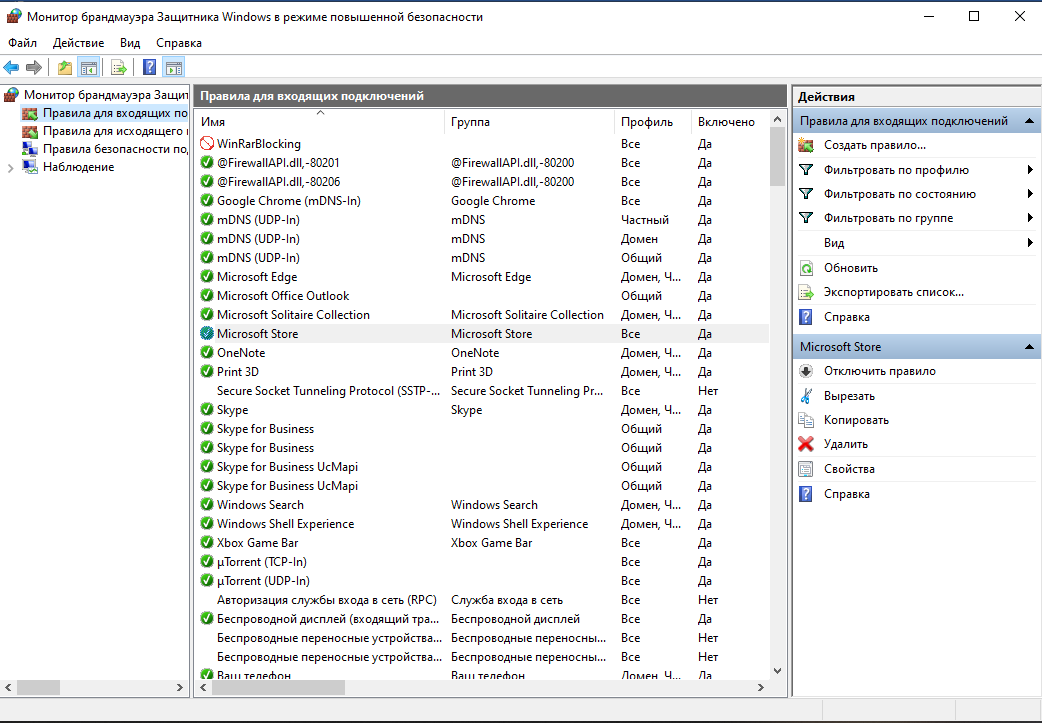


Рисунок 1.8 – Правила для входящих подключений

**Для 1 программы на разрешение подключения (рис. 1.9):**

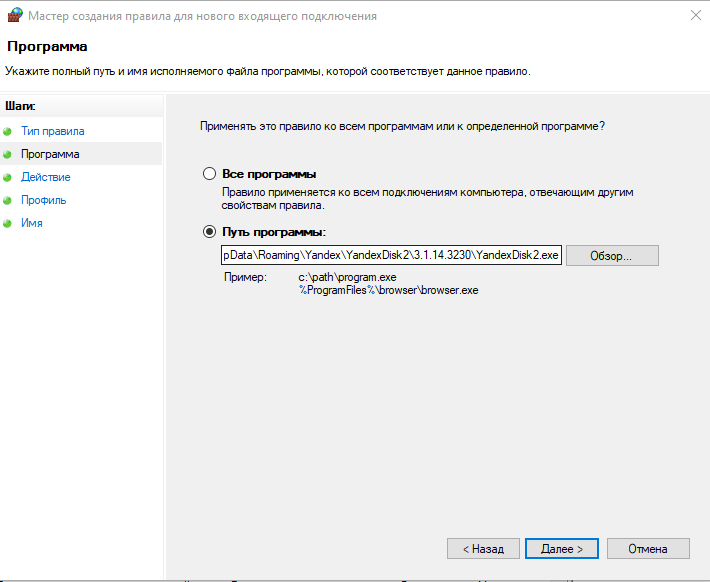


Рисунок 1.9 – Путь программы

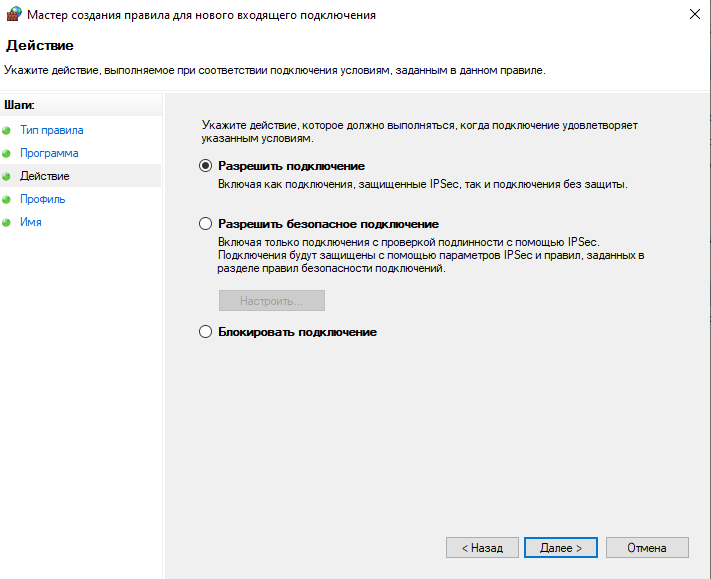


Рисунок 1.10 – Действие для программы

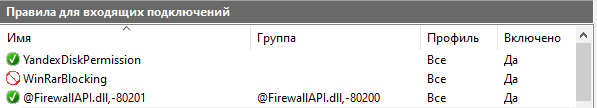


Рисунок 1.11 – Созданные правила

**Работа с командной строкой**

Для начала работы нужно открыть интерпретатор командной строки (рис. 1.12)

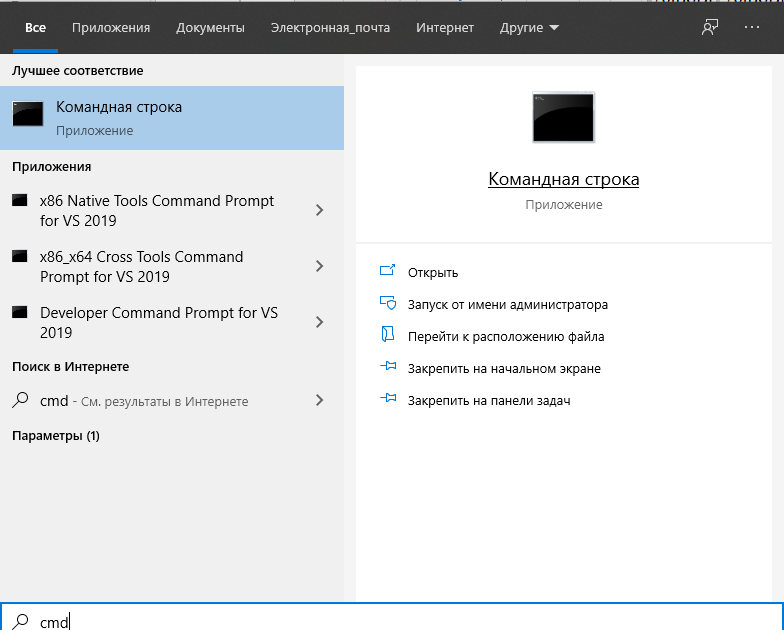


Рисунок 1.12 – Вызов командной строки

Команда DATE без параметров отображает текущую дату и запрашивает ввод новой даты. Для сохранения текущей даты нажмите клавишу ENTER.(рис 1.13)

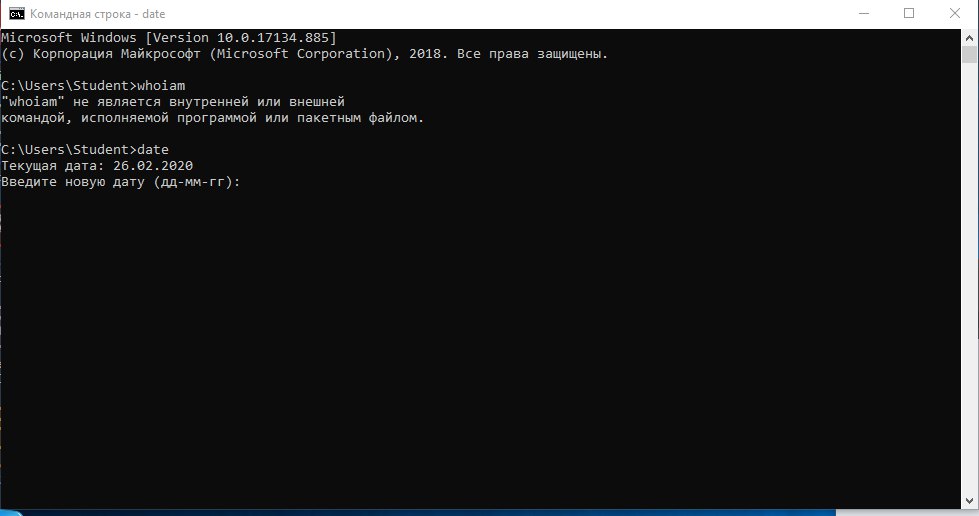


Рисунок 1.13 – Команда date

Команда PATH используется для указания или просмотра путей поиска исполняемых файлов. Пути поиска представляют собой строки, определяющие перечень каталогов файловой системы, в которых находятся исполняемые файлы (файлы с расширением .bat, .cmd, .exe, .vbs и т.п. ), разделенные точкой с запятой.(рис 1.14)

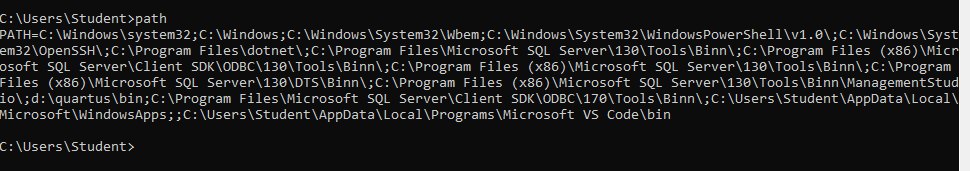


Рисунок 1.14 – Команда path

Команда WHOAMI используется для получения сведений об имени пользователя и группе, а также о соответствующих идентификаторах безопасности (SID), привилегиях, идентификаторах входа (ID) текущего пользователя (токене доступа) на локальном компьютере (рис 4.16).



При запуске whoami.exe без параметров, отображается имя пользователя в формате NTLM (домен\пользователь).

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

**Практическое занятие №5**

**Тема «Криптографическая защита информации»**

Цель: Овладение основными криптографическими алгоритмами симметричного шифрования.

**Сообщение:** Белявский Тихон Сергеевич

**Ключ:** 4

**Сообщение:** Защита

**Шифр Цезаря:** Еипгёхомн Цмщтс Хифжииёмы

**Шифр Трисемуса: ЕЛИЁЦГГ ДГЪУС ЦЛХЖЛЛГЬ**

k = 4\*p

****

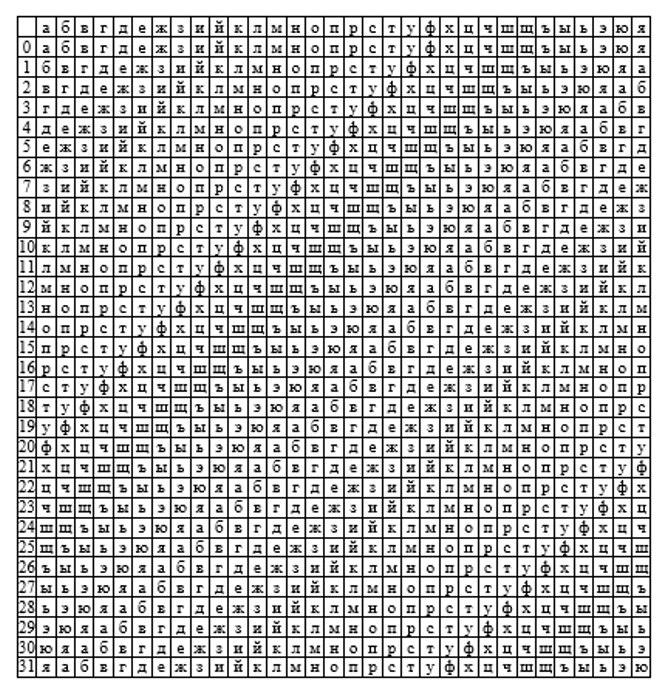
**Шифр Плейфейра:** ВЁ ЭН ГР ЗН ЗГ УВ КС ЖП ВС БЁ ЫЗ

|  |  |  |  |
| --- | --- | --- | --- |
| 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 |

БЕ ЛЯ ВС КИ ЙТ ИХ ОН СЕ РГ ЕВ ИЧ

ВЁ ЭН ГР ЗН ЗГ УВ КС ЖП ВС БЁ ЫЗ

**Шифр Виженера:** ИЕЕЗФСТИГ ЫЫХЦН КНГГМЕЫСЙ

,

**Задание (Вариант 4):**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Лжбзеииеизиачзнр** | Расшифровать с помощью **Магического квадрата**   |  |  |  |  | | --- | --- | --- | --- | | 7 | 12 | 1 | 14 | | 2 | 13 | 8 | 11 | | 16 | 3 | 10 | 5 | | 9 | 6 | 15 | 4 | |

ОТВЕТ : БЕЗРАЗЛИЧИЕ ЖИЗНИ

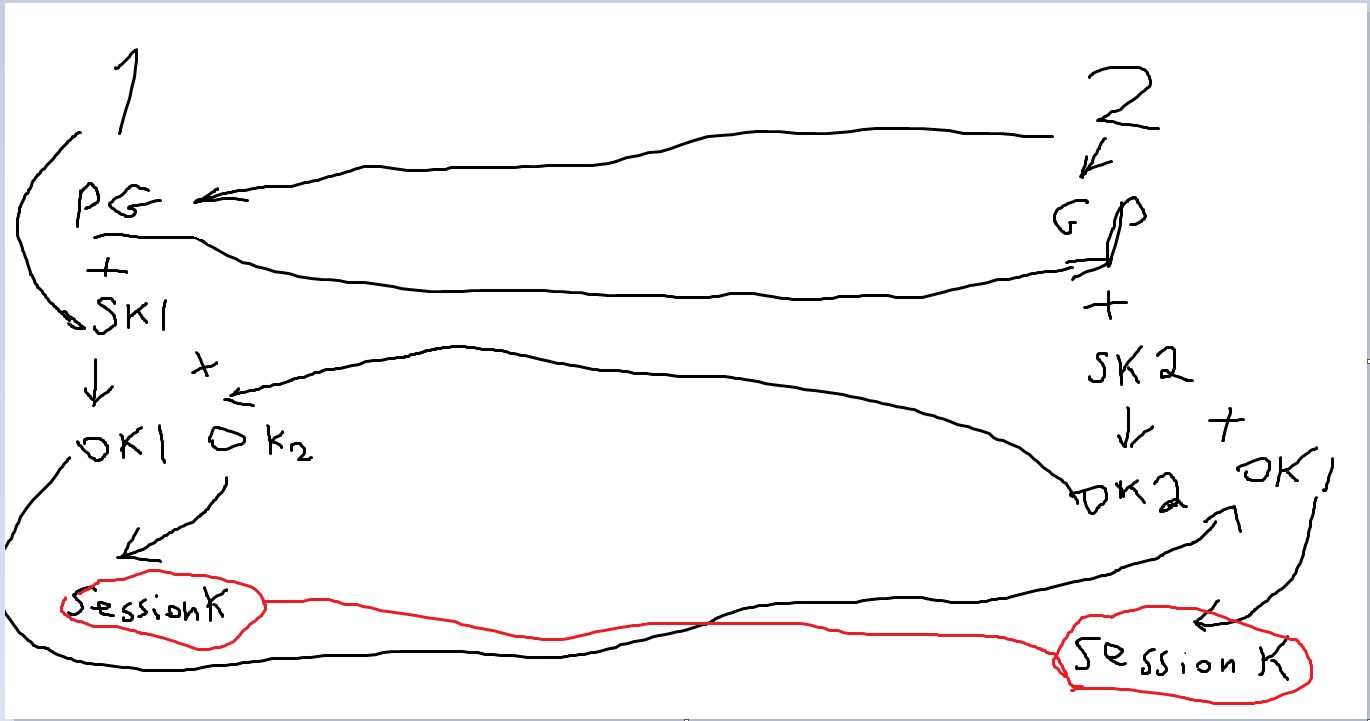
**Практическое занятие №6**

**Тема «Криптографическая защита информации»**

Цель: Овладение основными криптографическими алгоритмами асимметричного шифрования .

**Алгоритм Диффи-Хеллмана:**

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.

****

**RSA-шифрование:**

|  |  |  |
| --- | --- | --- |
| 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} |

**Шифр 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).

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 

**Практическое занятие №7**

**Тема «Криптографическая защита информации»**

Цель: Овладение основными криптографическими алгоритмами асимметричного шифрования .

**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:

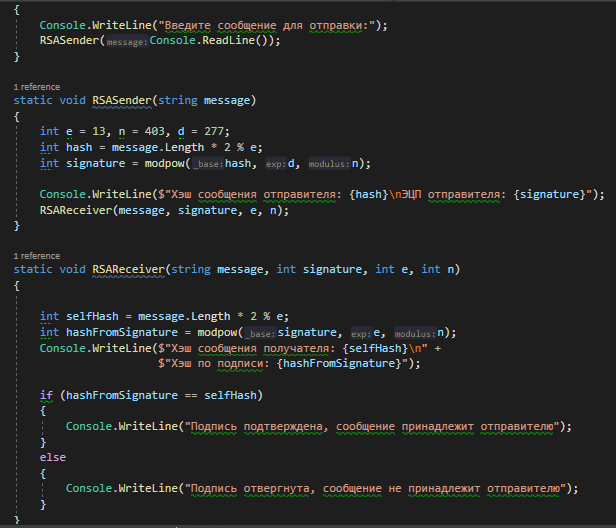
* применяет к полученному сообщению **T** хеш-функцию **h(T)** и получает хеш-образ r сообщения;
* расшифровывает хеш-образ **r’** из цифровой подписи s с использованием открытого ключа отправителя;
* проверяет соответствие хеш-образов r и r’ и если они совпадают, то отправитель действительно является 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;

****

**Практическое занятие №8**

**Тема «Криптографическая защита информации»**

Цель: Получение основных сведений из курса теории чисел

**Задание:**

1. Найти канонические разложения чисел *а* и *b*.

2. Найти НОД  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 .

4. Найти остаток от деления данного числа на простое.

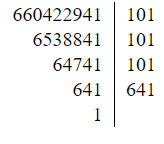
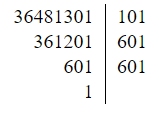
**Вариант 3**

1-3. *а* = 660422941, *b* = 36481301.

4. Найти остаток от деления  на 17.

**Решение:**

**1)** Найти канонические разложения чисел *а* и *b*.

** **

Следовательно, 660422941 = 101^3 \* 641

И 36481301 = 101 \* 601^2

**2)** Найти НОД  пользуясь

**a)** алгоритмом Евклида

660422941 = 36481301 \* 18 + 3759523;

36481301 = 3759523 \* 9 + 2645594;

3759523 = 2645594 \* 1 + 1113929;

2645594 = 1113929 \* 2 + 417736;

1113929 = 417736 \* 2 + 278457;

417736 = 278457 \* 1 + 139279;

278457 = 139279 \* 1 + 139178;

139279 = 139178 \* 1 + 101;

139178 = 101 \* 1378

Следовательно, НОД(660422941, 36481301) = 101

**б)** разложением чисел на простые множители.

Используя предыдущее задание, выбираем множители, которые есть и в одном, и в другом разложении:

660422941 = 101^3 \* 641;

36481301 = 101 \* 601^2;

Следовательно, НОД(660422941, 36481301) = 101

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

Имея НОД наших двух чисел, равный 101, найдем соотношение Безу:

660422941 = 36481301 \* 18 + 3759523;

3759523 = 660422941 + 36481301 \*(-18);

36481301 = 3759523 \* 9 + 2645594;

2645594 = 36481301 + 3759523 \*(-9);

3759523 = 2645594 \* 1 + 1113929;

1113929 = 3759523 + 2645594 \* (-1);

2645594 = 1113929 \* 2 + 417736;

417736 = 2645594 + 1113929 \* (-2);

1113929 = 417736 \* 2 + 278457;

278457 = 1113929 + 417736 \* (-2);

417736 = 278457 \* 1 + 139279;

139279 = 417736 + 278457 \* (-1);

278457 = 139279 \* 1 + 139178;

139178 = 278457 + 139279 \* (-1);

139279 = 139178 \* 1 + 101;

101 = 139279 + 139178 \* (-1);

Следовательно,

101 = 139279 + (278457 + 139279 \* (-1))\*(-1) = 139279\*2 + 278457\*(-1) = (417736 + 278457\*(-1))\*2 + 278457\*(-1) = 278457\*(-3) + 417736\*2 = (1113929 + 417736 \* (-2))\*(-3) + 417736\*2 = 417736\*8 + 1113929\*(-3) = (2645594 + 1113929 \* (-2))\*8 + 1113929\*(-3) = 1113929\*(-19) + 2645594\*8 = (3759523 + 2645594 \* (-1))\*(-19) + 2645594\*8 = 2645594\*27 + 3759523\*(-19) = (36481301 + 3759523 \*(-9))\*(-27) + 3759523\*(-19) = 3759523\*224 + 36481301\*(-27) = (660422941 + 36481301 \*(-18))\*(224) + 36481301\*(-27) = 36481301\*(-4059)+660422941\*(224)

= 660422941\*(224) + 36481301\*(-4059);

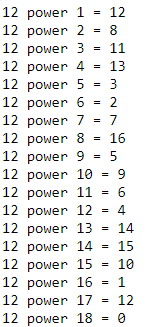
При условии, что av + bu = НОД(a,b), найдем целые числа

V = 224; u = -4059

**4)** Найти остаток от деления данного числа на простое.

Найти остаток от деления на 17.

Далее воспользуемся чудесами IT и найдем начало зацикливания остатка:



Видим, что длина цикла при данных числах равна 17

Тогда 2001 = 117\*17 + 12, значит число дает тот же остаток от деления на 17, что и , то есть 4.

**Ответ:** 4

**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 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?**

* 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).

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

Права, разрешающие выполнять 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?**

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

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

* Издательский договор
* Постановочный договор
* Сценарный договор
* Договор о депонировании рукописи
* Договор художественного заказа
* Договор об использовании в промышленности

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.

**Тема 10 «Составление и оформление заявок на объекты промышленной собственности»**

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

**Теоретическое введение**

Правовая охрана объектов промышленной собственности (ОПС) осуществляется в рамках государственной, а также международных (надгосударственных) патентных систем. Уполномоченные организации выдают от имени государства или группы государств соответствующий охранный документ.

Охранный документ (патент, свидетельство) – это выдаваемый патентным органом от имени государства документ, который удостоверяет авторство, приоритет на объект промышленной собственности и исключительное право на его использование.

Приоритет − первенство, чаше всего, определяемое датой подачи заявки на ОПС.

Конвенционный приоритет обозначает, что заявка, поданная в одной стране-участнице конвенции, обладает во всех других странах приоритетом в течение года, исчисляемого с момента подачи заявки в первой стране.

Одной из наиболее распространенных коммерчески значимых форм правовой охраны является патент, который обеспечивает патентообладателю исключительное (монопольное) право на использование объекта промышленной собственности и запрещает всем третьим лицам их использование в коммерческих целях без разрешения патентообладателя. Являясь одновременно правовым, техническим и информационным документом, патент выступает не только в качестве формы правовой охраны от несанкционированного использования, но и своеобразным экономическим стимулом для инвестиций в научные исследования и промышленность.

**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.

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 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.

**Вывод:** в ходе выполнения данной работы я овладел навыками составления и оформления заявок на объекты промышленной собственности.

**Практическое занятие №11**

**Тема «Патентные исследования»**

**Цель:** изучить виды, содержание и порядок проведения патентных исследований.

**Задание для выполнения.**

Необходимо выполнить экспертизу патентной чистоты конструкции механизма для обеспечения линейного перемещения исследуемых препаратов, отличающегося взаимным расположением перемещающихся элементов

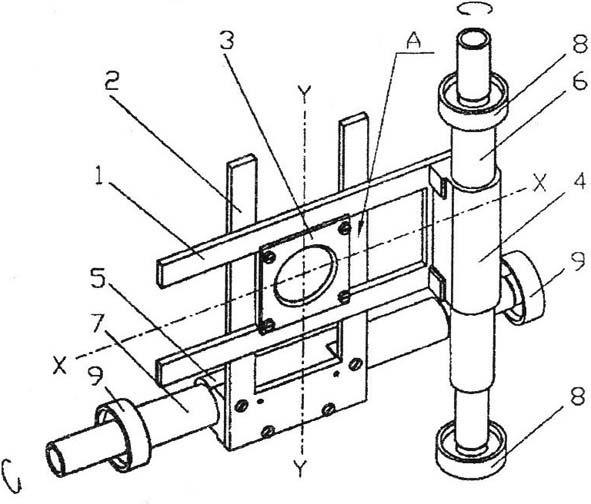


Рисунок 11.1 – механизм линейного перемещения

Механизм линейного перемещения (Рис.11.1), включающий корпус, подвижную площадку для тестируемого изделия и два регулировочных узла, отличающийся тем, что содержит две направляющие, каждая из которых выполнена в виде плоской пластины с прямоугольным пазом, расположенные под прямым углом друг относительно друга с образованием прямоугольного окна, в котором установлена подвижная площадка, сжимающая направляющие к общей плоскости с возможностью их скольжения друг относительно друга и имеющая возможность перемещения в пазах пластин, каждый регулировочный узел выполнен в виде передачи винт-гайка, винт которой выполнен на валу, установленном в корпусе с возможностью вращения, гайка закреплена на направляющей и установлена с возможностью линейного перемещения вдоль оси винта, причем валы регулировочных узлов расположены в корпусе взаимно перпендикулярно.

Наличие предполагаемых существенных признаков и планируемый выпуск продукции являются предпосылками для патентования разработки.

Необходимо выполнить экспертизу патентной чистоты разработанного конструктивного решения (ОПС).

В качестве существенных признаков при патентовании предполагаемого изобретения, выносится конструктивный признак: отличие взаимным расположением перемещающихся элементов

**Выполнение задания**

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

* объект – *механизм перемещения;*
* страна поиска – *Республика Беларусь*;
* источники информации – *патентные*;
* ретроспективность – *5 лет*;
* информационная база - *Афiцыйны бюлетэнь «Вынаходствы, карысныя мадэлi, прамысловыя узоры» Нацыянальнага цэнтра iнтэлектуальная уласнасцi Рэспублiкi Беларусь, каталог МПК.* [http://www.belgospatent.org.by](http://www.belgospatent.org.by/)

Проведенный патентный поиск по указанному сайту, выявил следующие аналогичные по конструктивному выполнению патенты и полезные модели, приведенные ниже:

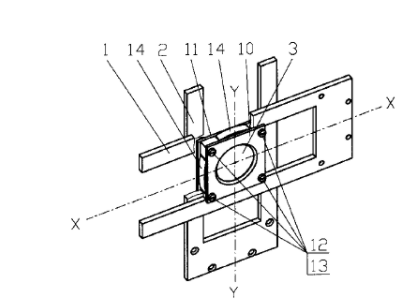


Рисунок 11.2 – Механизм линейного перемещения

Механизм линейного перемещения (Рис.11.2),включающий корпус, подвижную площадку для юстируемого изделия и два регулировочных узла, отличающийся тем, что содержит две направляющие, каждая из которых выполнена в виде плоской пластины с прямоугольным пазом, расположенные под прямым углом друг относительно друга с образованием прямоугольного окна, в котором установлена подвижная площадка, сжимающая направляющие к общей плоскости с возможностью их скольжения друг относительно друга и имеющая возможность перемещения в пазах пластин, каждый регулировочный узел выполнен в виде передачи винт-гайка, винт которой выполнен на валу, установленном в корпусе с возможностью вращения, гайка закреплена на направляющей и установлена с возможностью линейного перемещения вдоль оси винта, причем валы регулировочных узлов расположены в корпусе взаимно перпендикулярно.

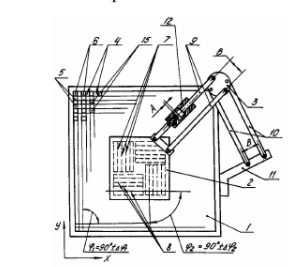


Рисунок 11.3 – Механизм шагового перемещения

Механизм шагового перемещения (Рис.11.3), содержащий индуктор в виде ферримагнитного зубчатого основания, подвижный якорь в виде каретки с электромагнитами, установленными на индукторе с возможностью установки параллельных рядов зубцов электромагнитов параллельно соответствующим рядам зубцов индуктора, отличающийся тем, что содержит устройство ограничения разворота якоря, выполненное в виде двух параллелограммов, шарнирно связанных между собой.

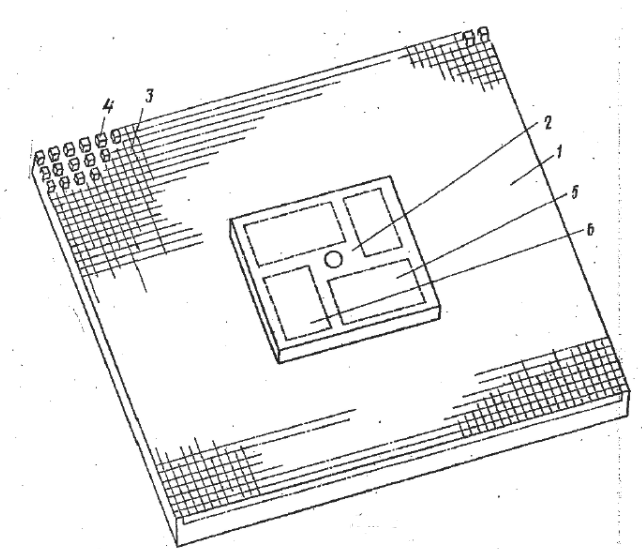


Рисунок 11.4 – Механизм шагового перемещения

Механизм шагового перемещения (Рис.11.4), подвижные элементы перемещаются по направляющим и по траверсе на воздушной подушке, без механических соединений. Прототипом является магнитное устройство для перемещения, содержащее основание, верхняя поверхность которого несет решетку из немагнитного материала, внутри которого располагаются участки из ферромагнитного материала, каретку, имеющую два параллельных ряда магнитов по каждой из двух перпендикулярных осей управления.

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

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Таблица 1 – 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 охранного документа или причина его аннулирования (только для анализа патентной чистоты) |
| Механизм линейного перемещения | | Патент РБ  № 6634  МПК  D G12 B 1/00 (2004.12) | Войцехович Артур Альбертович (BY)  Стрижевич Тамара Аркадьевна (BY)  Кудряшов Александр Алексеевич (BY),  Заявка u 20130078 от 2013.01.25, опубл. 2013.08.30 | Механизм линейного перемещения | Действует |
| Патент РБ  № 3271  МПК D G12 D 2/00 | Замостоцкий Евгений Геннадьевич (BY),  Коган Александр Григорьевич (BY),  Иванова Татьяна Петровна (BY). Заявка u 20060460 от 2006.07.10, опубл. 2006.12.30 | Механизм шагового перемещени | Действует |
| Патент РБ  № 93  6 D 03D 15/00 | Степанчук Светлана Владимировна (BY).  Заявка u 19980058 от 1998.12.22, опубл. 2000.03.30 | Механизм шагового перемещени | Действует |

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

**Вывод:** Изучил виды, содержание и порядок проведения патентных исследований.

**Практическое занятие №12**

**«Патентный поиск»**

**Цель:** освоить навыки проведения патентного поиска по заданной тематике.

**Задание для выполнения**

Проведение патентного поиска по теме: "Стенографический метод передачи информации в html-файлах".

Стеганография — это метод организации связи, который, собственно, скрывает само наличие связи. В отличие от криптографии, где неприятель точно может определить является ли передаваемое сообщение зашифрованным текстом, методы стеганографии позволяют встраивать секретные сообщения в безобидные послания так, чтобы невозможно было заподозрить существование встроенного тайного послания.

Слово "стеганография" в переводе с греческого буквально означает "тайнопись" (steganos - секрет, тайна; graphy - запись). К ней относится огромное множество секретных средств связи, таких как невидимые чернила, микрофотоснимки, условное расположение знаков, тайные каналы и средства связи на плавающих частотах и т. д.

Стеганография занимает свою нишу в обеспечении безопасности: она не заменяет, а дополняет криптографию. Сокрытие сообщения методами стеганографии значительно снижает вероятность обнаружения самого факта передачи сообщения. А если это сообщение к тому же зашифровано, то оно имеет еще один, дополнительный, уровень защиты.

В настоящее время в связи с бурным развитием вычислительной техники и новых каналов передачи информации появились новые стеганографические методы, в основе которых лежат особенности представления информации в компьютерных файлах, вычислительных сетях и т. п. Это дает нам возможность говорить о становлении нового направления - компьютерной стеганографии.

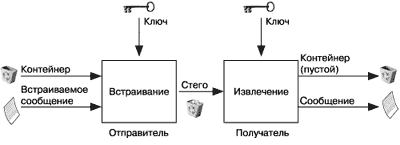


Рис.1 -  структурная схема

Несмотря на то что стеганография как способ сокрытия секретных данных известна уже на протяжении тысячелетий, компьютерная стеганография - молодое и развивающееся направление.

До недавнего времени для описания модели стеганографической системы использовалась предложенная 1983 году Симмонсом так называемая "проблема заключенных". Она состоит в том, что два индивидуума хотят обмениваться секретными сообщениями без вмешательства охранника (Вилли), контролирующего коммуникационный канал. При этом имеется ряд допущений, которые делают эту проблему более или менее решаемой. Первое допущение облегчает решение проблемы и состоит в том, что участники информационного обмена могут разделять секретное сообщение перед заключением. Другое допущение, наоборот, затрудняет решение проблемы, так как охранник имеет право не только читать сообщения, но и модифицировать их.

|  |  |  |
| --- | --- | --- |
| Таблица 1 – Патентная документация | | |
| Классы МПК: | | H04L9/00 Устройство для секретной или скрытой связи  G09C5/00 Способы и устройства для шифрования или дешифрования, не отнесенные к другим группам данного подкласса, например маскировка и искажение графических данных, таких как чертежи, письменные или печатные сообщения |
| Патентообладатель: | | Гайворонский Борис Юрьевич (RU) |

**Вывод:** в ходе практической работы я провел поиск наличия патента в базах данных Национального центра интеллектуальной собственности, Российского агентства по патентам и товарным знакам, Евразийских патентов, Европейского патентного офиса, Патентного бюро Японии и составил перечень похожих полезных программных обеспечений.