Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Электронная тетрадь**

по Основам Защиты Информации

Студентка: Кохнюк А. С.

ФИТ 2 курс 3 группа

Преподаватель: Ржеутская Н. В.

Минск 2022

# **Практическое занятие №1**

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

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

1. **Что такое информационная безопасность?**

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

1. **Перечислить основные национальные интересы в информационной сфере?**

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

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

Основные национальные интересы в политической сфере:

* реализация конституционных прав граждан на получение, хранение и распространение полной, достоверной и своевременной информации;
* формирование и поступательное развитие информационного общества;
* равноправное участие Республики Беларусь в мировых информационных отношениях;
* преобразование информационной индустрии в экспортно-ориентированный сектор экономики;
* эффективное информационное обеспечение государственной политики;
* обеспечение надежности и устойчивости функционирования критически важных объектов информатизации.

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

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

Внутренние источники угроз:

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

Внешние источники угроз:

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

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

Нейтрализация источников внутренних угроз и защита от внешних угроз национальной безопасности является одной из основных.

**В информационной сфере с целью нейтрализации** **внутренних источников угроз национальной безопасности совершенствуются механизмы реализации прав граждан на получение, хранение, пользование и распоряжение информацией**, в том числе с использованием современных информационно-коммуникационных технологий. **Государство гарантирует обеспечение установленного законодательством порядка доступа к государственным информационным ресурсам**, в том числе удалённого, и возможностям получения информационных услуг. Значимым этапом станет разработка и реализация стратегии всеобъемлющей информатизации, ориентированной на развитие электронной системы осуществления административных процедур, оказываемых гражданам и бизнесу государственными органами и иными организациями, и переход государственного аппарата на работу по принципу информационного взаимодействия. Ускоренными темпами будет развиваться индустрия информационных и телекоммуникационных технологий. **Особое внимание будет уделяться последовательному повышению качества, объема и конкурентоспособности национального контента**, который призван занимать доминирующее положение внутри страны, и его продвижению во внешнее информационное пространство.

**Приоритетным направлением является совершенствование нормативной правовой базы обеспечения информационной безопасности и завершение формирования комплексной государственной системы обеспечения информационной безопасности**, в том числе путем оптимизации механизмов государственного регулирования деятельности в этой сфере. При этом важное значение отводится наращиванию деятельности правоохранительных органов по предупреждению, выявлению и пресечению преступлений против информационной безопасности, а также надежному обеспечению безопасности информации, охраняемой в соответствии с законодательством. Активно продолжится разработка и внедрение современных методов и средств защиты информации в информационных системах, используемых в инфраструктуре, являющейся жизненно важной для страны, отказ или разрушение которой может оказать существенное отрицательное воздействие на национальную безопасность.

**Защита от внешних угроз национальной безопасности в информационной сфере осуществляется путем участия Республики Беларусь в международных договорах**, регулирующих на равноправной основе мировой информационный обмен, в создании и использовании межгосударственных, международных глобальных информационных сетей и систем. **Для недопущения технологической зависимости государство сохранит роль регулятора при внедрении иностранных информационных технологий.**

**Вывод:** Изучила концепцию национальной безопасности РБ.

# **Практическое занятие №2**

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

**Вариант 5**

**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.

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № варианта | *E*0 | *E* | *K* | *C* |
| 5 | 11000 | 9500 | 3 | 1500 |

***Е0*** – положительный эффект, который создает информационный объект; ***E*** – эффективность функционирования объекта с учетом воздействия несанкционированного доступа; – полезный эффект от функционирования объекта, который уменьшается при несанкционированном доступе.

**Полезный эффект от функционирования объекта:**

|  |  |
| --- | --- |
| Относительная эффективность: |  |

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

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

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 Δ***Е3***, а коэффициент снижения негативного воздействия несанкционированного доступа на эффективность функционирования объект ‑ через ***К***, тогда:

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

**Следовательно:**

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

**Формула относительной эффективности:**

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

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

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Поскольку затраты на установку средств защиты можно рассматривать как ущерб владельцу объекта от возможности осуществления несанкционированного доступа, то суммарный ущерб объекту:   |  |  | | --- | --- | |  | (8) |   Если эффективность функционирования объекта имеет стоимостное выражение (доход, прибыль и т.д.), то UΣ непосредственно изменяет эффективность:   |  |  | | --- | --- | |  | (9) | |  |

В результате у нас получилось следующее, E > Е3, из этого делаем вывод, что данная защита не эффективна.

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

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

или

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

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

**Вывод:** Научилась решать задачи разработки средств защиты для обеспечения максимальной эффективности объекта в условиях несанкционированного доступа

# **Практическое занятие №3**

**Тема «Разработка политики информационной безопасности поликлинники»**

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

**Введение**

Cегодня невозможно представить практически ни одну сферу деятельности без средств вычислительной техники и телекоммуникаций. Информационные технологии предлагают все новые и новые сервисы. Через Интернет становятся доступными электронные платежные системы, персональные финансовые порталы, электронные биржи и т. д. Внедряя новые услуги, компании укрепляют свое положение на рынке.С другой стороны, вопросы информационной безопасности всегда, как минимум, на шаг отстают от нововведений. Достаточно посмотреть, сколько версий должно миновать, пока тот или иной программный продукт не приобретет репутацию надежного.Эти две очевидные тенденции приводят к необходимости здорового консерватизма в построении информационных систем корпоративного уровня. Нужен взвешенный подход, учитывающий риски и стоимость отдачи от вложенных средств.Информационные технологии все шире применяются в качестве инструментаведения бизнеса. И понятие риска является краеугольным как для бизнеса, так и для системы организации информационной безопасности.Но при этом следует понимать, что стандарты и передовые практики обычно не рассматривают конкретные программы и детальные методики, а концентрируются на основных принципах и примерах.С точки зрения рисков следует иметь в виду два аспекта:- Во-первых, любую систему безопасности можно взломать, имея достаточно ресурсов и времени. Поэтому риски могут быть идентифицированы и уменьшены, но никогда не сведены полностью на нет. - - Во-вторых, все организации разные, поэтому процесс смягчения рисков для каждой имеет свои уникальные черты.

1. **Описание структуры**

Поликлиника – это многопрофильное лечебно-профилактическое учреждение, оказывающее медицинскую помощь населению на закрепленной территории на догоспитальном этапе. В городах имеются два типа поликлиник для взрослого населения:

* объединенные с больницами;
* необъединенные (самостоятельные)

К основным задачам, решаемым амбулаторно-поликлиническими организациями, относятся:

* накопление и анализ информации о состоянии здоровья обслуживаемого населения (заболеваемости, инвалидности, смертности);
* проведение широких профилактических мероприятий и работы по формированию здорового образа жизни;
* раннее выявление больных;
* проведение диспансерных мероприятий среди здоровых и больных;
* оказание квалифицированной, в т.ч. и специализированной, медицинской помощи;
* развитие ресурсосберегающих, в т.ч. стационар замещающих технологий.

От того, в какой мере и насколько качественно решаются данные задачи, зависит объем работы других медицинских организаций, а также многие показатели, характеризующие деятельность системы здравоохранения в целом.

Поликлиника возглавляется **главным врачом.** В структуру поликлиники входят: **регистратура, отделение профилактики, лечебно-профилактические отделения и кабинеты, лечебно-диагностические подразделения, административно-хозяйственная часть, отделения восстановительного лечения и др.**

**Регистратура** является основным структурным подразделением по организации приема больных. В функции регистратуры входит:

- регистрация первичных пациентов;

- организация предварительной и неотложной записи больных на прием к врачу как при непосредственном обращении в поликлинику, так и по телефону;

- обеспечение регулирования интенсивности потока пациентов с целью создания равномерной загрузки врачей и распределения пациентов по видам оказываемой помощи.

Основными организационно-методическими принципами работы поликлиник являются участковость (закрепление за врачебной должностью нормативного числа жителей) и широкое использование диспансерного метода (систематическое активное наблюдение за состоянием здоровья определенных контингентов).

Структура поликлинники представлена ниже на рисунке *1.1*

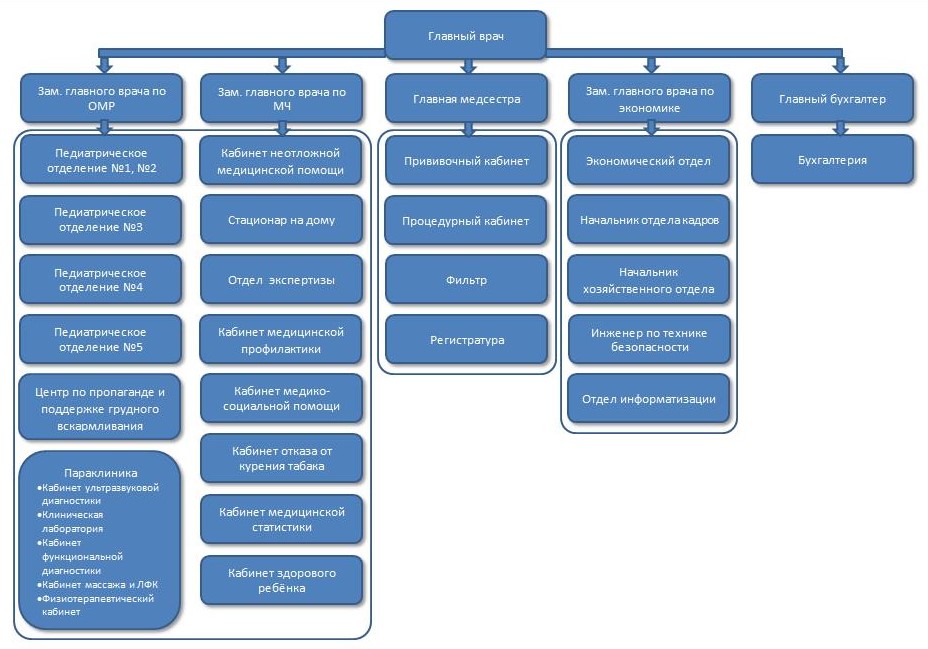


Рис. *1.1* – Структура поликлинники

1. **Оценка рисков**

Политика безопасности строится на основе анализа рисков, которые признаются реальными для информационной системы организации. Когда риски проанализированы, стратегия защиты определена, тогда составляется программа, реализация которой должна обеспечить информационную безопасность. Под эту программу выделяются ресурсы, назначаются ответственные, определяется порядок контроля выполнения программы.

**При оценивании рисков учитывается:**

* ценность ресурсов;
* оценка значимости угроз;
* эффективность существующих и планируемых средств защиты.

Анализ рисков состоит в том, чтобы выявить существующие риски и предложить способ их оценки.

В самом широком смысле мера риска может рассматриваться в дальнейшем как описание видов неблагоприятных действий, воздействию которых может подвергнуться система или организация, и вероятностей того, что эти действия могут произойти. Результат этого процесса должен указать поликлиннике степень риска, связанного с определенными ценностями. Этот результат важен, потому что он является основой для дальнейшего выбора средств защиты и решений по минимизации риска.

Существует вероятность возникновения следующих нарушений информационной безопасности:

* получение неправомерного доступа к информации, другими словами, нарушение конфиденциальности;
* утрата сведений, вызванная разрушением носителя информации или стиранием данных;
* внесение изменений при прямом доступе к базе данных или через интерфейс системы;
* отказ функционала, связанный с получением доступа к информации;
* получение доступа к базе данных – полное или частичное;
* некорректное функционирование информационной системы вследствие несанкционированного изменения модулей.

**Хищение медицинских данных чревато следующими последствиями:**

* медицинские карты используются на черном рынке для получения медицинской помощи незастрахованными лицами;
* в карту могут быть внесены сведения вора, в результате пациент рискует получить помощь, основанную на чужой истории болезни, группе крови, непереносимости и аллергической реакции;
* мошенники могут исчерпать страховой лимит, и законный владелец лишится возможности получать медицинскую помощь в самое неподходящее время. Большинство страховых планов имеют ограничения на отдельные виды услуг. Например, страховая компания откажется оплачивать два оперативных вмешательства по удалению аппендицита;
* получив доступ к данным пациента, мошенники могут злоупотреблять рецептами на лекарства, лишив этой возможности владельца карты. Рецепты, как правило, лимитированные;
* если с устранением массовых кибератак на банковские карты проблемы не возникают, то защита от фишинговых атак потребует больших усилий. Кража электронной медицинской карты может и вовсе остаться незамеченной. И если этот факт обнаруживается, то, как правило, в ситуациях, когда последствия угрожают жизни.

**Способы усиления защиты сведений в информационных системах медицинских организаций.**

Построение системы защиты может выполняться в несколько этапов:

* собираются сведения о существующих информационных системах персональных сведений;
* моделируются угрозы безопасности;
* разрабатываются технические задания;
* проектируется система защиты информации;
* разрабатывается организационно-распорядительная документация, которая регламентирует процессы обработки и защиты сведений;
* поставляются, устанавливаются и настраиваются средства защиты информации;
* проводится аттестация информационных систем сведений, согласно требованиям безопасности.

К объектам защиты медицинской информационной системы относят:

* сведения в базе данных;
* резервные и архивные копии сервера;
* целевые данные администратора и начальника;
* средства обеспечения функционирования медицинской информационной системы;
* обработка информации в медучреждении – сбор, хранение, передача;
* производительность файлового сервера.

1. **Разработка мер защиты**

Есть и другие способы обеспечения безопасности, которые не относятся к медицинской информационной системе напрямую. Такие меры предполагают выполнение персоналом некоторых регламентов по работе с системой:

* организация охраны помещения, работы с документацией, сотрудниками. Использование технических средств и информационно-аналитической деятельности с целью выявления угроз – внутренних и внешних;
* исключение проникновения на территорию и в здание злоумышленников;
* организация работы с сотрудниками в части доступа к информации;
* обеспечение правильной работы с документами и документированными сведениями;
* задействование технических средств по сбору, накоплению, обработке и хранению конфиденциальных данных;
* организация работы по анализу угроз конфиденциальных сведений – внутренних и внешних;
* организация работы по выполнению контроля над работой сотрудников с информацией.

Также внедряются и специализированные средства контроля доступа в помещение. Это могут быть:

* исполнительные устройства, включая кабины, турникеты, шлагбаумы;
* кардридеры, считывающие информацию;
* панели для введения кода с помощью клавиатуры;
* концентраторы и контроллеры;
* средства идентификации, включая брелоки, карты и биометрию;
* индивидуальное программное обеспечение.

С целью защиты данных пациента применяются несколько программных компонентов и механизмов. Для предотвращения несанкционированного доступа развертываются средства авторизации, внедряются системы обнаружения и предотвращения вторжений, а также утечек информации. Может устанавливаться антивирусное программное обеспечение. Существует успешная практика использования файерволов.

*К криптографическим средствам* защиты относят алгоритмы шифрования данных и внедрение [электронной цифровой подписи](https://www.1cbit.ru/1csoft/ecp-dlya-vrachei/). Системы аутентификации предполагают внедрение защиты с паролем, подпись сертификатами и открытие доступа по биометрическим данным.

*Инструментальные средства* анализа предполагают внедрение программного обеспечения для проведения мониторинга. *К техническим* относят комплексное внедрение технических средств защиты. Система бесперебойного питания предполагает установку, обслуживание источников бесперебойного питания, установку генераторов напряжения и резервирование нагрузки.

С целью предотвращения взлома и краж используются специальные средства, включая электронные ключи и смарт-карты. Эти технологии позволяют повысить уровень защиты информационной системы на этапе аутентификации.

**Выводы:** В ходе этой работы были проанализированы риски, связанные с информационной безопасностью поликлинники. Были предусмотрены явления, которые могут оказать влияние на целостность системы и вывести ее из строя. Разработанная политика безопасности не способна обеспечить полную защиту всей информации компании, но она необходима для обеспечения некоторых гарантий.

Политика безопасности определяет стратегию организации в области информационной безопасности, а также ту меру внимания и количество ресурсов, которую руководство считает целесообразным выделить.

Политика безопасности строится на основе анализа рисков, которые признаются реальными для информационной системы организации. Когда риски проанализированы, стратегия защиты определена, тогда составляется программа, реализация которой должна обеспечить информационную безопасность. Под эту программу выделяются ресурсы, назначаются ответственные, определяется порядок контроля выполнения программы и т.п.

# **Практическое занятие №4**

**Тема «Настройка Брандмауэра Windows»**

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

**Задание 1.** Создать правила для входящих подключений. (1 – на блокировку, 2 – на разрешение)

* 1. Для создания правила по ограничению доступа программ к сети необходимо открыть «Панель управления». Далее выбрать вкладку «Защита и безопасность». Там находим «Брандмауэр Защитника Windows» и проверяем включён ли он. Окно представлено на рисунке *1.1*

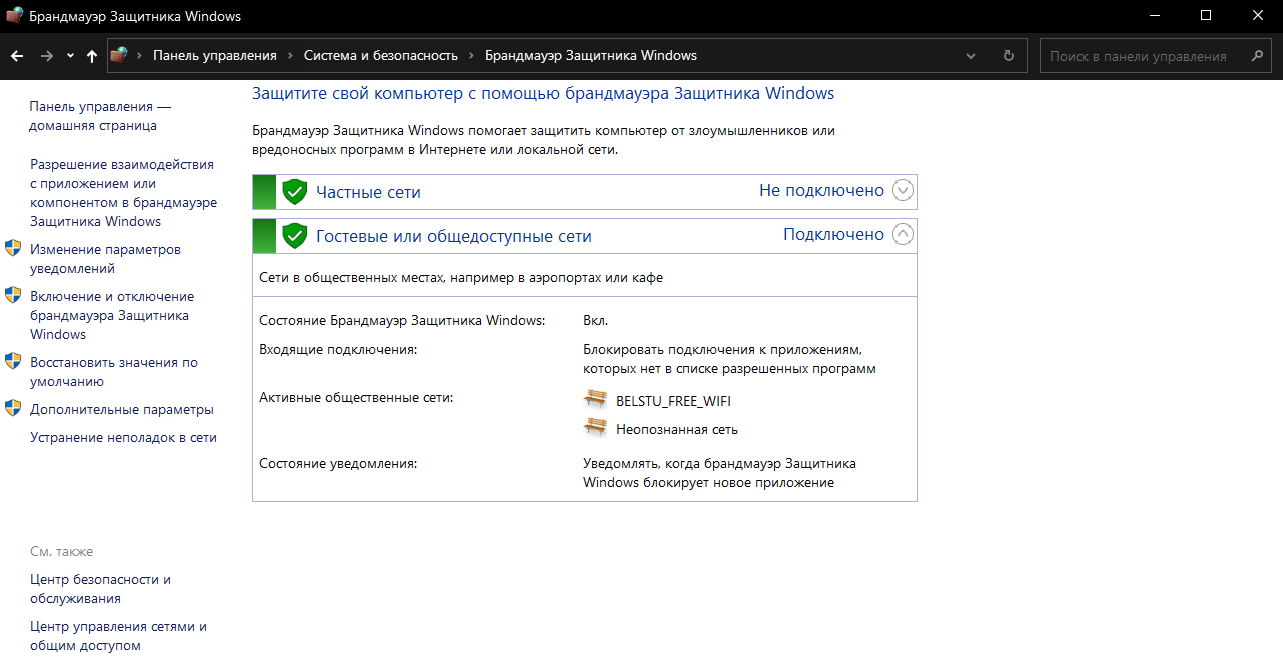


Рис. *1.1* – Окно состояния Брандмауэра

После этого приступаем к выполнению задания. Переходим во вкладку «Дополнительные параметры» и откроется окно, показанное на рисунке *1.2.*

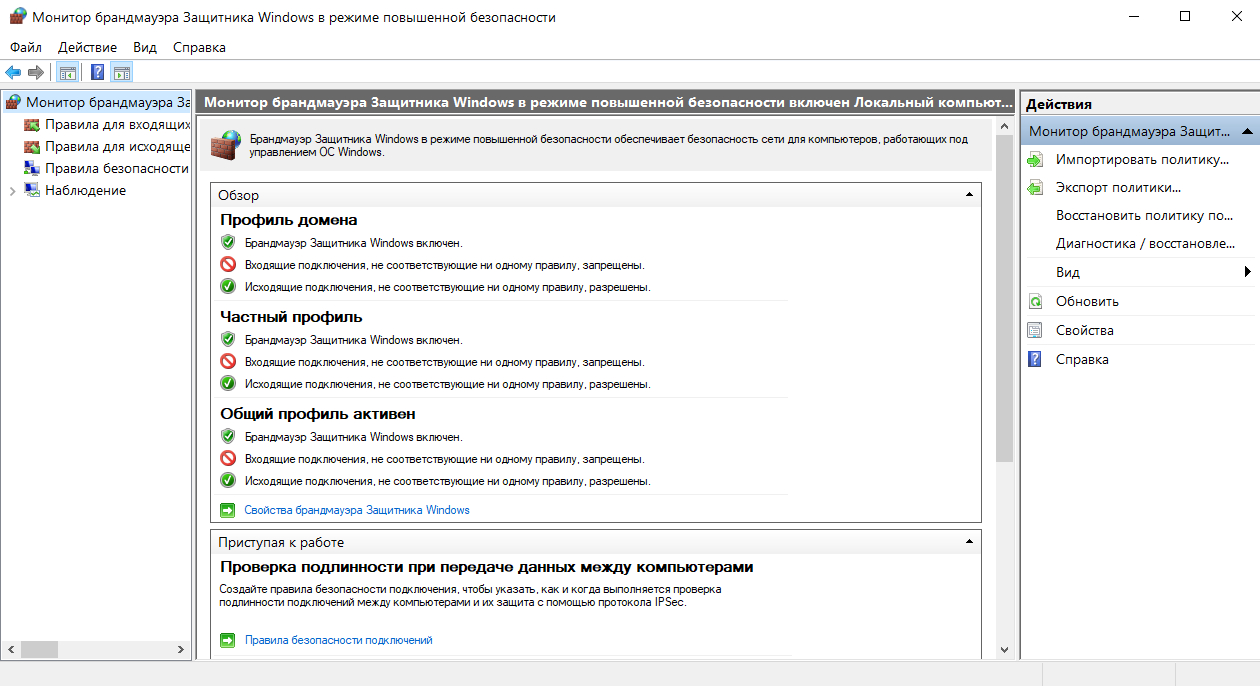


Рис. *1.2* – Монитор Брандмауэра

Далее в левом контекстном меню переходим во вкладку «Правила для входящих исключений». Затем во вкладке меню «Действие» выбираем «Создать правило», либо нажимаем «Создать правило» в правой панели.

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

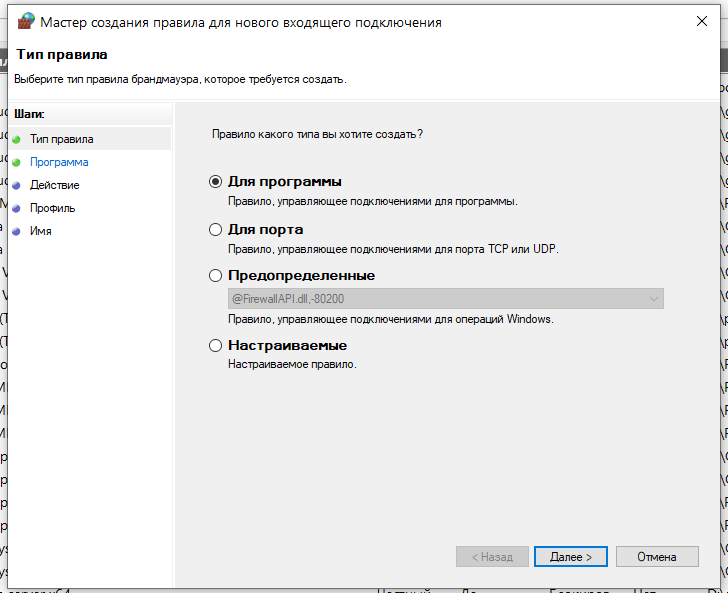


Рис. *1.3* – Окно создания правила

Далее указываем путь к программе (рис. *1.4*) и в действия указываем “Блокировать подключение” (рис. *1.5*). В конце указываем имя для правила.

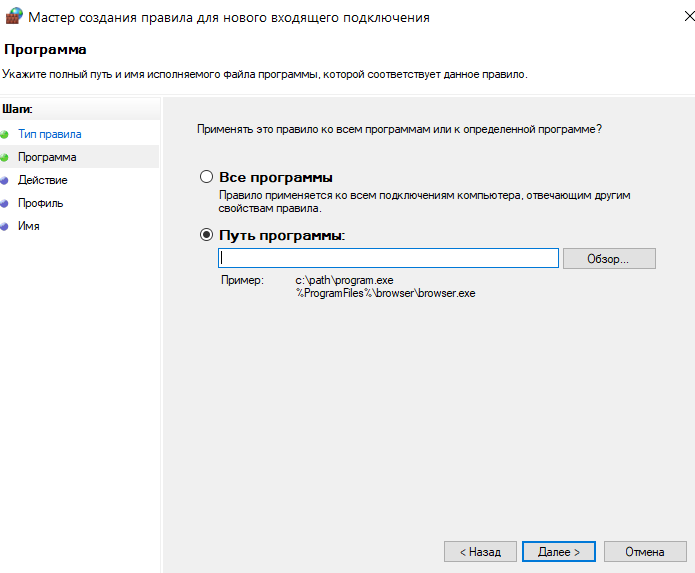


Рис. *1.4* – Окно создания правила, вкладка «Программа»

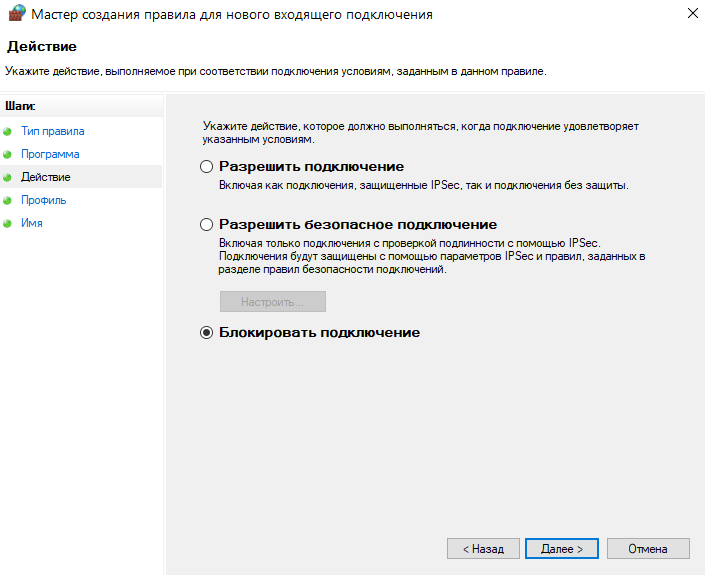


Рис. *1.5* – Окно создания правила, вкладка «Действие»

В общем списке появилось созданное правило. Правила можно отключать, копировать, удалять с помощью кнопок на правой панели (рис. *1.6*).

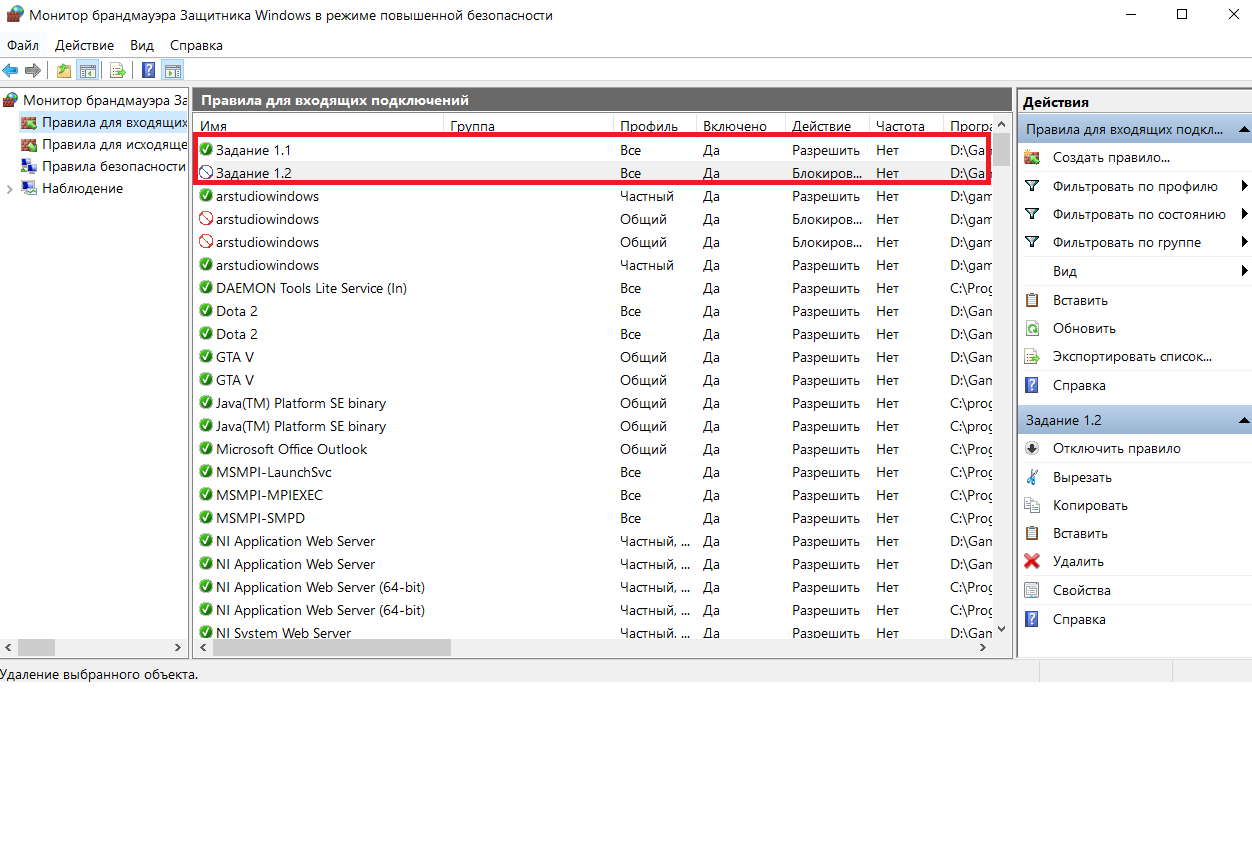


Рис. *1.6* – Общий список

* 1. Проделываем все действия из задания *1*, выбрав другую нужную нам программу, однако в конце нужно будет выбрать во вкладке «Действия – разрешить подключение» (рис. *1.7*)

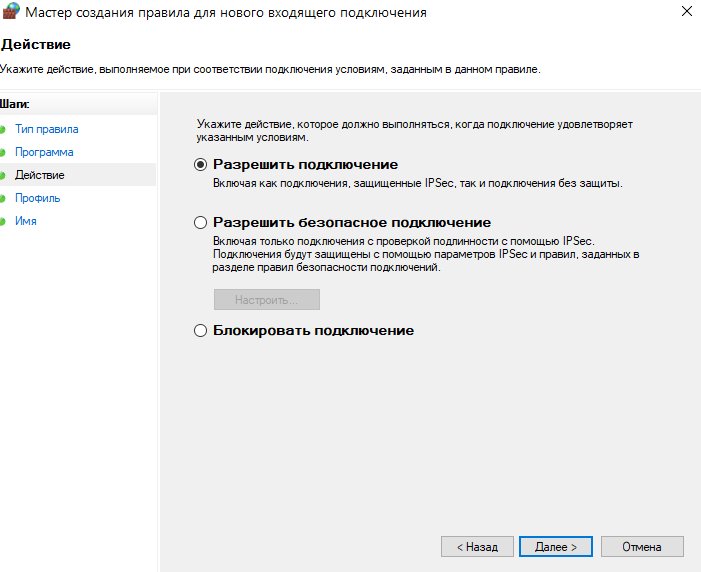


Рис. *1.7* – Окно создания правила, вкладка «Действие»

**Задание 2.** Создать правила для исходящих подключений (1 – на блокировку, 2 – на разрешение)

* 1. Для выполнения данного задания нужно повторить все действия из задания *1.1*, только изначально перейти по вкладке «Правила для исходящего подключения». Созданные правила представлены на рис. *2.1*

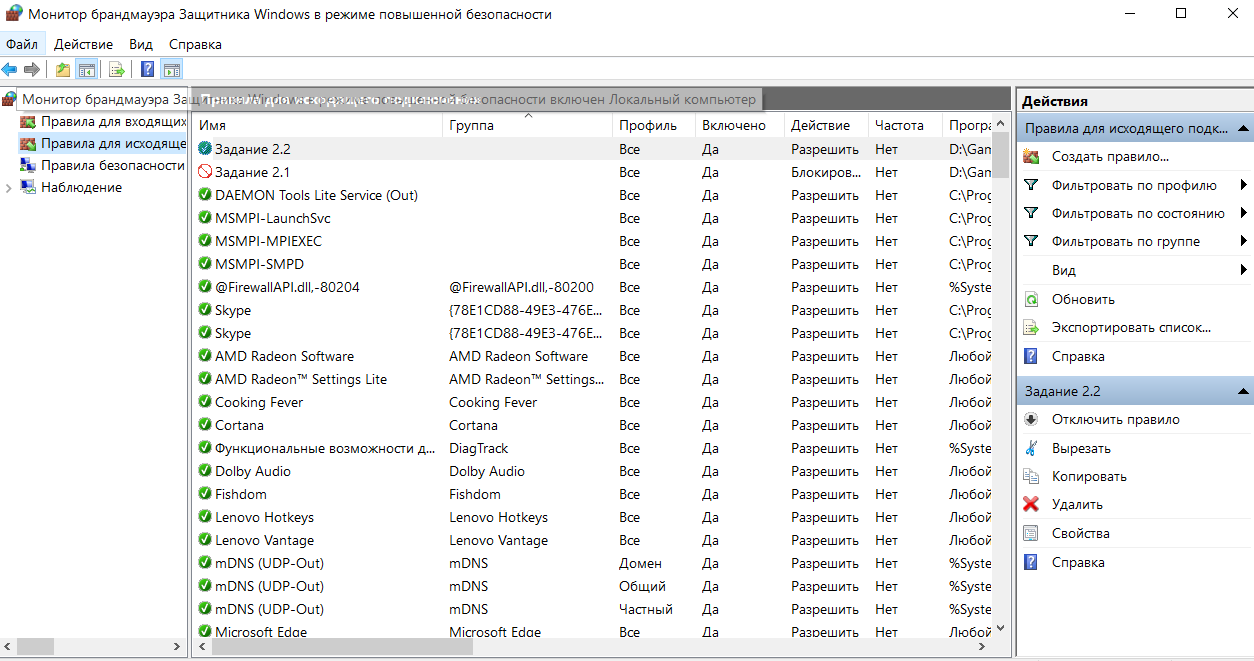
****

Рис. *2.1* – Общий список

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

Для возврата в исходное состояние достаточно в правом окошке действий выбрать пункт «Удалить» для созданных нами ранее правил (рис *3.1*).

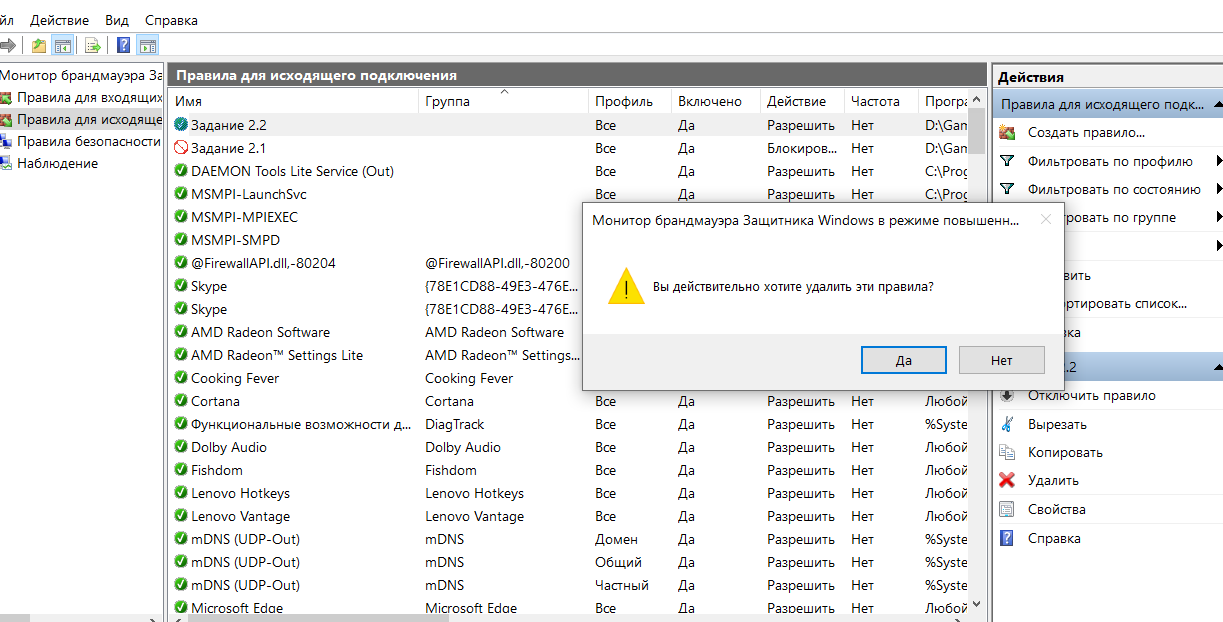


Рис. *3.1* – Удаление правил

В итоге вернём Брандмауэр в исходное состояние (рис. *3.2*).

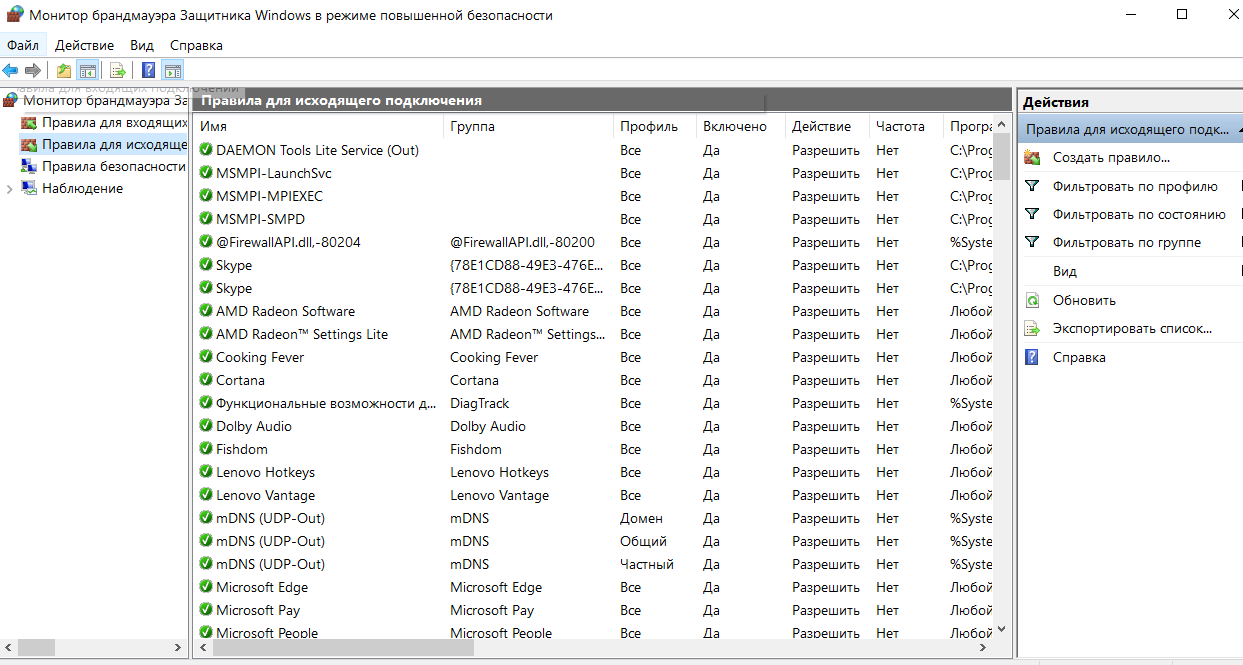
****

Рис. *3.2* – Исходное состояние

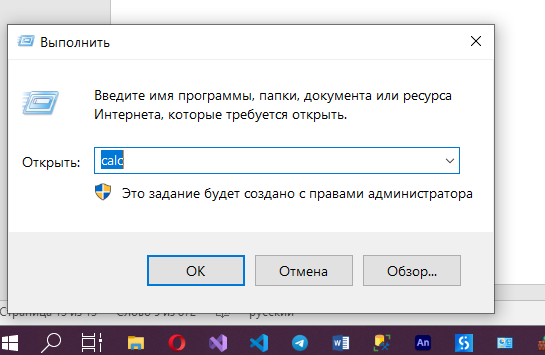
**Задание 4.** Опробовать действие нескольких команд.

Калькулятор-calc  
Командная строка-cmd  
Консоль управления-dcomcnfg

Для выполнения каждой из них нужно нажать сочетание клавиш “Win + R”.

При выполнении первой появится откроется встроенный в систему калькулятор (рис. *4.1*).

При выполнении второй откроется командная строка, а при выполнении третей откроется встроенный в систему калькулятор.

  
Рис. *4.1* – Окно Выполнения

**Вывод:** Овладела навыками настройки и использования Брандмауэра Windows.

# **Практическое занятие №5**

**Тема «Криптографическая защита информации»**

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

**Теоретические сведения**

**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.

Обмен информацией осуществляется в 3 этапа:

* отправитель передает получателю ключ (в случае сети с несколькими абонентами у каждой пары абонентов должен быть свой ключ, отличный от ключей других пар);
* отправитель, используя ключ, зашифровывает сообщение, которое пересылается получателю;
* получатель получает сообщение и расшифровывает его.

Если для каждого дня и для каждого сеанса связи будет использоваться уникальный ключ, это повысит защищенность системы.

При блочном шифровании информация разбивается на блоки фиксированной длины и шифруется поблочно. Блочные шифры бывают двух основных видов:

* шифры перестановки (transposition, permutation, P-блоки);
* шифры замены (подстановки, substitution, S-блоки).

Шифры перестановок переставляют элементы открытых данных (биты, буквы, символы) в некотором новом порядке. Различают шифры горизонтальной, вертикальной, двойной перестановки, решетки, лабиринты, лозунговые и др.

Шифры замены заменяют элементы открытых данных на другие элементы по определенному правилу. Paзличают шифры простой, сложной, парной замены, буквенно-слоговое шифрование и шифры колонной замены. Шифры замены делятся на две группы:

* моноалфавитные (код Цезаря);
* полиалфавитные (шифр Видженера, цилиндр Джефферсона, диск Уэтстоуна, Enigma).

В моноалфавитных шифрах замены буква исходного текста заменяется на другую, заранее определенную букву. Например в коде Цезаря буква заменяется на букву, отстоящую от нее в латинском алфавите на некоторое число позиций.

Очевидно, что такой шифр взламывается совсем просто. Нужно подсчитать, как часто встречаются буквы в зашифрованном тексте, и сопоставить результат с известной для каждого языка частотой встречаемости букв.

В полиалфавитных подстановках для замены некоторого символа исходного сообщения в каждом случае его появления последовательно используются различные символы из некоторого набора. Понятно, что этот набор не бесконечен, через какое-то количество символов его нужно использовать снова. В этом слабость чисто полиалфавитных шифров.

В современных криптографических системах, как правило, используют оба способа шифрования (замены и перестановки). Такой шифратор называют составным (product cipher). Oн более стойкий, чем шифратор, использующий только замены или перестановки.

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

Схема обмена информацией такова:

* получатель вычисляет открытый и секретный ключи, секретный ключ хранит в тайне, открытый же делает доступным (сообщает отправителю, группе пользователей сети, публикует);
* отправитель, используя открытый ключ получателя, зашифровывает сообщение, которое пересылается получателю;
* получатель получает сообщение и расшифровывает его, используя свой секретный ключ.

**Задание 2.** 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.

Текст для шифровки: Кохнюк Александра Сергеевна

Ключ: 5

**Шифр Цезаря.** При шифровании каждый символ заменяется другим, отстоящим от него в алфавите на фиксированное число позиций. Шифр Цезаря можно классифицировать как шифр подстановки, при более узкой классификации — шифр простой замены.

Алфавит:



Шифрование:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Сообщение** | **К** | **О** | **Х** | **Н** | **Ю** | **К** |
| Номер | 12 | 16 | 23 | 15 | 32 | 12 |
| Номер + 5 | 17 | 21 | 28 | 20 | 4 | 17 |
| **Шифр** | **П** | **У** | **Ь** | **Т** | **Г** | **П** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Сообщение** | **А** | **Л** | **Е** | **К** | **С** | **А** | **Н** | **Д** | **Р** | **А** |
| Номер | 1 | 13 | 6 | 12 | 19 | 1 | 15 | 5 | 18 | 1 |
| Номер + 5 | 6 | 18 | 11 | 17 | 24 | 6 | 20 | 10 | 23 | 6 |
| **Шифр** | **Е** | **Р** | **Й** | **П** | **Ц** | **Е** | **Т** | **И** | **Х** | **Е** |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Сообщение** | **С** | **Е** | **Р** | **Г** | **Е** | **Е** | **В** | **Н** | **А** |
| Номер | 19 | 6 | 18 | 4 | 6 | 6 | 3 | 15 | 1 |
| Номер + 5 | 24 | 11 | 23 | 9 | 11 | 11 | 8 | 20 | 6 |
| **Шифр** | **Ц** | **Й** | **Х** | **З** | **Й** | **Й** | **Ж** | **Т** | **Е** |

**Ответ:** ПУЬТГПЕРЙПЦЕТИХЕЦЙХЗЙЙЖТЕ

**Шифр Трисемуса**. Здесь шаг смещения делается переменным, то есть зависящим от каких-либо дополнительных факторов. Например, можно задать закон смещения в виде линейной функции (уравнения зашифрования) позиции шифруемой буквы.

Для получения такого шифра замены обычно использовались таблица для записи букв алфавита и ключевое слово. В таблицу сначала вписывалось по строкам ключевое слово, причем повторяющиеся буквы отбрасывались. Затем эта таблица дополнялась не вошедшими в нее буквами алфавита по порядку.

При шифровании находят в этой таблице очередную букву открытого текста и записывают в шифртекст букву, расположенную ниже ее, в том же столбце. Если буква текста оказывается в нижней строке таблицы, тогда для шифртекста берут самую верхнюю букву из того же столбца.

**Ключевое слово:** ЗАЩИТА

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

КОХНЮКАЛЕКСАНДРАСЕРГЕЕВНА

**Ответ:** УЧЮЦВУЕФПУЫЦОЪЕЫПЪНППМЦЕ

**Шифр Плейфера.** Шифр Плейфера использует матрицу 5х5 (для латинского алфавита, для кириллического алфавита необходимо увеличить размер матрицы до 4х8), содержащую ключевое слово или фразу. Для создания матрицы и использования шифра достаточно запомнить ключевое слово и четыре простых правила. Чтобы составить ключевую матрицу, в первую очередь нужно заполнить пустые ячейки матрицы буквами ключевого слова (не записывая повторяющиеся символы), потом заполнить оставшиеся ячейки матрицы символами алфавита, не встречающимися в ключевом слове, по порядку (в английских текстах обычно опускается символ «Q», чтобы уменьшить алфавит, в других версиях «I» и «J» объединяются в одну ячейку). Ключевое слово может быть записано в верхней строке матрицы слева направо, либо по спирали из левого верхнего угла к центру. Ключевое слово, дополненное алфавитом, составляет матрицу 5х5 и является ключом шифра.

Для того чтобы зашифровать сообщение, необходимо разбить его на биграммы (группы из двух символов), например «Hello World» становится «HE LL OW OR LD», и отыскать эти биграммы в таблице. Два символа биграммы соответствуют углам прямоугольника в ключевой матрице. Определяем положения углов этого прямоугольника относительно друг друга. Затем, руководствуясь следующими 4 правилами, зашифровываем пары символов исходного текста:

1. Если два символа биграммы совпадают (или если остался один символ), добавляем после первого символа «Х», зашифровываем новую пару символов и продолжаем. В некоторых вариантах шифра Плейфера вместо «Х» используется «Q».

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

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

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

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **A** | **B** | **C** | **D** | **E** | **F** | **G** | **H** | **I** | **J** | **K** | **L** | **M** |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| **N** | **O** | **P** | **Q** | **R** | **S** | **T** | **U** | **V** | **W** | **X** | **Y** | **Z** |
| 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

**Ключевое слово:** PROTECTION = PROTECIN

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| P | R | O | T | E |
| C | I | N | A | B |
| D | F | G | H | K |
| L | M | Q | S | U |
| V | W | X | Y | Z |

KOHNYUK ALEKSANDRA SERGEEVNA

**Биграммы:** KO HN YU KQ AL EK SA ND RA SE RG EQ EV NA

KO = GE

HN = GA

YU = ZS

KQ = GU

AL = CS

EK = BU

SA = HY

ND = CG

RA = TI

SE = UT

RG = OF

EQ = OU

EV = PZ

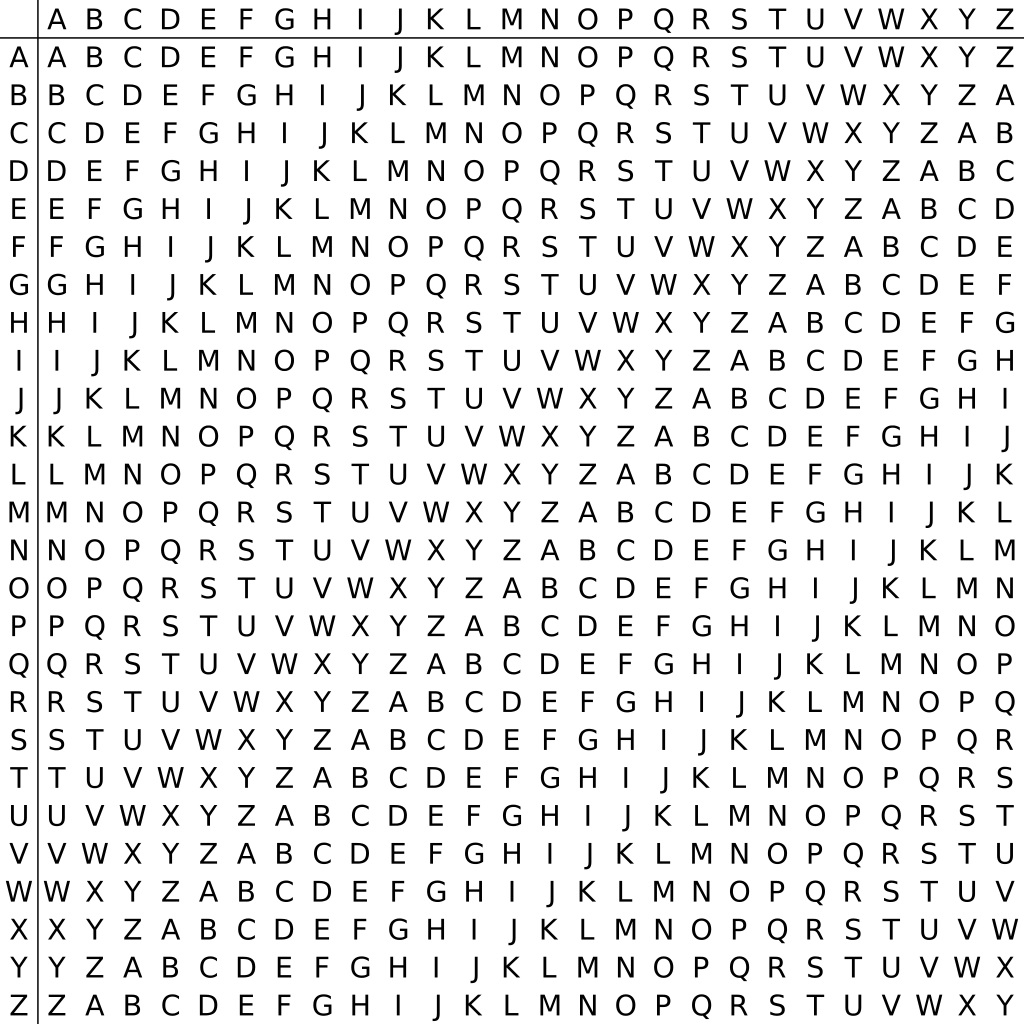
NA = AB

**Ответ**: GEGAZSGUCSBUHYCGTIUTOFOUPZAB.

**Шифрование Вижинера**. Шифр Виженера состоит из последовательности нескольких шифров Цезаря с различными значениями сдвига. Для зашифровывания может использоваться таблица алфавитов, называемая tabula recta или квадрат (таблица) Виженера. Применительно к латинскому алфавиту таблица Виженера составляется из строк по 26 символов, причём каждая следующая строка сдвигается на несколько позиций. Таким образом, в таблице получается 26 различных шифров Цезаря. На каждом этапе шифрования используются различные алфавиты, выбираемые в зависимости от символа ключевого слова.

**Шифруемый текст**: K O H N Y U K A L E K S A N D R A S E R G E E V N A

**Ключ:** P R O T E C T I O N P R OT E C T I O N P R O T E C



**Ответ**: ZFVGCWDIZRZJOGHTTASEVVSORC

**Задание 3**. Расшифровать сообщение “**тяеонаыбиьсрль\_т**” c помощью магического квадрата

|  |  |  |  |
| --- | --- | --- | --- |
| 9 | 16 | 2 | 7 |
| 6 | 3 | 13 | 12 |
| 15 | 10 | 8 | 1 |
| 4 | 5 | 11 | 14 |

Магическими квадратами называются квадратные таблицы со вписанными в их клетки последовательными натуральными числами от 1, которые дают в сумме по каждому столбцу, каждой строке и каждой диагонали одно и то же число.

При расшифровывании текст вписывается в квадрат, и открытый текст читается в последовательности чисел «магического квадрата».

|  |  |  |  |
| --- | --- | --- | --- |
| 9т | 16я | 2е | 7о |
| 6н | 3а | 13ы | 12б |
| 15и | 10ь | 8с | 1р |
| 4л | 5ь | 11- | 14т |

**Ответ:** Реальность бытия.

**Выводы:** Овладела основными криптографическими алгоритмами симметричного шифрования.

# **Практическое занятие №6**

**Тема «Криптографическая защита информации»**

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

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

**RSA (аббревиатура от фамилий Rivest, Shamir и Adleman)** — криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших целых чисел.

**Алгоритм состоит из следующих этапов:**

* 1. Генерация ключей (выбрать два простых различных числа, вычислить модуль (произведение), вычислить функцию Эйлера, выбрать открытую экспоненту, вычислить секретную экспоненту, опубликовать открытый ключ, сохранить закрытый ключ)
  2. Шифрование (выбрать текст для зашифровки, вычислить шифротекст)
  3. Расшифрование (вычислирть исходное сообщение)

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

Алгоритм Диффи-Хелмана (Whitfield Diffie и Martin Hellman, 1976 год) использует функцию дискретного возведения в степень.

Сначала генерируются два больших простых числа *n* и *q*. Эти два числа не обязательно хранить в секрете. Далее один из партнеров P1 генерирует случайное число x и посылает другому участнику будущих обменов P2 значение *A* = *qx* *mod n*

По получении А партнер P2 генерирует случайное число *у* и посылает P2 вычисленное значение *B* = qy mod n

Партнер P1, получив В, вычисляет *Kx* = *Bx mod n*, а партнер P2 вычисляет *Ky = Ay mod n*. Алгоритм гарантирует, что числа *Ky* и *Kx* равны и могут быть использованы в качестве секретного ключа для шифрования. Ведь даже перехватив числа *А* и *В*, трудно вычислить *Kx* или *Ky*.

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

**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.

#include <iostream>

using namespace std;

int power(int a, int b, int n) { // a^b mod n

int tmp = a;

int sum = tmp;

for (int i = 1; i < b; i++) {

for (int j = 1; j < a; j++) {

sum += tmp;

if (sum >= n) {

sum -= n;

}

}

tmp = sum;

}

return tmp;

}

int mul(int a, int b, int n) { // a\*b mod n

int sum = 0;

for (int i = 0; i < b; i++) {

sum += a;

if (sum >= n) {

sum -= n;

}

}

return sum;

}

void rsa()

{

int p, q, eiler, e, n, m, c;

double d;

cout << "Введите простое число p: ";

cin >> p;

cout << "Введите простое число q: ";

cin >> q;

cout << "Введите открытую экспоненту е: ";

cin >> e;

n = p \* q;

eiler = (p - 1) \* (q - 1);

cout << "Произведение: " << n << endl;

cout << "Функция Эйлера: " << eiler << endl;

cout << "Открытая экспонента: " << e << endl;

d = power(e, -1, eiler);

cout << "Секретная экспонента: " << d << endl;

cout << "Открытый ключ: {" << e << ", " << n << "}" << endl;

cout << "Закрытый ключ: {" << d << ", " << n << "}" << endl << endl;

cout << "Введите число для зашифровки: ";

cin >> m;

c = power(m, e, n);

cout << "Шифротекст: " << c << endl << endl;

cout << "Расшифровка: " << power(c, d, n);

}

void diffie()

{

int p, g, a = 6, b = 15;

cout << "Введите простое число p: ";

cin >> p;

cout << "Введите простое число g, которое меньше " << p << "): ";

cin >> g;

cout << "Секретный ключ Алисы: " << a << endl;

cout << "Секретный ключ Боба: " << b << endl;

cout << "Открытый ключ Алисы: " << power(g, a, p) << endl;

cout << "Открытый ключ Боба: " << power(g, b, p) << endl;

cout << "Общий секретный ключ (по Алисе): " << power(power(g, b, p), a, p) << endl;

cout << "Общий секретный ключ (по Бобу): " << power(power(g, a, p), b, p) << endl;

}

void elgamal()

{

int M, M1, p, g, x, y, k, a, b;

cout << "Введите простое число p: ";

cin >> p;

cout << "Введите случайный примитивный элемент g: ";

cin >> g;

cout << "Введите случайное целое число х (1 < x < " << p - 1 << "): ";

cin >> x;

y = power(g, x, p);

cout << "Открытый ключ: тройка (" << p << ", " << g << ", " << y << ")" << endl;

cout << "Закрытый ключ: " << x << endl;

cout << "Введите число для шифрования: ";

cin >> M;

cout << "Введите сессионный ключ (1 < k < " << p - 1 << "): ";

cin >> k;

a = power(g, k, p);

b = mul(power(y, k, p), M, p);

cout << "Шифротекст: пара (а, b) = (" << a << ", " << b << ")" << endl << endl;

M1 = mul(b, power(a, p - 1 - x, p), p);

cout << "Расшифровка: " << M1;

}

int main()

{

int pulse;

setlocale(LC\_CTYPE, "Rus");

do

{

cout << endl << "Выберите тип шифровки:" << endl;

cout << "1) RSA" << endl;

cout << "2) Диффи-Хеллман" << endl;

cout << "3) Эль-Гамаль" << endl;

cout << "4) Выход" << endl;

cout << "-------------------------------" << endl;

cin >> pulse;

switch (pulse)

{

case 1: rsa(); break;

case 2: diffie(); break;

case 3: elgamal(); break;

case 4: break;

}

} while (pulse != 4);

}

**Выводы:** Овладение основными криптографическими алгоритмами асимметричного шифрования.

# **Практическое занятие №7**

**Тема «Криптографическая защита информации»**

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

**Теоретические сведения**

Протоколы ЭЦП с одной стороны относят к протоколам аутентификации, т.к. гарантируют, что сообщение поступило от достоверного отправителя, а с другой стороны к протоколам контроля целостности, т.к. гарантируют, что сообщение пришло в неискаженном виде. Более того, получатель в дальнейшем может использовать ЭЦП как доказательство достоверности сообщения третьим лицам (арбитру) в том случае, если отправитель впоследствии попытается отказаться от него.

**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").

**Ответы на 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

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

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.

**3. Перечислите специальные схемы ЭЦП.**

**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;

#include <iostream>

using namespace std;

int power(int a, int b, int n) { // a^b mod n

int tmp = a;

int sum = tmp;

for (int i = 1; i < b; i++) {

for (int j = 1; j < a; j++) {

sum += tmp;

if (sum >= n) {

sum -= n;

}

}

tmp = sum;

}

return tmp;

}

void rsa()

{

int p = 17, q = 5, eiler, e = 3, n, h1 = 10, h2, c, d, s;

cout << "p = " << p << endl;

cout << "q = " << q << endl;

n = p \* q;

eiler = (p - 1) \* (q - 1);

cout << "Произведение:" << n << endl;

cout << "Функция Эйлера: " << eiler << endl;

cout << "Открытая экспонента: " << e << endl;

/\* d = power(e, -1, eiler); \*/ d = 43;

cout << "Секретная экспонента: " << d << endl;

cout << "Открытый ключ: {" << e << ", " << n << "}" << endl;

cout << "Закрытый ключ: {" << d << ", " << n << "}" << endl << endl;

cout << "Число для зашифровки: " << h1 << endl;

c = power(h1, e, n);//шифртекст

cout << "Шифротекст: " << c << endl;

cout << "Расшифровка: " << power(c, d, n) << endl; // c^d mod n

s = power(h1, d, n); // h1^d mod n

h2 = power(s, e, n); // s^e mod n, вычисление хеш-образа из цп

if (h1 == h2)

{

cout << "Подпись правильная!" << endl;

}

else

{

cout << "Подпись некорректная" << endl;

}

}

int main()

{

int pulse;

setlocale(LC\_CTYPE, "Rus");

rsa();

}

**Вывод:** **Изучила и закрепила умение реализации ЭЦП на примере RSA.**

# **Практическое занятие №8**

**Тема «Криптографическая защита информации»**

**Цель:** Получение основных сведений из курса теории чисел**.**

**Теоретические сведения**

Ниже рассматриваются: *N* – множество натуральных чисел, *Z* – множество рациональных чисел. Множество целых чисел *Z* – счетное, состоит из элементов 0; ±1; ±2; …; ± *n*,…. На нем определены две алгебраические операции – сложение и умножение. Эти операции обладают следующими свойствами (для любых ):

1. ассоциативность: ; ;

2. коммутативность: ; ;

3. существует нейтральный элемент – 0 и 1 соответственно:



4.  – закон дистрибутивности;

5. для каждого целого  существует единственное противоположное, то есть такое целое *b*, что *a* + *b* = *b* + *a* = 0.

*Теорема 2.1* (*О делении с остатком*). Для любых целых чисел *a* и *b*, , существует единственные целые числа *q* и  , такие, что .

В этом равенстве  называют остатком, а  – частным (неполным частным – при ) от деления *a*  на  При *r* = 0 величины *b* и *q* называют делителями или множителями числа *а*. Читатель со школьной скамьи умеет находить частное и остаток методом деления уголком.

Если целые числа  делятся на целое , то *d*  называют их *общим делителем*.

В дальнейшем речь идет только о положительных целых делителях.

Максимальный из общих делителей целых чисел  называется их *наибольшим общим делителем* и обозначается через НОД ().

*Теорема 2.2.* Если *,* то НОД *(a, b)*=НОД *(b, c).*

Теорема 2.2 позволила Евклиду (примерно 2300 лет тому назад) обосновать следующий факт.

*Теорема 2.3.* Наибольший общий делитель целых чисел  *a* и *b*   равен последнему отличному от нуля остатку цепочки равенств:

*;*

*;*

*…………………*

**

**

то есть  *=* НОД *.*

Теорема 2.3 формулирует алгоритм Евклида нахождения наибольшего общего делителя целых чисел. Его вариантом является следующий – второй способ вычисления наибольшего общего делителя по алгоритму Евклида – вычисляем последовательно разности  до получения последней ненулевой разности, которая и совпадает с НОД *(a, b).*

**Задание для выполнения**

**Вариант 5**

1.Найти канонические разложения чисел *а = 9118515943* и *b = 3386496689*

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 ** на 23.

**Задание 1.** Найти канонические разложения чисел:

9118515943 = 97 \* 97 \* 97 \* 97 \* 103

3386496689 = 97 \* 97 \* 419 \* 859

**Задание 2.** Найти НОД :

А) По алгоритму Евклида:

9 118 515 943 / 3 386 496 689 = 2 (остаток 2 345 522 565)

3 386 496 689 / 2 345 522 565 = 1 (остаток 1 040 974 124)

2 345 522 565 / 1 040 974 124 = 2 (остаток 263 574 317)

1 040 974 124 / 263 574 317 = 3 (остаток 250 251 173)

263 574 317 / 250 251 173 = 1 (остаток 13 323 144)

250 251 173 / 13 323 144 = 18 (остаток 10 434 581)

13 323 144 / 10 434 581 = 1 (остаток 2 888 563)

10 434 581/ 2 888 563 = 3 (остаток 1 768 892)

2 888 563/ 1 768 892 = 1 (остаток 1 119 671)

1 768 892 / 1 119 671 = 1 (остаток 649 221)

1 119 671 / 649 221 = 1 (остаток 470 450)

649 221 / 470 450 = 1 (остаток 178 771)

470 450 / 178 771 = 2 (остаток 112 908)

178 771 / 112 908 = 1 (остаток 65 863)

112 908 / 65 863 = 1 (остаток 47 045)

65 863 / 47 045 = 1 (остаток 18 818)

47 045 / 18 818 = 2 (остаток 9 409)

**18 818 / 9 409 = 2 (остаток 0),** так как 18818 = 9409 \* 2 + 0,равен 0, значит НОД равен предыдущему остатку от деления - **9409**

Б) Разложение чисел на простые множители:

9118515943 = 97 \* 97 \* 97 \* 97 \* 103

3386496689 = 97 \* 97 \* 419 \* 859

**НОД(а, б) = 97 \* 97 = 9409**

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

9118515943*u +* 3386496689*v = 9409*

*u =* 151238 *v =* -407225

**Задание 4.** Найти остаток от деления ** на 23.

1999 делится на 23 с остатком 21, 19992 делится на 23 с остатком 4, 19993 делится на 23 с остатком 15, 19994 делится на 23 с остатком 16, 19995 делится на 23 с остатком 14, 19996 делится на 23 с остатком 18, 19997 делится на 23 с остатком 10, 19998 делится на 23 с остатком 3, 19999 делится на 23 с остатком 17, 199910 делится на 23 с остатком 12, 199911 делится на 23 с остатком 22, 199912 делится на 23 с остатком 2, 199913 делится на 23 с остатком 19, 199914 делится на 23 с остатком 8, 199915 делится на 23 с остатком 7, 199916 делится на 23 с остатком 9, 199917 делится на 23 с остатком 5, 19994 делится на 23 с остатком 13

21 делится на 23 с остатком 21, 212 делится на 23 с остатком 4, 213 делится на 23 с остатком 15, 214 делится на 23 с остатком 16, 214 делится на 23 с остатком 14, 216 делится на 23 с остатком 18, 217 делится на 23 с остатком 10, 218 делится на 23 с остатком 3, 219 делится на 23 с остатком 17, 2110 делится на 23 с остатком 12, 2111 делится на 23 с остатком 22, 2112 делится на 23 с остатком 19, 2114 делится на 23 с остатком 8, 2115 делится на 23 с остатком 7, 213 делится на 23 с остатком

** mod 23 = 15

# **Практическое занятие №9**

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

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

**Ответить на следующие вопросы:**

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

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

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

*1. 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.

*2. Производные произведении*

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

*3. 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 права 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 других государств (и их правопреемников), обнародованные (либо необнародованные, но находящиеся в какой-либо объективной форме) за пределами РБ - в соответствии с международными договорами РБ.

**Авторское право не распространяется на идеи, методы, процессы, системы, способы, концепции, принципы, открытия, факты.**

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

*Личные неимущественные права:*

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

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

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

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

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

1. **Каковы особенности авторского права на составные произведения?**

*Авторское право 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.

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. **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.

**Но недееспособные, став субъектами авторского права, не имеют 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.**

За авторами - гражданами РБ и их правопреемниками авторское право признается на все произведения независимо от места их обнародования или нахождения в какой-либо объективной форме.

**Авторское право может принадлежать нескольким лицам - соавторам.** Авторское право на произведение, созданное совместным творческим трудом двух или более лиц, принадлежит соавторам совместно, независимо от того, образует ли такое произведение одно неразрывное целое или состоит из частей, каждая из которых имеет самостоятельное значение.

**Соавторство всегда является результатом соглашения о совместной работе.** По крайней мере, между соавторами должно быть хотя бы устное или подразумеваемое соглашение о создании коллективного произведения.

Нераздельное соавторство возникает в отношении произведения, составляющего одно неразрывное целое. При нераздельном соавторстве выделить долю каждого автора в произведении невозможно, поэтому все соавторы пользуются неделимым авторским правом на всё произведение в целом и на каждую его часть.

Раздельное соавторство возникает на одно произведение, каждая часть которого выполнена самостоятельным автором, и долю каждого из них можно легко установить (соавторство композитора и либреттиста, соавторство на учебник группы авторов и т.д.). В этом случае наряду с совместным и неделимым правом всех соавторов на произведение в целом каждый из авторов сохраняет свое право на созданную им часть произведения, имеющую самостоятельное значение. Например, можно требовать указания своего авторства в отношении этой части и самостоятельно распоряжаться ее использованием, поскольку такое осуществление возможно отдельно от других частей, если иное не предусмотрено соглашением между соавторами.

Отношения между соавторами могут быть определены их соглашением. При отсутствии такого соглашения авторское право на коллективное произведение осуществляется всеми соавторами совместно. Споры между соавторами разрешаются судом.

1. **Что такое авторский договор?**

**Авторский договор –** соглашение, по которому одна сторона (автор) передает или обязуется передать в будущем имущественные права на произведение, а другая сторона (правообладатель) обязуется выплатить обусловленное сторонами вознаграждение, обеспечив при использовании указанных прав личные неимущественные права автора.

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

*В зависимости от степени готовности произведения выделяют:*

1) авторский договор заказа;

2) авторский договор на готовое произведение.

Также выделяют:

1) авторский договор на обнародованное произведение;

2) авторский договор на необнародованное произведение.

*В зависимости от характера передаваемых прав выделяют:*

1) авторский договор о передаче исключительных прав;

2) авторский договор о передаче неисключительных прав.

*В зависимости от способа использования произведения выделяют:*

1) издательский авторский договор;

2) постановочный авторский договор;

3) сценарный авторский договор;

4) авторский договор о депонировании рукописи;

5) авторский договор художественного заказа;

6) авторский договор об использовании в промышленности произведений декоративно-прикладного искусства;

7) авторский договор о передаче произведения в эфир или сообщении для всеобщего сведения по кабелю.

1. **Основные составляющие авторского договора?**

*В авторском договоре должны быть предусмотрены:*

* способы использования произведения (конкретные права, передаваемые по данному договору);
* срок, на который передается право;
* территория, на которой может осуществляться использование;
* размер вознаграждения и (или) порядок определения размера вознаграждения за каждый способ использования произведения, порядок и сроки его выплаты;
* другие условия, которые стороны сочтут существенными для данного договора.

Условия об объеме передаваемых прав по авторскому договору и размер вознаграждения являются существенными условиями договора.

**К другим важным условиям авторского договора относятся условия о сроке и территории, на которые передается право.** Но данные условия не являются обязательными, поскольку их отсутствие не влечет недействительности авторского договора.

**Немаловажное значение имеет соглашение о размере вознаграждения.**

Не каждый автор, заключив договор с издателем, может определить в твердой сумме вознаграждение или оценить успех своего произведения. В договоре должна быть сделана «оговорка об успехе».

**В авторский договор с участием**[**иностранных**](http://baza-referat.ru/%D0%98%D0%BD%D0%BE%D1%81%D1%82%D1%80%D0%B0%D0%BD%D1%86%D1%8B)**лиц должна быть включена валютная оговорка**. *Валютная оговорка*— это условие договора, которое указывает на то, валюта какой страны выступает в качестве валюты долга, в какой валюте должен быть произведен платеж и каким должно быть курсовое соотношение между указанными валютами на момент платежа.

Также авторским договором заказа должно быть установлено соглашение о творческой неудаче.

Все вышесказанное позволяет сделать вывод, что существенным условием авторского договора прежде всего является предмет договора. В отличие от таких условий, как срок и территория передачи авторского права, цена устанавливается соглашением сторон, несогласование этого условия приведет к признанию договора незаключенным.

**Вывод**: изучила основные положения авторского права и смежных прав.

# **Практическое занятие №10**

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

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

**Ответить на следующие вопросы:**

1. **Основные составляющие описания изобретения?**

Описание 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?**

*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.

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

**Аналог изобретения** – это известное до даты приоритета средство того же назначения, совокупность признаков которого сходна с совокупностью существующих признаков изобретения.

Приоритет изобретения устанавливается по дате поступления в патентный орган надлежащим образом оформленной заявки. Если в процесс экспертизы установлено, что идентичное изобретение имеет одну и туже дату приоритета, то патент может быть выдан по заявке, но которой доказана более ранняя дата ее отправки в патентный орган.

**За прототип изобретения принимается аналог наиболее близкий по совокупности признаков**. К приводимым сведениям о каждом из аналогов, в то числе о прототипе относятся библиографические данные источника информации, в котором он раскрыт, признаки аналога с указанием тех из них, которые совпадают с существенными признаками заявляемого изобретения, а также указание причин, препятствующих получению требуемого технического результата. Если аналогов несколько, то последним описывается прототип.

**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.

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

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.

**Патент** — охранный документ, удостоверяющий исключительное право, авторство и приоритет изобретения, полезной модели, промышленного образца либо селекционного достижения

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

**Вместе с заявкой 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.**

**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.**

**Описание изобретения наряду с формулой изобретения и графическими материалами (если они необходимы) является основным** **документом на выдачу патента.** Оно представляет собой технико-правовой документ и должно полностью раскрывать техническую сущность изобретения, а также содержать достаточную информацию для дальнейшей разработки объекта изобретения. Кроме того, описание изобретения должно давать точное и ясное представление о новизне, изобретательском уровне и промышленной применимости изобретения.

1. **ОТЛИЧИЯ заявок на охранные документы различных объектов промышленной собственности?**

Составление и оформление заявок на объекты промышленной собственности (изобретение, полезную модель, промышленный образец, товарный знак и др.).

**Алгоритм патентования:**

* отбор изобретений для патентования;
* подготовка заявок на выдачу патентов;
* подача заявок в соответствующие патентные ведомства;
* ведение переписки с патентными ведомствами в процессе проведения экспертизы по заявкам на патенты;
* ведение переписки по патентным спорам с административными и судебными органами;
* получение патентов;
* оплата пошлин за юридически значимые действия;
* поддержание в силе заявок на патенты и собственно патентов.

1. **На какие ОПС выдаются патенты?**

Изобретению может быть предоставлена правовая охрана, если оно:

* относится к продукту или способу, в частности, устройству, способу, веществу, биотехнологическому продукту, а также применению устройства, способа, вещества, биотехнологического продукта по определенному назначению
* является новым
* имеет изобретательский уровень
* промышленно применимо

**Изобретение признается новым, если оно не является частью уровня техники.**

**Изобретение признается имеющим изобретательский уровень, если оно для специалиста в той области, к которой оно относится, не следует явным образом из уровня техники**.

При этом в уровень техники включаются любые сведения, ставшие общедоступными в мире до даты приоритета изобретения, а также все имеющие более ранний приоритет поданные в Республике Беларусь другими лицами не отозванные заявки на изобретения и полезные модели и запатентованные в Республике Беларусь изобретения и полезные модели.

Не признается обстоятельством, препятствующим соответствию изобретения критериям патентоспособности, такое раскрытие информации, относящейся к заявленному техническому решению, автором, заявителем или любым лицом, которое получило от них прямо или косвенно эту информацию, при котором сведения о сущности изобретения стали общедоступными, если заявка на изобретение подана в Национальный центр интеллектуальной собственности не позднее двенадцати месяцев с даты раскрытия информации.

Изобретение признается промышленно применимым, если оно может быть использовано в промышленности, сельском хозяйстве, здравоохранении и других сферах деятельности.

**Не признаются патентоспособными**:

* сорта растений и породы животных;
* топологии интегральных микросхем;
* изобретения, противоречащие общественным интересам, принципам гуманности и морали.

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

**Свидетельство выдается на товарный знак, на географические указания на 10 лет с последующим продлением на неопределенное количество раз по 10 лет.**

**Товарным знаком и знаком обслуживания** (далее — товарный знак) признается обозначение, способствующее отличию товаров или услуг одного лица от однородных товаров или услуг других лиц. Правовая охрана товарного знака на территории Республики Беларусь осуществляется на основании его регистрации в патентном органе в порядке, установленном законодательством о товарных знаках и знаках обслуживания, или в силу международных договоров Республики Беларусь.

**Вывод:** Овладела навыками составления и оформления заявок на объекты промышленной собственности.

# **Практическое занятие №11**

**Тема «Патентный поиск»**

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

**Теоретические сведения**

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

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

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

##### **МЕЖДУНАРОДНЫЕ КЛАССИФИКАТОРЫ**

Для обеспечения единообразия в международном масштабе распределения патентных документов, а также упрощения поиска необходимой патентной документации применяются специально разработанные патентные классификаторы.

**Международная патентная классификация (МПК)**, принятая в соответствии со Страсбургским соглашением 1971 года, предусматривает создание единой системы классификации, охватывающей патенты на изобретения, включая опубликованные патентные заявки, авторские свидетельства, полезные модели и свидетельства о полезности. Аббревиатура **«МПК»** является общепринятым обозначением Международной патентной классификации.

**Международная классификация промышленных образцов (МКПО)** была принята 8 октября 1968 года дипломатической конференцией в г. Локарно (Швейцария), на которую были приглашены все страны-участницы Парижской конвенции по охране промышленной собственности.

**Международная классификация товаров и услуг (МКТУ)** в соответствии с Ниццким соглашением от 15 июня 1957 г., отражая единую классификацию товаров и услуг для регистрации товарного знака, позволяет c максимальной достоверностью идентифицировать и, соответственно, классифицировать товар или услугу с обеспечением их единообразного восприятия всеми заинтересованными лицами.

**Универсальная десятичная классификация** **(УДК),** первое сводное издание которой, вышло в 1905 г. в Брюсселе, получила широкое применение в качестве единой системы классификации информационных материалов в области естественных и технических наук. Ее применение позволяет обеспечить единообразие в организации справочно-информационных фондов в органах научно-технической информации, научных и технических библиотеках страны.

##### МЕЖДУНАРОДНАЯ ПАТЕНТНАЯ КЛАССИФИКАЦИЯ (МПК)

**МПК** является средством для единообразного в международном масштабе классифицирования патентных документов, позволяет эффективно осуществлять поиск патентных документов с целью установления новизны и оценки вклада изобретателя в заявленное техническое решение (включая оценку технической прогрессивности и полезного результата).

**МПК**, кроме того, является:

* инструментом для упорядоченного хранения патентных документов, что облегчает доступ к содержащейся в них технической и правовой информации;
* основой для избирательного распределения информации среди потребителей патентной информации;
* основой для определения уровня техники в отдельных областях;
* основой для получения статистических данных в области промышленной собственности, что в свою очередь позволит определять уровень развития различных отраслей техники.

**МПК** охватывает все области знаний, объекты которых могут подлежать защите охранными документами. Иерархическая структура МПК выражается в разбивке всех областей знаний на несколько классификационных уровней. В нисходящем порядке эти уровни иерархии соответствуют разделам, классам, подклассам, основным группам и подгруппам.

По своей структуре МПК разделена на восемь основных разделов.

***Индекс раздела.*** Каждый раздел обозначен заглавной буквой латинского алфавита от **А** до **Н**.

***Заголовок раздела*** лишь приблизительно отражает его содержание. Разделы имеют следующие названия:

**A**  - УДОВЛЕТВОРЕНИЕ ЖИЗНЕННЫХ ПОТРЕБНОСТЕЙ ЧЕЛОВЕКА

**B** - РАЗЛИЧНЫЕ ТЕХНОЛОГИЧЕСКИЕ ПРОЦЕССЫ; ТРАНСПОРТИРОВАНИЕ

**C**  - ХИМИЯ; МЕТАЛЛУРГИЯ

**D**  - ТЕКСТИЛЬ; БУМАГА

**E**  - СТРОИТЕЛЬСТВО; ГОРНОЕ ДЕЛО

**F**  - МЕХАНИКА; ОСВЕЩЕНИЕ; ОТОПЛЕНИЕ; ДВИГАТЕЛИ И НАСОСЫ; ОРУЖИЕ; БОЕПРИПАСЫ; ВЗРЫВНЫЕ РАБОТЫ

**G**  - ФИЗИКА

**H**  - ЭЛЕКТРИЧЕСТВО

***Содержание раздела***. В оглавлении к каждому разделу помещен перечень относящихся к нему *классов* и *подклассов*.

***Подраздел.*** Внутри разделов родственные классы условно объединяются в подразделы, которые не обозначаются индексами.

Например, в разделе **D** имеются подразделы:

натуральные и химические нити и волокна; прядение; пряжа; окончательная обработка пряжи; ткачество; плетение; изготовление кружев; трикотажно-вязальное производство; нетканые материалы; шитье, вышивание, производство прошивных изделий; обработка текстильных изделий, стирка, эластичные материалы; канаты, тросы или кабели; производство бумаги; производство целлюлозы.

***Класс.*** Каждый раздел делится на классы. Индекс класса состоит из индекса раздела и двузначного числа.

Например: **D 06**

Заголовок класса отражает его содержание.

Например: **D 06** Обработка текстильных изделий; стирка; эластичные материалы, не отнесенные к другим классам

Далее идет разбивка по подклассам, основным группам и подгруппам.

***Полный классификационный индекс.***  Полный классификационный индекс состоит из комбинации символов, используемых для обозначения раздела, класса, подкласса и основной группы или подгруппы.

**МЕЖДУНАРОДНАЯ КЛАССИФИКАЦИЯ ПРОМЫШЛЕННЫХ ОБРАЗЦОВ (МКПО)**

**МКПО** служит для классифицирования промышленных образцов и состоит из перечня классов и подклассов и алфавитного перечня наименований изделий, в котором промышленные образцы объединены с указанием соответствующих им классов и подклассов.

Например: **Класс 02** - предметы одежды, галантерея.

**МЕЖДУНАРОДНАЯ КЛАССИФИКАЦИЯ ТОВАРОВ И УСЛУГ (МКТУ)**

**МКТУ** используется при регистрации товарных знаков либо в качестве основной (единственной), либо вспомогательной классификации. В официальных публикациях о регистрации знаков указываются номера классов **МКТУ** товаров/услуг, в отношении которых зарегистрированы знаки.

Заголовки **классов** указывают в общем виде только области, к которым товары и услуги в принципе могут относиться, и не содержат названия конкретных товаров или услуг.

Для правильной классификации каждого конкретного товара или услуги необходимо пользоваться непосредственно перечнями товаров и услуг и пояснениями к каждому классу.

Например: **Класс 25 -** Одежда, обувь, головные уборы.

В опубликованные в официальных бюллетенях формы заявки на изобретение, полезную модель, промышленный образец и товарный знак с указанием соответствующих кодов МПК, МКПО и МКТУ

**ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТ ПО ПАТЕНТНЫМ ИССЛЕДОВАНИЯМ**

В общем случае, порядок выполнения работ по патентным исследованиям состоит из следующих этапов.

***ПЕРВЫЙ ЭТАП.***  *Разработка регламента поиска*.

Регламент поиска включает выбор источников информации страны, в которой будет вестись поиск, его ретроспективу и указание источников (этот этап оформляется в виде таблицы 1).

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Таблица 1 – Источники информации | | | | | | | | | | | |
| Источники информации, по которым будет проводиться поиск | | | | | | | | | | | |
| Предмет поиска (объект исследования, его составные части | Страна поиска | патентные | | НТИ | | конъюнктурные | | другие | | Ретро-спективность | Наименование информа-ционной базы (фонда) |
| наименование | Классификационные  рубрики: МПК (МКИ)\*  МКПО\*\* МКТУ\*\*\* другие | наименование | Рубрики УДК\*\*\*\* и другие | наименование | код товара ГС СМТК БТН | наименование | Классификационные индексы |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |

\* - МПК – Международная патентная классификация, МКИ – Международная классификация изобретений (обозначение, применяемое до 1 января 1990 г.).

\*\* - МКПО – Международная классификация промышленных образцов.

\*\*\* - МКТУ – Международная классификация товаров и услуг.

\*\*\*\* - УДК – Универсальная десятичная классификация.

Основные сведения по структуре и применению международных классификаторов приводятся ниже в тексте.

***ВТОРОЙ ЭТАП.***  *Поиск и отбор патентной и другой научно-технической документации.*

Поиск должен осуществляться при наименьших затратах времени и с помощью автоматизированных информационных систем. Поиск в зарубежном патентном ведомстве должен быть согласован с национальным патентным ведомством – ***Национальным центром интеллектуальной собственности***. Материалы, отобранные для поиска должны включать патентную документацию, научно-техническую, конъюнктурную, ТНПА (технические нормативно-правовые акты) и материалы государственной регистрации НИОКР (научно-исследовательские и опытно-конструкторские работы).

Данный этап оформляется в виде таблиц 2 и 3.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Таблица 2 – 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) |
| 1 | 2 | 3 | 4 | 5 |

|  |  |  |  |
| --- | --- | --- | --- |
| Таблица 3 – Научно-техническая, конъюнктурная, ТНПА и материалы государственной регистрации НИОКР | | | |
| Предмет поиска (объект исследования, его составные части) | Наименование источника информации с указанием страницы источника, номера и даты госрегистрации для НИОКР | Автор, фирма (держатель) технической документации | Год, место и орган издания (утверждения, депонирования источника), дата и № регистрации для НИОКР |
| 1 | 2 | 3 | 4 |

***ТРЕТИЙ ЭТАП.***  *Систематизация и анализ отобранной документации.*

По выявленным в процессе поиска документам, требующим, например, в случае нарушения прав ОПС незамедлительного принятия решений руководством организации, выводы и рекомендации исполнителей патентных исследований оформляются экспертным заключением.

В общем случае анализ отобранной документации включает:

* технический уровень и тенденции развития объекта;
* патентно-лицензионную ситуацию;
* использование ОПС и наличие у них правовой охраны;
* исследование патентной чистоты объекта.

***ЧЕТВЕРТЫЙ ЭТАП.***  *Оформление результатов исследований в виде отчета о патентных исследованиях.*

Отчет о патентных исследованиях должен содержать:

* титульный лист;
* список исполнителей;
* содержание;
* перечень сокращений, условных обозначений, символов, единиц, терминов;
* общие данные об объекте исследования;
* основную (аналитическую) часть;
* заключение;
* приложения.

Каждый из разделов ***аналитической части*** (ее содержание определяет третий этап) должен содержать:

* анализ и обобщение информации в соответствии с поставленными перед патентными исследованиями задачами;
* выводы и рекомендации для достижения конечного результата данной работы;
* оценку соответствия результатов патентных исследований заданию на их проведение, обоснование необходимости проведения дополнительных исследований.

В ***заключении*** в общем случае приводят:

* оценку состояния выполнения работы, составной частью которой являются патентные исследования, и ее соответствие планам программ, перспективным целям деятельности предприятия (организации);
* предложения по использованию результатов патентных исследований для создания новых объектов техники, замены или снятия с производства неконкурентоспособных объектов техники, приобретения лицензий, правовой охраны ОПС, получения доходов от продажи лицензий на ОПС или «ноу-хау».

Разделы аналитической части отчета иллюстрируются таблицами, например *патентно-лицензионная ситуация* (таблица 4), *исследование патентной чистоты объекта техники* (таблица 5).

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Таблица 4 – Патентно-лицензионная ситуация | | | | | | |
| Объект техники и его составные части | Страна подачи заявки | Количество патентов, опубликованных заявок по годам подачи заявки (исключая патенты-аналоги) | | | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7\* |

\* - Количество граф определяется глубиной поиска.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Таблица 5 - Исследование патентной чистоты объекта | | | | | | | |
| Наименование объекта техники и его составных частей | Обозначение (чертежей, ГОСТ, ТУ и т.д.). Дата утверждения чертежа | Страна, в отношении которой произво-дится исследо-вание патентной чистоты | Источники известности | | Действую-щие охран-ные доку-менты (в том числе патенты, аналоги, выложен-ные и ак-цептован-ные заяв-ки), подле-жащие анализу | Необходи-мость про-ведения сопостави-тельного анализа с объектом промыш-ленной собствен-ности («Подлежит» – «Не подлежит») | Приме-чание |
| Необходи-мость проведения сопостави-тельного анализа с объектом промыш-ленной собствен-ности («Подлежит» – «Не подлежит») | Патенты, выложен-ные и акцептован-ные заявки (номер доку-мента, даты приоритета и публика-ции, назва-ние объекта промышленной собст-венности, другие биб-лиографи-ческие данные) |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |

**Задание для выполнения.**

#### **Задание 1**

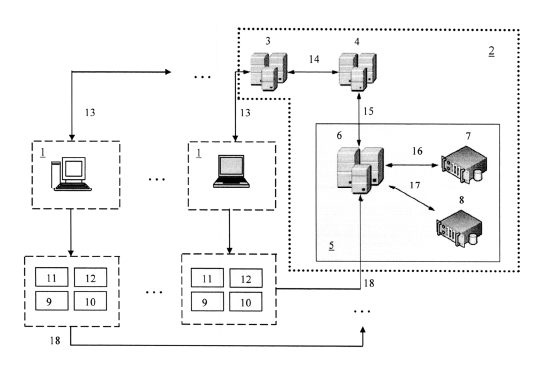
Изучить виды, содержание и порядок проведения патентных исследований.

**Задание 2**

В результате проведения исследовательских и проектно-конструкторских работ на промышленных предприятиях были разработаны методы испытания материалов. Для реализации этих методов предложены конструктивные решения приборов и приспособлений. В результате модернизации и совершенствования технологических процессов были предложены решения, позволяющие повысить качество и производительность выпускаемой продукции. Предполагается патентование разработок.

Необходимо выполнить экспертизу патентной чистоты разработанных конструктивных решений: методов испытания материалов и устройств для их осуществления; устройств и механизмов для реализации технологических процессов, представленном на *рисунке 1*, в соответствии со своим вариантом.

**Вариант 5**



# Рис. *1* – Разработана интерактивная игровая система

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

* объект – *интерактивная игровая система;*
* страна поиска – *Республика Беларусь*;
* источники информации – *патентные*;
* ретроспективность –*10 лет*;

Информационная база - *сайт национального центра интеллектуальной собственности:* [http://www.belgospatent.org.by](http://www.belgospatent.org.by/)

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

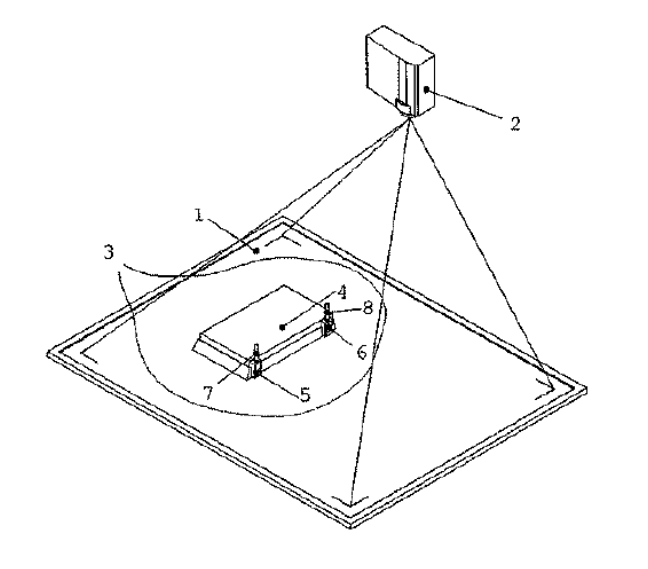


Рис. *2* – Интерактивная система сканирования, ввода и визуального отображения графических изображений

# 

Рис. *3* – Система игровая

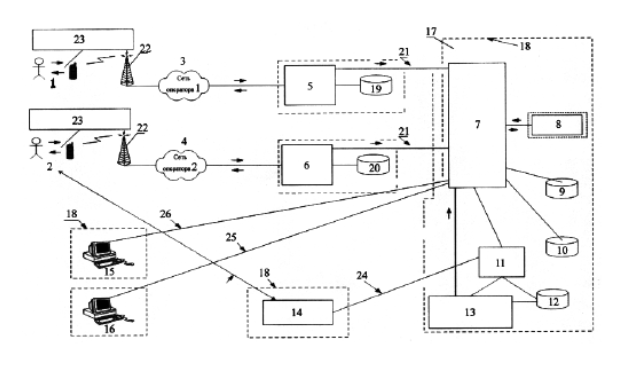


Рис. *4* – Система игровая лотерейная

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 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) |
| Интерактивная игровая система | Патент РБ № U 10699  МПК G 06F 3/033 | Государственное научное учреждение «Объединенный институт проблем информатики Национальной академии наук Беларуси» (BY), заявка № u 20140478 от 30.12.2014, опубл. 30.06.2015 | «Интерактивная система сканирования, ввода и визуального отображения графических изображений» | Действует |
| Патент РБ № U 1931  МПК A 63F 3/00 | Григорцевич Андрей Станиславович; Мамоненко Игорь Викторович; Колтович Юрий Николаевич; Парчинский Игорь Анатольевич (BY), заявка № u 20040474 от 22.10.2004, опубл. 30.06.2005 | «Система игровая» | Действует |
| Патент РБ № U 1741  МПК A 63F 3/00 | Григорцевич Андрей Станиславович; Мамоненко Игорь Викторович; Колтович Юрий Николаевич; Парчинский Игорь Анатольевич (BY), заявка №  u 20040297 от 18.06.2004,  опубл. 30.12.2004 | «Система игровая лотерейная» | Действует |

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

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

# **Практическое занятие №12**

**Тема** «Патентный поиск»

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

**Теоретические сведения**

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

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

**Задание**

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

* объект – *спортивный тренажер;;*
* страна поиска – *Республика Беларусь*;
* источники информации – *патентные*;
* ретроспективность –*10 лет*;

Информационная база - *сайт национального центра интеллектуальной собственности:* [http://www.belgospatent.org.by](http://www.belgospatent.org.by/)

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

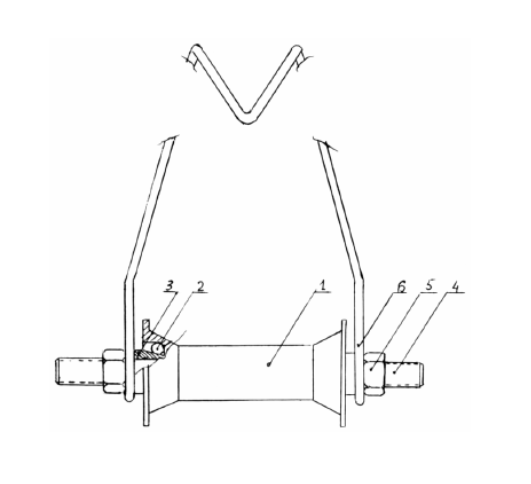


Рис. *1* – Портативный спортивно-оздоровительный тренажер

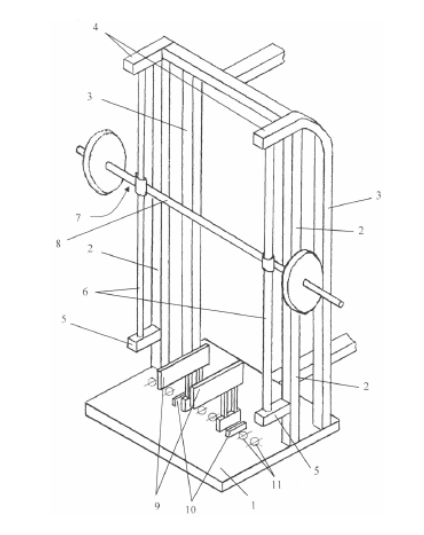


Рис. *2* – Устройство для тренировки и спортивный комплекс

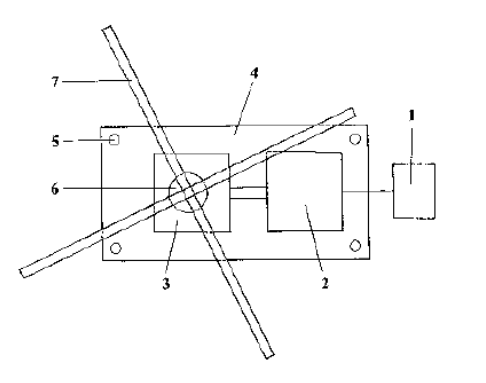


Рис. *3* – Устройство для тренировки мышц нижних конечностей

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 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) |
| Спортивные тренажеры | Патент РБ № U 9215  МПК А 63В 21/00 | Федотов Анатолий Яковлевич, Федотов Егор Сергеевич (BY), заявка № u 20120743 от 10.08.2012, опубл. 30.06.2013 | «Портативный спортивно-оздоровительный тренажер» | Действует |
| Патент РБ № U 9141  МПК А 63В 21/00  А 61В 17/00 | Куценко Геннадий Анатольевич, Линник Игорь Геннадьевич, Самсонович Татьяна Владимировна (BY), заявка № u 220120733 от 22.10.2004, опубл. 30.04.2013 | «Устройство для тренировки и спортивный комплекс» | Действует |
| Патент РБ № U 7594  МПК A 63В 23/04 | Кабанов Юрий Михайлович, Станский Николай Тимофеевич, Железнов Александр Васильевич, Трущенко Владимир Васильевич (BY), заявка №  u 20110188от 21.03.2011,  опубл. 30.10.2011 | «Устройство для тренировки мышц нижних конечностей » | Действует |

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

**Вывод:** освоила навыки проведения патентного поиска по заданной тематике.

# **Практическое занятие №13**

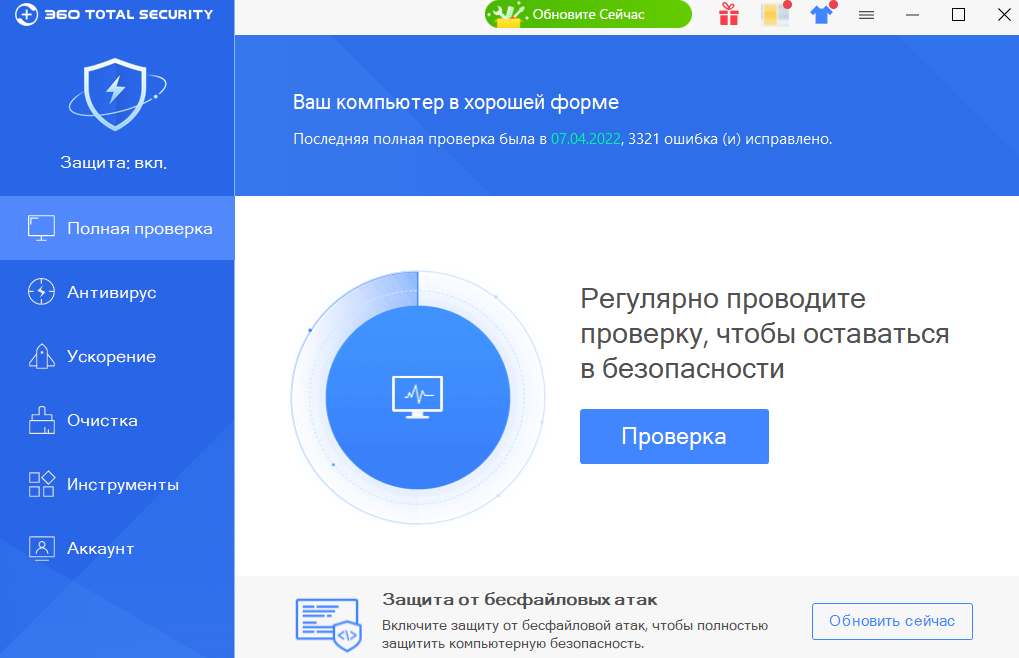
**Тема «Настройка антивирусов»**

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

**Задание**

1. Установить и настроить антивирусную программу по варианту.
2. Обновить базу данных сигнатур вирусов.
3. Выполнить сканирование дисков.

Рассмотрим антивирусное программное обеспечение 360 Total Security.



Рис*.1* – Главный экран

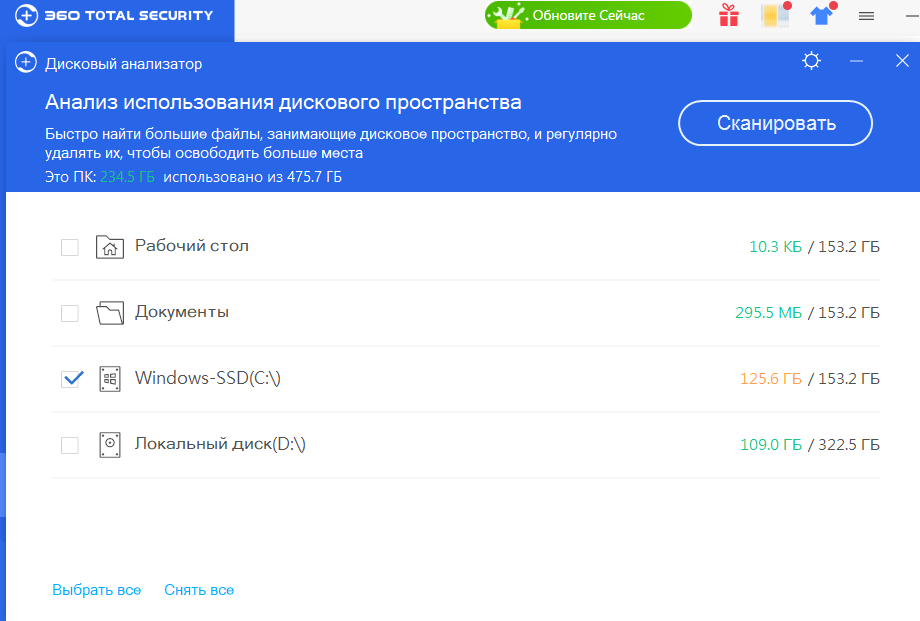
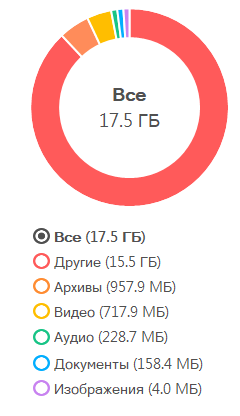


Рис.*2* – Сканирование дисков



Рис*.3* – Результат сканирования диска С

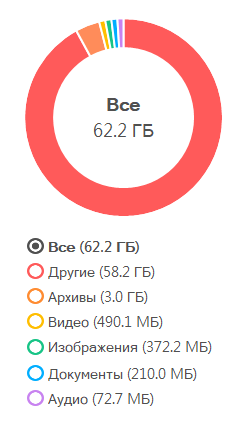


Рис.*4* – Результат сканирования диска D

**Вывод**: освоила навыки проведения патентного поиска по заданной тематике.

# **Практическое занятие №14**

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

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

**Ответить на следующие вопросы:**

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

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

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

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

· с конечным ключом;

· на основе генератора псевдослучайных чисел.

2. Блочные:

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

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

· моноалфавитные (Код Цезаря);

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

Шифр Трисемуса, Плейфера, Вижинера, Магический квадрат

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

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

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

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

Асимметричные (с открытым ключом, public-key):

· Диффи-Хеллман DH (Diffie, Hellman);

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

· Эль-Гамаль (ElGamal).

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

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

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

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

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

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

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

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

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

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

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

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

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