Учреждение образования

«Белорусский Государственный Технологический Университет»

Факультет информационных технологий

Кафедра информационных систем и технологий

Основы защиты информации

Студент: Сураго Дмитрий Александрович

ФИТ 2 курс 5 группа

Преподаватель: Берников Владислав Олегович

Минск 2020

**Практическое занятие №1**

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

Цель: Изучить концепцию национальной безопасности РБ.

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

Основными национальными интересами в информационной сфере являются:

* 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.

Деструктивное информационное воздействие на личность, общество и государственные институты, наносящее ущерб национальным интересам;

Нарушение функционирования критически важных объектов информатизации;

В информационной сфере внутренними источниками угроз национальной безопасности являются:

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

В информационной сфере внешними источниками угроз национальной безопасности являются:

* открытость и уязвимость информационного пространства Республики Беларусь от внешнего воздействия;
* доминирование ведущих зарубежных государств в мировом информационном пространстве, монополизация ключевых сегментов информационных рынков зарубежными информационными структурами;
* информационная деятельность зарубежных государств, международных и иных организаций, отдельных лиц, наносящая ущерб национальным интересам Республики Беларусь, целенаправленное формирование информационных поводов для ее дискредитации;
* нарастание информационного противоборства между ведущими мировыми центрами силы, подготовка и ведение зарубежными государствами борьбы в информационном пространстве;
* развитие технологий манипулирования информацией;
* препятствование распространению национального контента Республики Беларусь за рубежом 22;
* 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.

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 удаленного, 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.

Нейтрализации ряда внутренних источников угроз национальной безопасности способствует информационное обеспечение государственной политики, которое заключается в доведении до граждан Республики Беларусь и внешней аудитории объективной информации о государственном курсе во всех сферах жизнедеятельности общества, официальной позиции по общественно значимым событиям внутри страны и за рубежом, о деятельности государственных органов. Важной задачей при этом является расширение каналов и повышение качества информирования зарубежной общественности. Составной частью информационного обеспечения государственной политики выступает информационное противоборство, представляющее собой комплексное использование информационных, технических и иных методов, способов и средств для воздействия на информационную сферу с целью достижения политических, экономических и иных задач либо защиты собственного информационного пространства.

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:в данной работе мыизучили концепцию национальной безопасности РБ. Получили множественные знания в теории безопасности. Провели работу над заранее подготовленным текстом.

**Практическое занятие №2**

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

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

* законодательные (правовые);
* организационные;
* технические;
* комплексные.

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

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

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

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

Пусть имеется информационный объект, который при нормальном (идеальном) функционировании создает положительный эффект (экономический, политический, технический и т.д.). Этот эффект обозначим через *Е*0. Несанкционированный доступ к объекту уменьшает полезный эффект от его функционирования (нарушается нормальная работа, наносится ущерб из-за утечки информации и т.д.) на величину *ΔЕ*. Тогда эффективность функционирования объекта с учетом воздействия несанкционированного доступа:

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

Относительная эффективность:

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

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

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

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

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

где К≥1.

Выражения (2.2) и (2.4) примут вид:

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

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

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

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

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

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

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

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

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

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

или

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

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

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

**Задание на выполнение**

Решить задачу разработки средств защиты для обеспечения максимальной эффективности объекта в условиях несанкционированного доступа в соответствии с вариантом, используя таблицу 2.1.

Таблица 2.1 – Исходные данные

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № варианта | *E*0 | *E* | *K* | *C* |
| 3 | 20000 | 18000 | 10 | 1000 |

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

Несанкционированный доступ к объекту уменьшает полезный эффект от его функционирования (нарушается нормальная работа, наносится ущерб из-за утечки информации и т.д.) на величину *ΔЕ*. Тогда эффективность функционирования объекта с учетом воздействия несанкционированного доступа высчитаем по формуле (2.1):



Относительная эффективность в соответствии с формулой (2.2):



Уменьшение эффективности функционирования объекта приводит к материальному ущербу для владельца объекта. Тогда снижение эффективности функциональности объекта при наличии средств защиты равно в соответствии с формулой (2.4):



Выражение для эффективности и относительной эффективности, применяя формулы (2.5) и (2.6) соответственно, примут вид:





Если эффективность функционирования объекта имеет стоимостное выражение (доход, прибыль и т.д.), то UΣ непосредственно изменяет эффективность в соответствии с формулой (2.9):



**Вывод:** я научился решать задачи разработки средств защиты для обеспечения максимальной эффективности объекта в условиях несанкционированного доступа. Это нужно для того, чтобы обеспечить безопасность данных с минимальными затратами и добиться эффективности защитного ПО. Получили, что,  следовательно, эта защита будет неэффективна.

**Практическое занятие №3**

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

# Введение

Основой мер административного уровня,то есть мер, предпринимаемых руководством организации, является политика безопасности. Под политикой безопасностипонимается совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов. Политика безопасности определяет стратегию организации в области информационной безопасности, а также ту меру внимания и количество ресурсов, которую руководство считает целесообразным выделить. Положения о политике информационной безопасности чаще всего в виде отдельного документа появляются во исполнение требования регулятора – организации, регламентирующей правила работы юридических лиц в той или иной отрасли. Если положения об информационной безопасности нет, то не исключены определенные репрессии в отношении нарушителя, которые могут вылиться даже в приостановку деятельности последнего. Также политика безопасности является обязательной составляющей определенных стандартов (местных или международных). Необходимо соответствие конкретным требованиям, которые обычно выдвигают внешние аудиторы, изучающие деятельность организации. Отсутствие политики безопасности порождает отрицательные отклики, а подобные оценки негативно влияют на такие показатели, как рейтинг, уровень надежности, инвестиционная привлекательность и т. д. Обеспечение информационной безопасности – необходимое условие для успешного осуществления уставной деятельности Учреждения. Обеспечение информационной безопасности включает в себя любую деятельность, направленную на защиту информационных ресурсов и/или поддерживающей инфраструктуры. Политика охватывает все автоматизированные и телекоммуникационные системы, владельцем и пользователем которых является Учреждение. Реализация Политики должна исходить из предпосылки, что невозможно обеспечить требуемый уровень защищённости информационных ресурсов не только с помощью отдельного средства, но и с помощью их простой совокупности. Необходимо их системное, согласованное между собой применение, а отдельные разрабатываемые элементы информационной системы должны рассматриваться как часть единой информационной системы в защищённом исполнении при оптимальном соотношении технических и организационных мероприятий.

# Обозначения и сокращения

В данной работе приведены термины и сокращения:

АРМ – автоматизированное рабочее место;

АСУ ТП – автоматизированная система управления технологическими процессами;

ИБ – информационная безопасность;

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

ЛВС – локальная вычислительная сеть;

ОС – операционная система;

ПО – программное обеспечение;

СУБД – система управления базами данных;

ТЗ – техническое задание.

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

Комплекс средств автоматизации включает:

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

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

Объектами защиты автоматизированной системы управления технологическими процессами являются:

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

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

– АРМ операторов и специалистов;

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

– каналы передачи данных;

– ПО;

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

# Структура предприятия

Для того чтобы разработать план по информационной безопасности СЗАО "БЕЛДЖИ" нужно сначала понять, что из себя представляет его структура информации. Информация представляется в бумажном и электронном виде.

Так как в СЗАО "БЕЛДЖИ" храниться большая и важная документация, то доступ к информации имеется в зависимости от прав работника. Права работника назначаются в зависимости от должности.

Если это электронный носитель, то существует определенная группа, которую можно назвать администраторами. Администраторы могут вносить какие-либо изменения, поправки. Но также существует группа обычных пользователей, которые могут только просматривать эту информацию. Так как важность документов очень велика, то доступ ко всей информации не может быть скопирован ни одним из уровней пользования. Такая же система и с бумажными вариантами документации, которая храниться в архиве.

Политики информационной безопасности

По мнению специалистов по информационной безопасности компании Cisco, отсутствие сетевой политики безопасности может привести к серьезным инцидентам. Ее разработку рекомендуется начинать с оценки рисков сети и создания рабочей группы по реагированию на инциденты.

В компании Cisco рекомендуют создавать политики использования, которые описывают роли и обязанности сотрудников компании для надлежащей защиты корпоративной конфиденциальной информации. Начать можно с разработки главной политики безопасности, в которой четко нужно прописать общие цели и задачи организации режима информационной безопасности компании.

Следующий шаг – создание политики допустимого использования для партнеров, чтобы проинформировать их о доступной им информации. При этом следует четко изложить любые действия, которые будут восприниматься как враждебные, а также описать возможные способы реагирования при обнаружении таких действий.

В заключение необходимо создать политику допустимого использования для администраторов, где будут описаны процедуры администрирования учетных записей сотрудников, внедрения политики и проверки привилегий. Также, если в компании существуют определенные политики использования паролей или категорирования информации, они должны быть здесь упомянуты. Далее необходимо проверить названные политики на непротиворечивость и полноту, а также убедиться в том, что сформулированные требования к администраторам нашли свое отображение в планах по обучению.

Определение уровней рисков и типов доступа, требуемых для каждой сети, позволяет сформировать некоторую матрицу безопасности. Эта матрица безопасности является стартовой точкой для дальнейших шагов по обеспечению безопасности, например, таких, как создание соответствующей стратегии по ограничению доступа к сетевым ресурсам.

# Оценка рисков

Стратегический анализ и планирование деятельности предприятия, отрасли и любой экономической системы необходимы для определения факторов достижения стратегической цели, ответа на вопрос «как достичь желаемого состояния?», а также учета факторов риска, которые могут поставленным целям препятствовать. Стратегическое планирование должно осуществляться с учетом воздействия внешней среды, для которой свойственны различного рода резкие изменения: конъюнктуры рынка, количества и влияния на рынок конкурентов, уровня насыщения рынков сбыта, появление новых товаров, изменения политической ситуации в стране, платежеспособности клиентов экономической системы и т.п. Эти колебания создают высокую степень неопределенности для предприятия при принятии решений. Также необходимо анализировать сильные и слабые стороны самой организации при постановке тех или иных задач стратегического развития, поскольку при определенных обстоятельствах сильные стороны могут стать слабыми (и наоборот). Следовательно, необходимо отдельно анализировать внутренние и внешние риски организации с учетом поставленной стратегической цели. Анализ и оценка рисков, а также сильных сторон организации и возможностей внешней среды должны обязательно учитываться при разработке плана стратегического развития.

Угрозы информационной безопасности могут быть классифицированы по различным признакам:

– по аспекту информационной безопасности, на который направлены угрозы:

а)угрозы конфиденциальности (неправомерный доступ к информации);

б) угрозы целостности (неправомерное изменение данных);

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

– по степени преднамеренности действий:

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

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

– по расположению источника угроз:

а) внутренние (источники угроз располагаются внутри системы);

б) внешние (источники угроз находятся вне системы);

– по размерам наносимого ущерба:

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

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

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

– по степени воздействия на информационную систему:

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

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

Основными угрозами ИБ АСУ ТП являются:

– несанкционированное вмешательство в управление технологическими процессами;

– нарушение функционирования АСУ ТП или ее отдельных элементов;

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

В результате реализации угроз ИБ могут быть нарушены:

– целостность (утрата, уничтожение, модификация) информации;

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

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

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

Таблица 1. Внутренние риски предприятия СЗАО "БЕЛДЖИ"

|  |  |  |
| --- | --- | --- |
| № п/п | Факторы | Внутренние риски |
| 1 | 2 | 3 |
| 1 | Производство | Проблемы с производственной кооперацией: неготовность предприятий к участию в кооперации; необходимость доработки заказов, сделанных по кооперации; наличие убыточных предприятий в кооперации.  Дисбаланс между показателем объема продукции, изготовляемой по кооперации, и объемом, выполняемым собственными силами |
| Невозможность в полном объеме и в заданные сроки выполнить ГОЗ |
| Нерациональное использование производственных мощностей; неэффективное использование оборудования; неполная загруженность производственных мощностей |
| Ограниченность производственных мощностей и их несоответствие планируемым объемам производства |
| Потери рабочего времени; недостатки в нормировании производственных процессов; необеспеченность сырьем и материалами; неэффективная работа вспомогательных служб |
| Слабая обновляемость производственных фондов |
| Необходимость роста производственных мощностей для разработки новых изделий техники и освоения ранее разработанной |
| 2 | Управление | Необходимость поиска новых подходов к управлению в ситуации, обусловленной ростом объемов работ и недостаточной готовностью предприятий, участвующих в кооперации, к решению поставленных перед предприятием задач |
| Необходима проработка вопроса создания интегрированной структуры управления, включающей ведущие НИИ и производственные предприятия |
| Недостатки в организационной структуре предприятия; недостатки оперативного планирования, стратегического менеджмента и прогнозирования; неверный выбор методов управления |
| Риски, связанные с реструктуризацией предприятия для совершенствования системы управления |
| Не совершенны организационная, юридическая, информационная базы, регулирующие процессы взаимодействия предприятия с заказывающими и выполняющими работы структурами |
| 3 | Техника и технология | Нарушение правил эксплуатации техники, моральный и физический износ оборудования; недостаточная надежность оборудования; нарушение сроков эксплуатации |
| Неверный способ технологической подготовки производства; использование непрогрессивных технологических процессов; использование неэффективных технологий; низкий уровень технологов; отсутствие программного обеспечения |
| Высокие затраты для перехода на новые технологии и оборудование |
| 4 | Рыночные показатели | Длительный производственно-финансовый цикл |
| Узкий ассортимент продукции |
| Сбои в снабжении |
| Отсутствие службы маркетинга; недостаточное определение спроса на выпускаемую продукцию; недостоверное определение доли рынка |
| Отсутствие рекламы |
| Достижение конкурентных преимуществ нерыночными способами. Нерыночные методы управления. Нерыночные способы реализации |
| Слабая политика продвижения товаров на рынок |
| Недостаток сведений о конкурентах; неверное позиционирование товаров |
| Отсутствие анализа информации о потребителях |
| 5 | Финансы | Повышение себестоимости |
| Снижение показателей рентабельности; недостаточная окупаемость капиталовложений. Низкая рентабельность работ, сделанных по кооперации |
| Задержки оплаты ГОЗ; неполучение требуемых запланированных кредитов. Затягивание процедур оплаты работ заказчиками |
| Снижение показателей ликвидности и финансовой устойчивости |
| Высокая дебиторская задолженность |
| 6 | Инновации | Недостаточная эффективность НИОКР; низкий вес наукоемкой продукции; малое/недостаточное количество патентов и лицензий |
| Недостаточное финансирование инновационной деятельности; трудность учета фактора времени при разработках; отсутствие исследовательской базы |
| Превышение объемов производства над объемами НИР |
| 7 | Персонал | Неучастие персонала в принятии управленческих решений. Низкая заинтересованность рядовых сотрудников в развитии предприятия |
| Большая зависимость от высококвалифицированных специалистов. Нехватка квалифицированных специалистов для выполнения заказов (особенно в научно-исследовательской сфере и области инноваций) |

Таблица 2. Внешние риски предприятия СЗАО "БЕЛДЖИ"

|  |  |  |
| --- | --- | --- |
| № п/п | Факторы | Внешние риски |
| 1 | 2 | 3 |
| 1 | Экономические | Макроэкономическая нестабильность; значительный рост инфляции; нерациональная налоговая политика; резкое изменение курса валют |
| Риск нарушения законодательства в сфере налогообложения |
| Рост затрат, связанных с гонкой вооружений |
| Секвестр бюджетов федеральных целевых программ |
| Риски неверного прогнозирования макроэкономической ситуации и развития рынков |
| Риск нарушения условий бюджетного финансирования; прекращение государственных гарантий; нарушение финансирования госзаказа; срывы сроков финансирования ГОЗ |
| Неготовность предприятия СЗАО "БЕЛДЖИ" к освоению возрастающих объемов производства (срыв работ по кооперации) |
| Нерациональная политика ценообразования в сфере ОПК |
| Снижение реальных доходов населения; снижение уровня жизни населения; снижение макроэкономических показателей страны; неконкурентоспособность отраслей экономики |
| Возможные процедуры банкротства; повышение тарифов; приостановление деятельности предприятия или его подразделений |
| 2 | Международные | Негативное изменение законодательства стран ‒ заказчиков продукции предприятия. Изменение международных стандартов; запрет на ввозимую продукцию, сырье, материалы. Резкое ухудшение экономического состояния зарубежных заказчиков |
| Неблагоприятные значительные изменения ценовой политики зарубежных стран потребителей |
| Срыв заключенных ранее международных договоров |
| Появление иностранных конкурентов с товарами, обладающими высокими техническими характеристиками |
| Переориентация зарубежных заказчиков на других исполнителей заказов. Снижение объемов поставляемых изделий в другие страны |
| Возникновение международных конфликтов, оказывающих негативное влияние на выполнение заключенных договоров |
| Неблагоприятные изменения политической ситуации в странах, с которыми заключены договоры. Нарушение стабильности в регионах за рубежом, препятствующее экспорту |
| 3 | Научно-технические | Снижение уровня государственной поддержки развития науки |
| Появление на рынке альтернативных товаров вследствие научно-технической революции |
| Риск морального устаревания производимой продукции |
|  |  | Значительное повышение уровня научных разработок за рубежом |
|  |  | Существенное повышение требований заказчиков к техническому уровню в системах вооружения и военной техники |
|  |  | Отсутствие или недостаточное целевое финансирование минобороны НИОКР, производства новых изделий и проведения испытаний |
| Ухудшение ситуации с отечественной элементной базой |
| Риск эффективности инновационной деятельности |
| 4 | Конкуренции | Возникновение на рынке новых конкурентов в нашей стране и за рубежом |
| Повышение качества и снижение цены продукции, предлагаемой конкурентами |
| Недобросовестная конкуренция при участии в конкурсах на выполнение НИОКР по ГОЗ. Недобросовестный конкурсный отбор проектов |
| Повышение барьеров входа на рынок |
| Частичная или полная потеря рынка |
| 5 | Спроса | Значительное уменьшение ёмкости рынка |
| Снижение уровня ГОЗ |
| Нарушение сроков выполнения ГОЗ, приводящее к снижению спроса на продукцию предприятия |
| Отсутствие стабильности спроса |
| 6 | Сбыта и поставки продукции | Наличие недобросовестных предприятий-посредников; повышение цен; поставка сырья и материалов несоответствующего качества |
| Недостатки современных информационно-коммуникационных технологий, используемых при сбыте продукции |
| Недостаточная развитость систем выбора поставщиков |
| Изменение правил торговли В и ВТ |
| Риски неисполнения контрактных обязательств; срыв поставок; невозвращение предоплаты |
| 7 | Политические и правовые | Политическая нестабильность в стране и в странах, в которые поставляется продукция предприятия |
| Риск коррумпированности властных структур, имеющих отношение к хозяйственной деятельности предприятия |
| Недостаточная разработанность законодательных и правовых актов, относящихся к предприятиям, имеющим стратегическое значение |
| Слабая реализация законов и решений правительства, относящихся к оборонной тематике |
| Превалирование политики над экономикой при решении задач, имеющих государственную значимость |
| Риск появления новых законодательных ограничений |
| Риск национализации бизнеса, передела собственности |
| 8 | Социально-демографические | Неблагоприятная демографическая ситуация |
| Значительный «отток» высококвалифицированных кадров в зарубежные страны; |
| Низкий уровень оплаты труда на предприятии СЗАО "БЕЛДЖИ" |
| Недостаточное материальное/моральное стимулирование работников |
| 9 | Природные и экологические | Риск, связанный с природными условиями |
| Риск повышения требований по охране окружающей среды |

# 

# Разработка мер защиты

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

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

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

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

Используемая антивирусная система защиты имеет:

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

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

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

– дополнительные механизмами для обнаружения новых неизвестных вредоносных программ;

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

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

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

– физической защитой сетевого оборудования и средств защиты;

– контролем логического доступа к сетевому оборудованию;

– шифрованием каналов управления;

– контролем сетевых соединений;

– обнаружением и предотвращением вторжений;

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

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

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

– применением средств мониторинга и регистрации событий.

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

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

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

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

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

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

# Заключение

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

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

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

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

**Практическое занятие №4**

Тема «Настройка Брандмауэра Windows »

Цель: Овладение навыками настройки и использования Брандмауэра Windows.

**Теоретическое введение**

Брандмауэр (Межсетевой экран) - это аппаратный или программный комплекс, позволяющий проверять (фильтровать) входные и выходные потоки данных, проходящие через интернет или сеть. В случаи нарушения политики безопасности компьютера, брандмауэр блокирует эти данные (рис. 1).

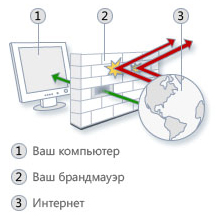


Рисунок 1 – Принцип действия Брандмауэра

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

К числу таких служб и протоколов относятся:

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

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

**Задания на выполнение**

Для создания правила по ограничению доступа программ к сети необходимо открыть Панель управления в меню Пуск. В зависимости от версии операционной системы Windows может отображаться классический вид панели управления или с разделениям по категориям.

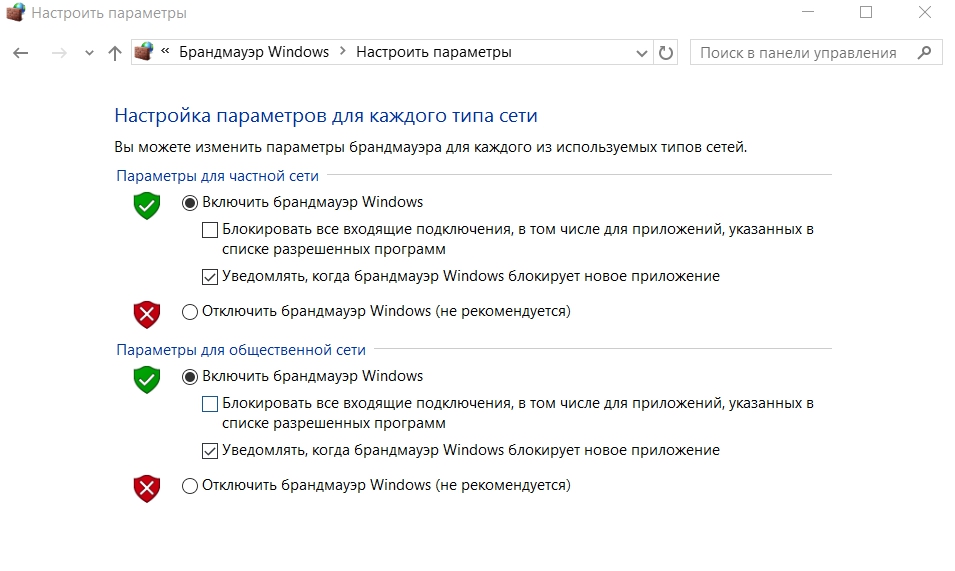


Рисунок 1 ­– Включение брандмауэра Windows

Первым этапом необходимо включить брандмауэр, в случае, если он был ранее выключен. Необходимо выбрать в левой панели управления вкладку «Включение и отключение брандмауэра Windows» (Рис.1)

Правила для входящих подключений:

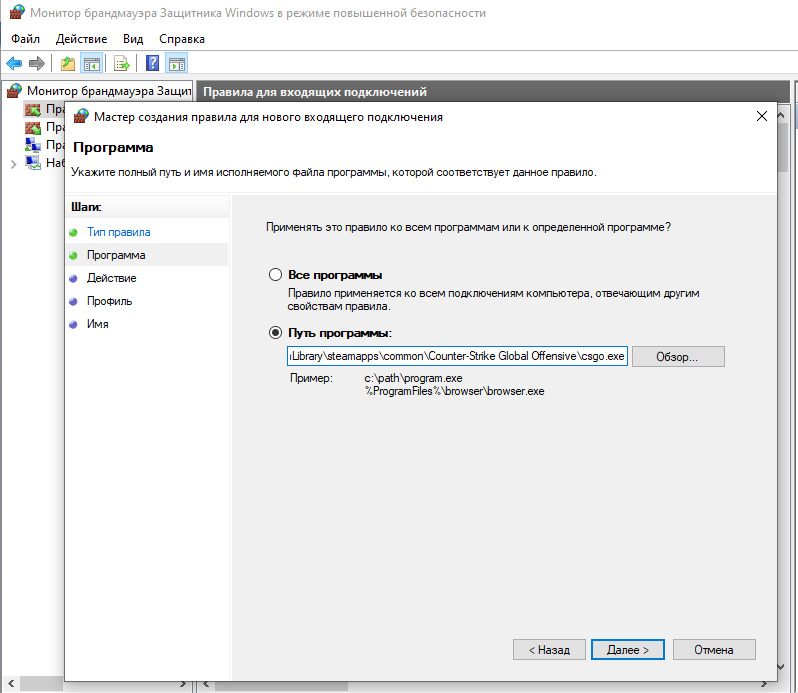


Рисунок 2 – Настройка пути программы

В открывшемся мастере создания правила выбираем «Для программы». При ограничении работы программы, далее необходимо указать её путь, обязательно через папку, в которой она установлена (Рис.2).

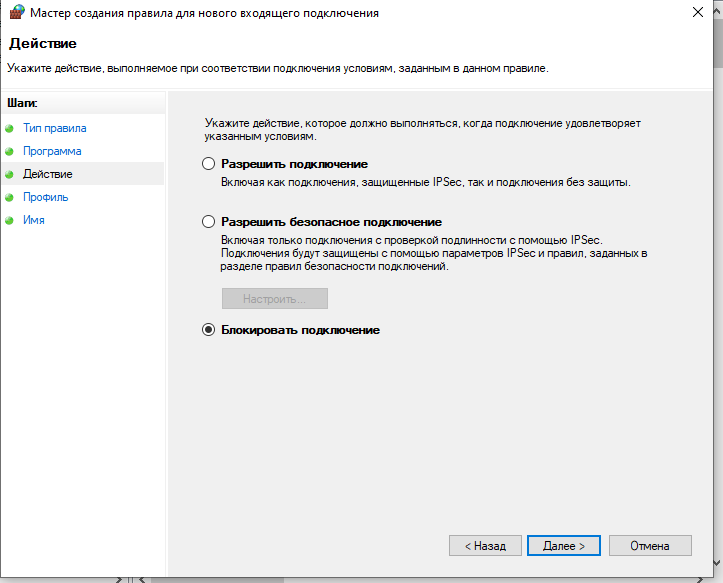


Рисунок 3 – Выбор действия

Указывается какое именно действие нужно применить. В данном случае необходимо блокировать подключение (Рис.3).

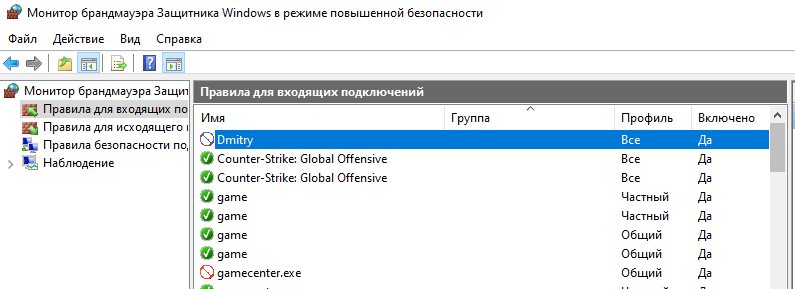
****

Рисунок 4 – Созданное правило

В общем списке появилось созданное правило. Правила можно отключать, копировать, удалять с помощью кнопок на правой панели (Рис.4).

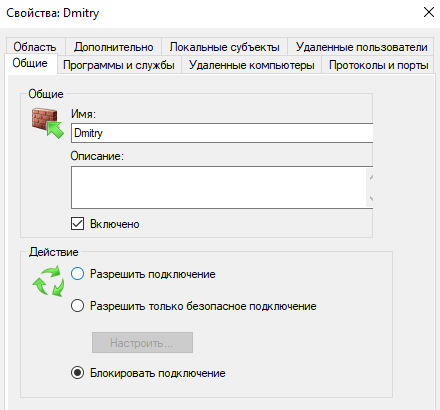


Рисунок 5 – Свойства правила

Проверяем свойства правила (Рис.5).

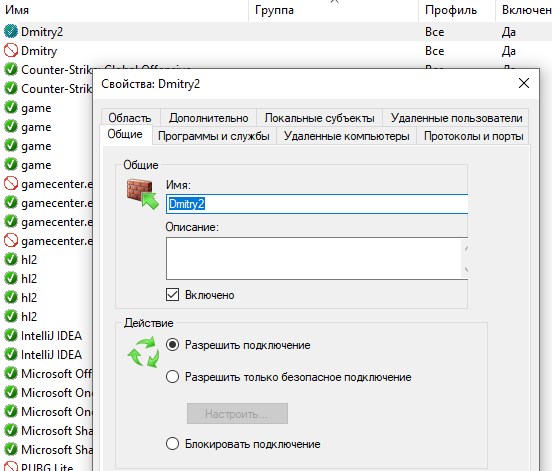
****

Рисунок 6 – Свойства правила

Делаем все то же самое, только разрешаем подключение. Проверяем свойства правила (Рис.6).

Правила для исходящих подключений:

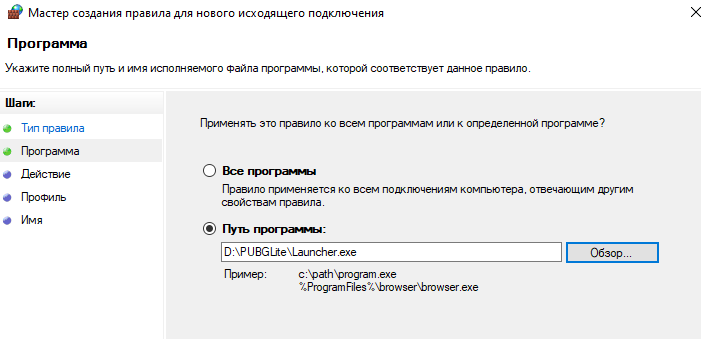


Рисунок 7 – Настройка пути программы

Устанавливаем путь программы, для которой устанавливаем правило исходящего подключения (Рис.7).

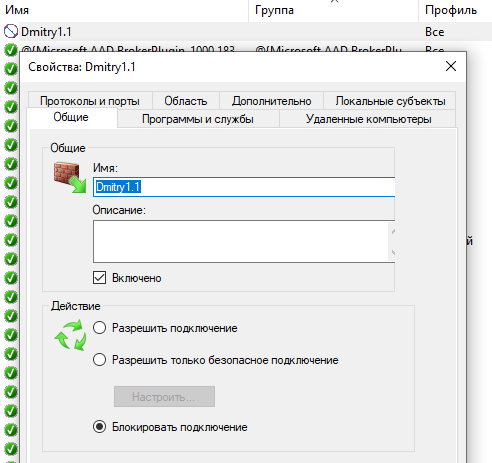


Рисунок 8 – Свойства правила

Проверяем созданное правило и его свойства (Рис.8).

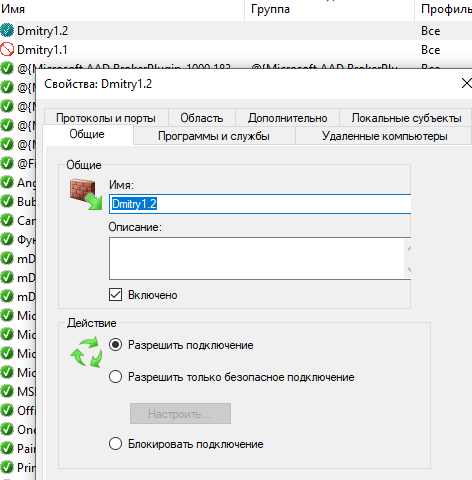


Рисунок 9 – Свойства правила

Делаем все то же самое, только разрешаем подключение. Проверяем свойства правила (Рис.9).

Проверка использования команды *control admintools* (Рис.10):

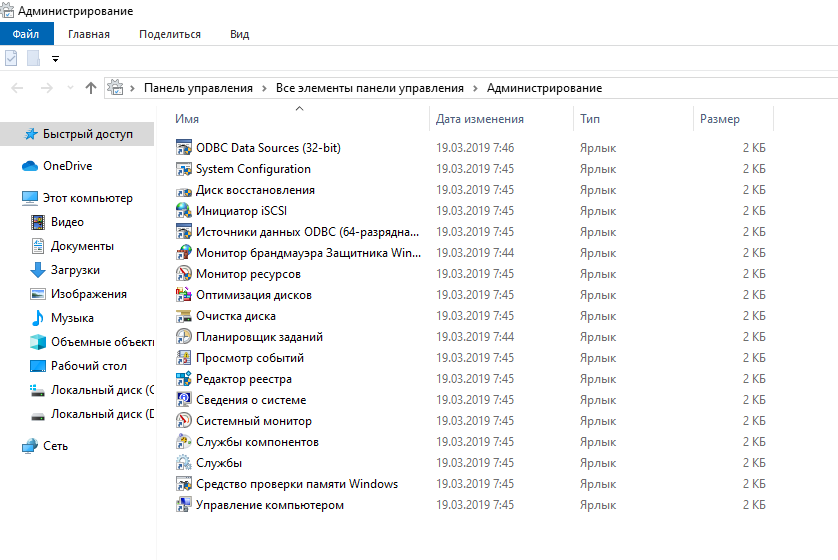


Рисунок 10 – control admintools

Проверка использования команды *cmd* (Рис.11):

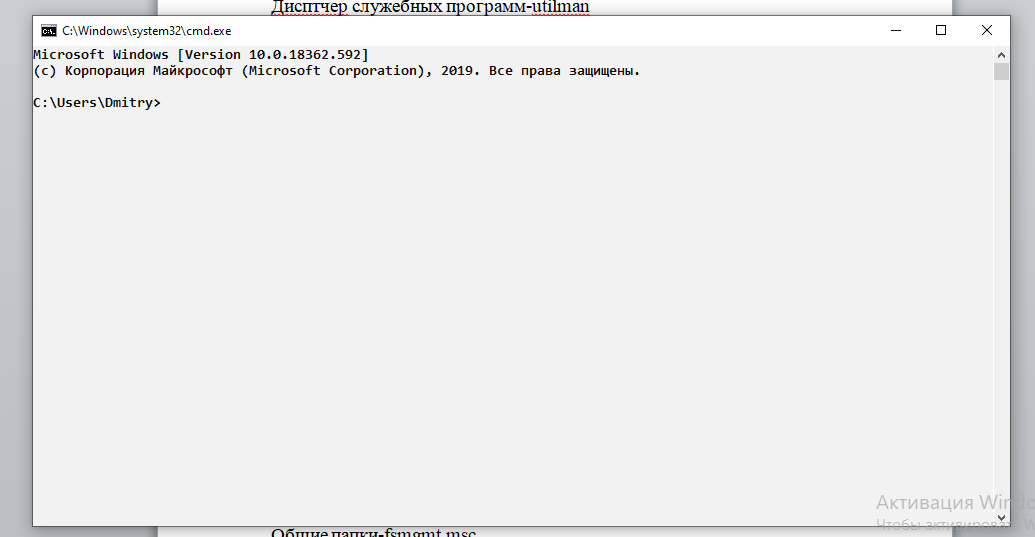


Рисунок 11 – cmd

Проверка использования команды *regedit* (Рис.12):

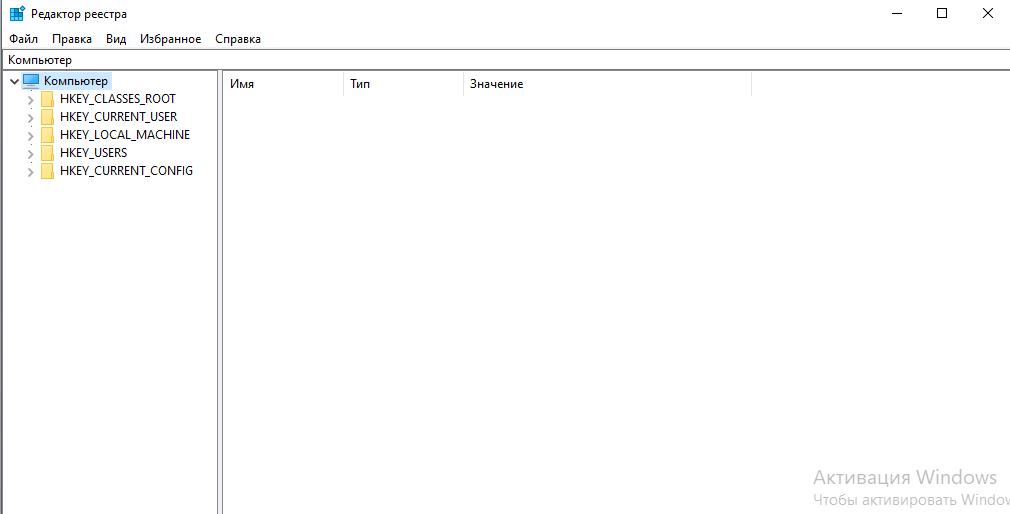


Рисунок 12 – regedit

**Вывод**: В ходе выполнения данной работы я изучил работу брандмауэра Windows, научился включать и отключать запреты на подключения для программ. Так же изучил команды, необходимые для работы администратора.

**Практическое занятие №5**

**Тема «Настройка антивирусов»**

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

Настройка режима фильтрации файервола антивируса:

Настройка режима фильтрации: переходим в левом окне в пункт персональный файервол, в поле Режим фильтрации выбираем один из пункт удовлетворяющий потребности пользователя, в данном случае Автоматический режим с исключениями.

Существуют и другие режимы:

**Автоматический режим**

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

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

**Интерактивный режим**

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

**Режим на основе политик**

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

Автоматический режим с исключениями

Данный режим позволяет настроить вручную правила. В этом случае, если будет запрос на соединение извне, файервол сначала проверит правила, которые прописал пользователь, и если найдет соответствующее, то оно будет задействовано. Если правила не будет, тогда соединение будет разорвано. Во всех остальных случаях этот режим полностью соответствует автоматическому режиму.

**Режим обучения**

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

**Ход работы:**

Открываем ESET NOD32 Smart Security. Открываем «Дополнительные настройки», нажав клавишу F5 на клавиатуре – «Файервол». Открылось окно расширенной настройки. В расположенном справа раскрывающемся меню «Режим фильтрации» выбираем нужный режим фильтрации (Рис. 13).

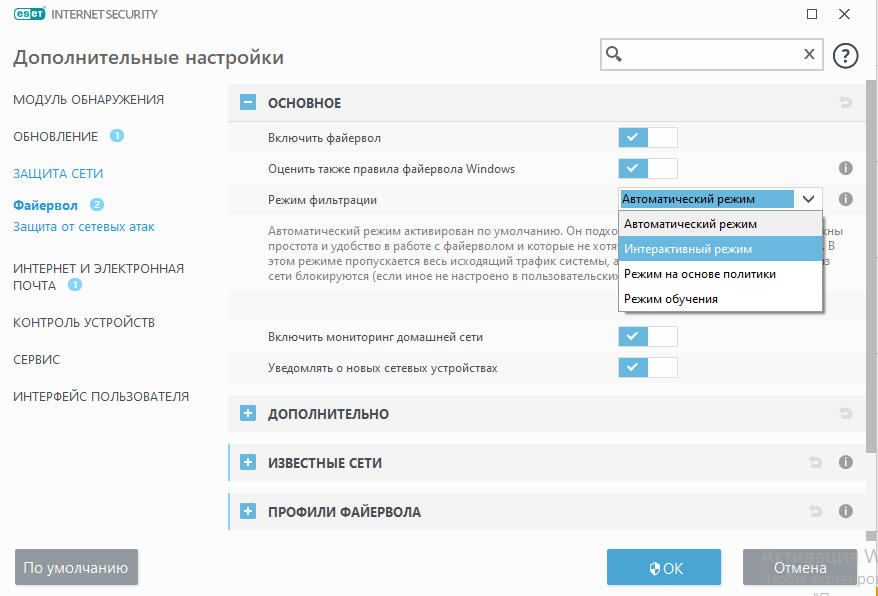


Рисунок 13 – Режим фильтрации

Обновление NOD32 – обновление сигнатур угроз из локальной папки:

Нажал F5 для управления настройками NOD32 и выбрал пункт «Обновление» (Рис. 14).

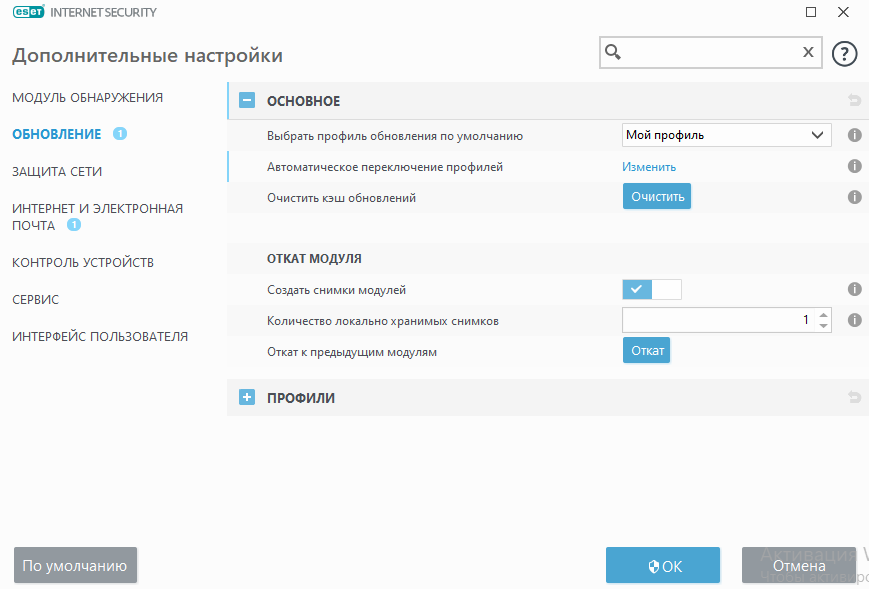


Рисунок 14 – Настройки обновления

Обновление без подключения к сети Интернет возможно только для пользователей версии 4.2 (рис.15).

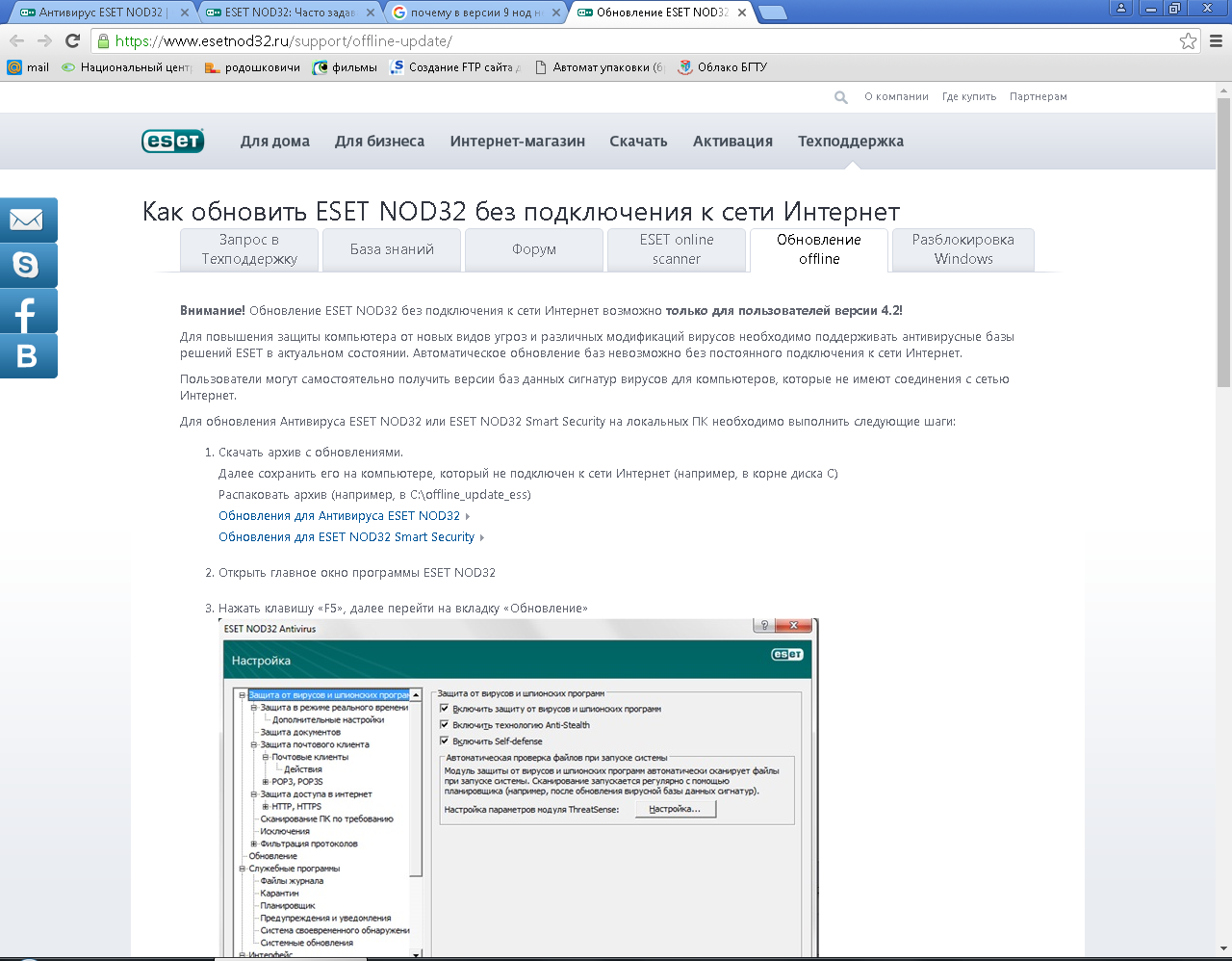


Рисунок 15 – Оффлайн обновление

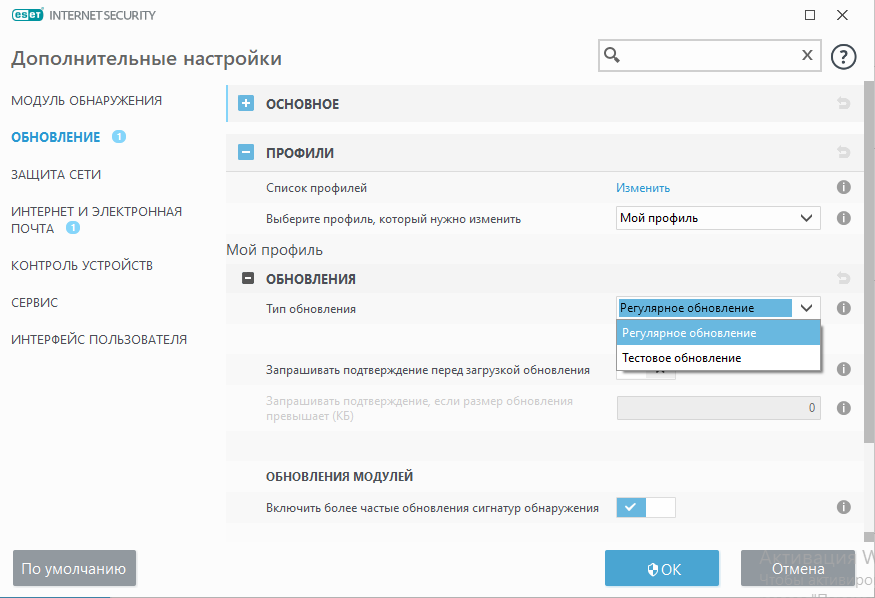


Рисунок 16 – Выбор типа обновления

Основные настройки – выбор типа и режима обновления (Рис. 16).

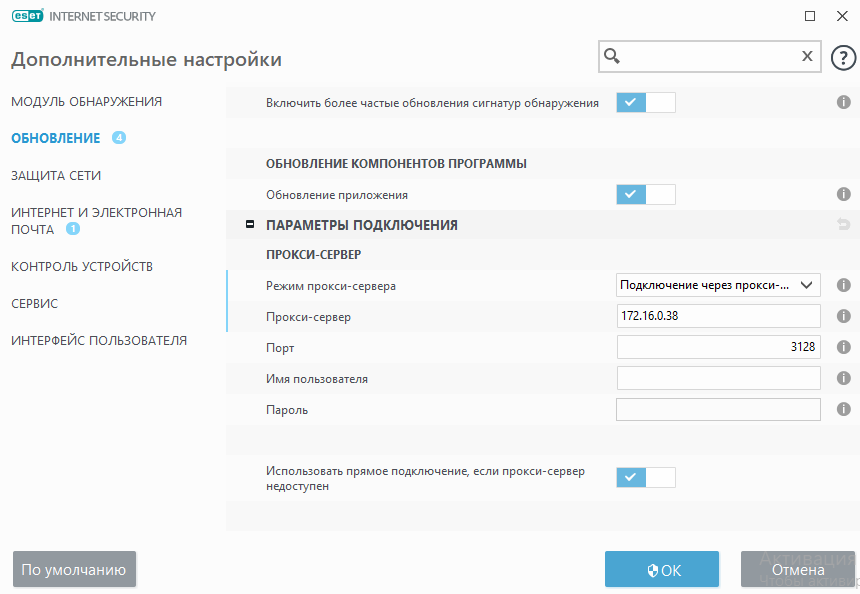


Рисунок 17 – Настройка прокси-сервера

Прокси-сервер HTTP (Рис. 17) Вводим необходимый адрес.

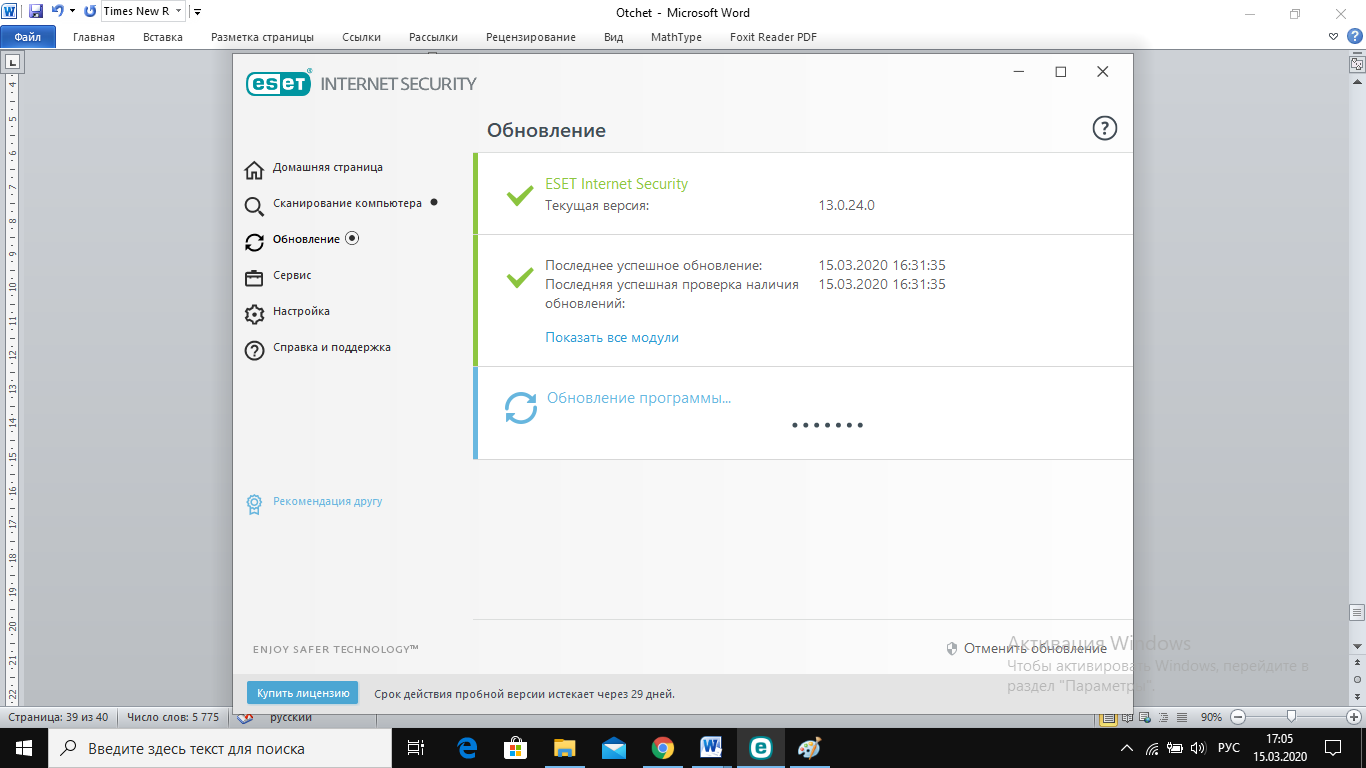


Рисунок 18 – Процесс обновления

**Вывод**: в ходе выполненной работы я научился обновлять антивирус. Настроил фаервол для безопасности персонального компьютера. В результате этого, можно обезопасить себя от несанкционированного использования личного компьютера программами и пользователями.

**Практическое занятие №6**

**Тема «Изучение принципов работы с компьютерными программами для криптографической защиты информации при передаче и хранении»**

**Цель:** Овладение навыками работы с компьютерными программами для криптографической защиты информации при передаче и хранении.

**Теоретическое введение**

С задачей подбора программного обеспечения для криптографической защиты данных сталкивается каждый, кто всерьез задумывается о безопасности своей конфиденциальной информации. И в этом нет абсолютно ничего удивительного - шифрование на сегодняшний день является одним из самых надежных способов предотвратить несанкционированный доступ к важным документам, базам данных, фотографиям и любым другим файлам.

Проблема заключается в том, что для грамотного выбора необходимо понимать все аспекты работы криптографических продуктов. В противном случае можно очень легко ошибиться и остановиться на ПО, которое либо не позволит защитить всю необходимую информацию, либо не обеспечит должной степени безопасности. На что же нужно обращать внимание? Во-первых, это доступные в продукте алгоритмы шифрования. Во-вторых, способы аутентификации владельцев информации. В-третьих, способы защиты информации. В-четвертых, дополнительные функции и возможности. В-пятых, авторитет и известность производителя, а также наличие у него сертификатов на разработку средств шифрования.

**Ход работы:**

Запустив программу, мы выбираем виртуальный диск, который хотим создать.

Далее, тут вам необходимо определится, какой раздел вы создадите: скрытый или обычный. Руководство покажет создания обычного раздела. Опция уже выставлена. Поэтому нажимаем «Next».

Этап предполагает указание места расположения раздела TrueCrypt. При этом поведение контейнера идентичное с поведением самого обыкновенного файла(рис. 6.1).

Жмем Select File. Открывается окошко для выбора файла.

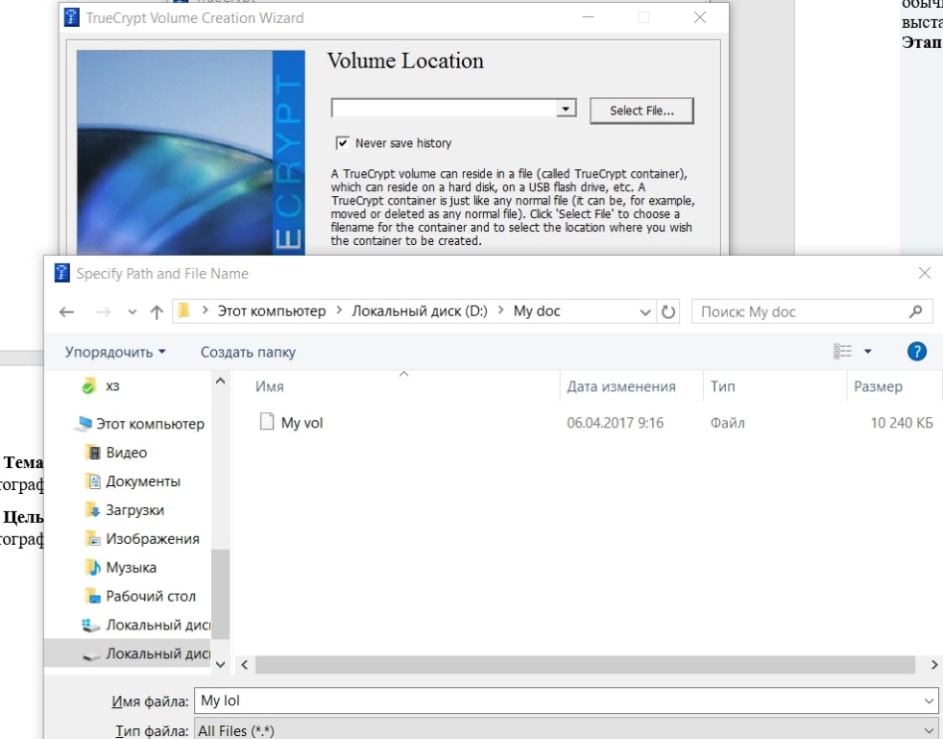


Рисунок 6.1 – Окно для выбора файла

В следующем разделе вам предлагается сделатиь выбор алгоритма для шифрования, а так же хеш – алгоритма предназначенного для раздела. Если вы не в состоянии что то выбрать, оставляем всё как есть и жмем  «Next»(рис. 6.2).

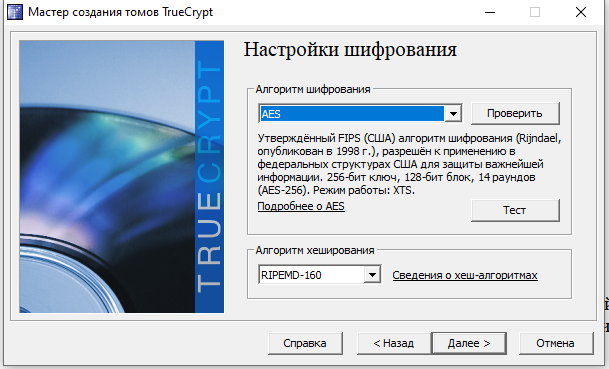


Рисунок 6.2 – Выбор алгоритма шифрования

Далее в окне мы указываем предполагаемый размер контейнера TrueCrypt в 1 мегабайт. Можно выбрать и другой размер, а затем нажимаем «Next»(рис. 6.3).

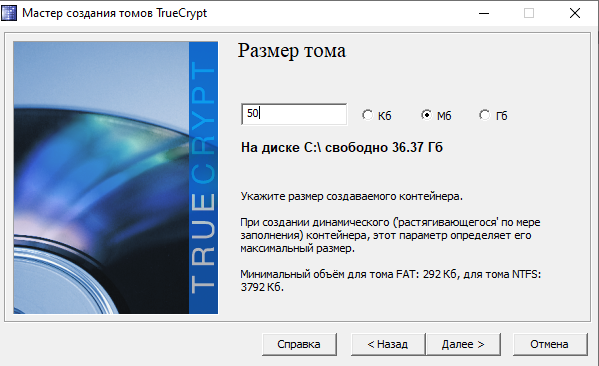


Рисунок 6.3 – Размер контейнера

Этот этап самый основной. Тут необходимо определится с паролем для раздела. Стоит ознакомится с информацией, которое дает определение качественного пароля.

После того как вы определитесь введите пароль в первое поле, а затем продублируйте его во второе и нажмите «Next»(рис. 6.4).

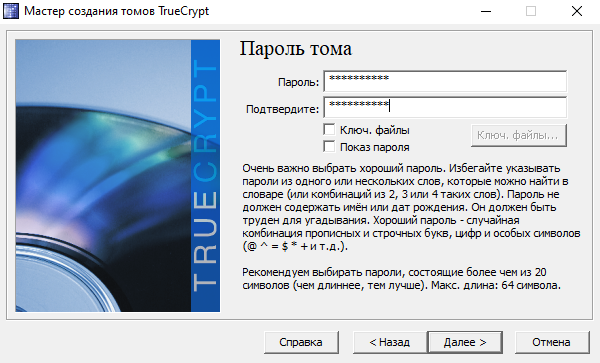


Рисунок 6.4 – Задание пароля

В открывшемся окне следует двигать мышкой в случайном порядке не менее 30 секунд. Чем дольше будет продолжаться процесс – тем лучше. Это повлияет на увеличение криптографических свойств ключей. Жмем Format. Далее начинается процесс создания раздела. На диске D:\My Documents\ появится файл My Volume. Он будет выступать контейнером в котором будет находится шифрованный раздел TrueCrypt. По окончанию вы увидите окно показанное ниже(рис. 6.5).

Жмем «ОК» для его закрепления.

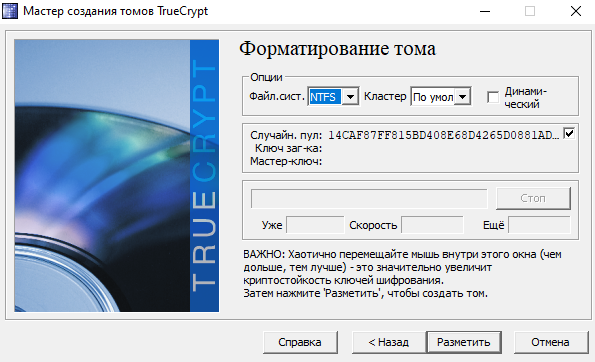


Рисунок 6.5 – Получение криптографических свойств ключа

Выбираем одну из букв представленных в списке, это будет буква диска к которому вы примонтируете ваш контейнер(рисю 6.6).

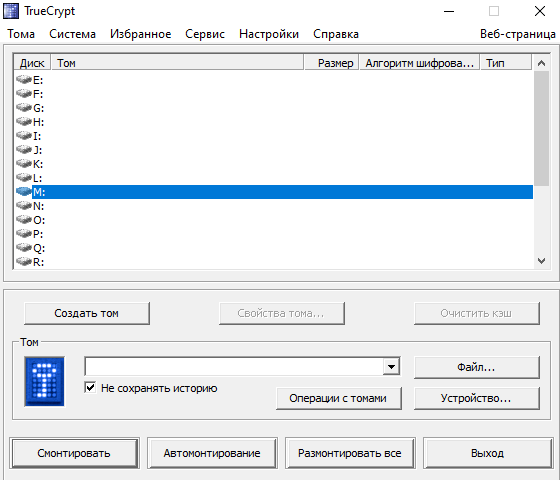


Рисунок 6.6 – Выбор диска

В оставшемся окошке TrueCrypt жмем Mount. Появляется окно, которое запрашивает ваш пароль.

Вводим пароль, который вы установили на 10 этапе в поле выделенное красным(рис. 6.7)

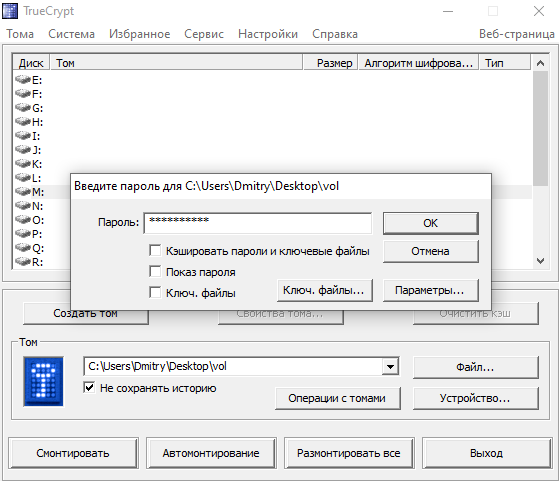


Рисунок 6.7 – Ввод пароля

Только что успешно прошла монтировка на один из виртуальных дисков. Диск полностью зашифрован и при этом ничем не отличается от прочих дисков. Вы можете помешать данные на данный диск и при этом они автоматически будут зашифровываться(рис. 6.8).

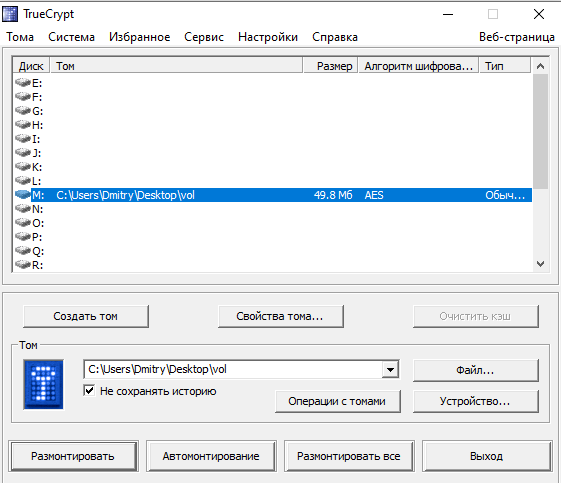


Рисунок 6.8 – Проверка

Проверяем, появился ли созданный диск у нас на компьютере (рис. 6.9)

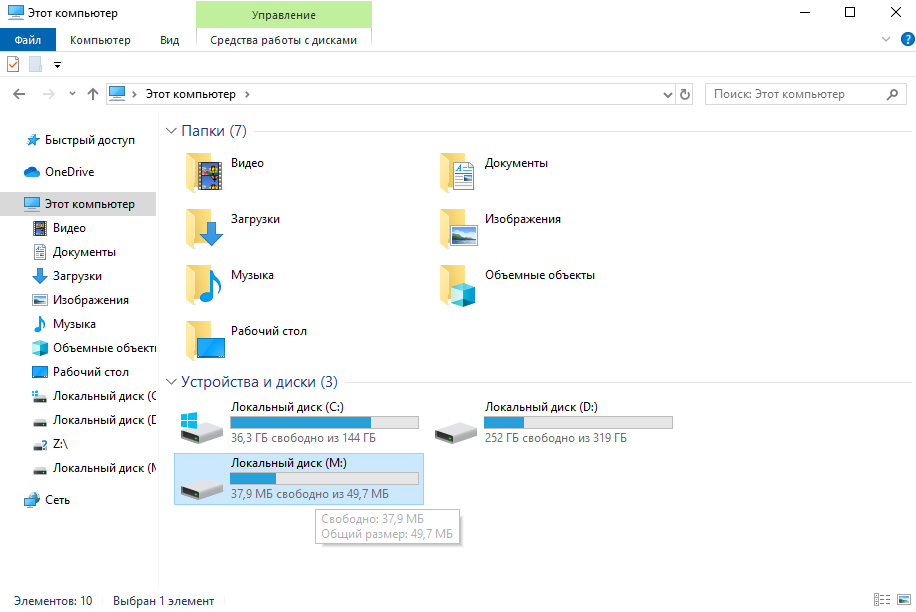


Рисунок 6.9 – Отображение на компьютере

**Вывод:** мы овладели навыками работы с компьютерными программами для криптографической защиты информации при передаче и хранении. Испытали всё на своём компьютере для закрепления навыков.

**Практическое занятие №7**

**Тема «Криптографическая защита информации»**

Цель: Овладение основными криптографическими алгоритмами шифрования.

**Теоретическое введение**

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

Шифрованием (encryption) называют процесс преобразования открытых данных (plaintext) в зашифрованные (шифртекст, ciphertext) или зашифрованных данных в открытые по определенным правилам с применением ключей.

В коде Цезаря буква заменяется на букву, отстоящую от нее в латинском алфавите на некоторое число позиций (рис. 7.1).



Рис. 7.1 – Пример кода Цезаря

Алгоритм Диффи-Хелмана (WhitfieldDiffie и MartinHellman, 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 = qxmod n

По получении А партнер P2 генерирует случайное число у и посылает P1 вычисленное значение B = qymod n

Партнер P1, получив В, вычисляет Kx = Bxmod n, а партнер P2 вычисляет Ky = Aymod 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, ч то 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.

**Практическая часть**

g = открытое простое число. g = 18

p = открытое простое число. p = 5

a = секретный ключ Человека1. a = 10

A = открытый ключ Человека1. A = gamod p = 4

b = секретный ключ Человека2. b = 7

B = открытый ключ Человека2. B = gbmod p = 2

s = секретный ключ.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Человек1 | | Человек2 | | Человек3 | | |
| Знает | Не знает | Знает | Не знает | | Знает | Не знает |
| p = 33 | b = ? | p = 33 | a = ? | | p = 33 | a = ? |
| g = 11 |  | g = 11 |  | | g = 11 | b = ? |
| a = 23 |  | b = 30 |  | |  | s = ? |
| A = 1123mod 33 = 11 |  | B = 1130mod 33 = 22 |  | | A = 1123mod 33 = 11 |  |
| B = 11bmod 33 = 22 |  | A = 11amod 33 = 11 |  | | B = 1130mod 33 = 22 |  |
| s = 22amod 33= 22 |  | s = 11bmod 33 = 22 |  | | s = 22a mod 33 |  |
|  |  |  |  | | s = 11b mod 33  22a mod 33 = 11b mod 33 |  |
| s = 22 |  | s = 22 |  | |  |  |

"хочузачетавтоматом"

АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ

"кдмиэхмъзхчздвхздв"

**Вывод:** мы овладение основными криптографическими алгоритмами шифрования. Зашифровали сообщение с помощью шифра Цезаря и научились применять алгоритм Диффи-Хелмана.

**Практическое занятие №8**

**Тема «Криптографическая защита информации»**

Цель: Овладение навыками работы с известными криптографическими алгоритмами.

**Теоретическое введение**

Несмотря на достаточно большое число различных систем с открытыми ключами, одной из наиболее популярных остается криптосистема RSA, созданная в 1977 г. и названная в честь ее создателей Рона Ривеста, Ади Шамиpа и Леонарда Эйдельмана. Они воспользовались тем фактом, что нахождение больших простых чисел в вычислительном отношении осуществляется легко, а разложение на множители произведения двух таких чисел – сложно.

В статье этих авторов, вышедшей в 1978 г., премия в сто долларов была назначена тому, кто первым расшифрует сообщение

68613754622061477140922254355882905759991125743198746951209308162982251457083569314766288398962801339199055182994515781515.

Метод шифрования был известен, единственное, что требовалось – разложить на два сомножителя 129-значное число, приведенное в этой статье.

Это было сделано только в 1994 г.

Задача была решена с помощью 600 человек и потребовала 220 дней и 1600 компьютеров, связанных через Internet.

**Теоретические основы алгоритма RSA**

Рассмотрим математические результаты, которые положены в основу этого алгоритма.

Определение 1. Сравнением целых чисел a и b будем называть соотношение между ними вида a = b + mk, означающее, что их разность (a – b) делится на заданное положительное число m, называемое модулем сравнения. При этом, а называется вычетом числа b по модулю m.

Определение 2. Говорят, что два целых числа a и b сравнимы между собой и обозначают этот факт через a = b (mod m), если a и b имеют одинаковые остатки при делении на m.

Приведем некоторые очевидные свойства сравнений.

Пусть a = b (mod m) и с = d (mod m). Тогда:

1. a (+-) c = b (+-) d (mod m),
2. a\*c (+-) b\*d (mod m).

Легко также проверить, что операция сравнения по модулю m является эквивалентностью (выполняются свойства рефлексивности, транзитивности и симметричности), и, следовательно, можно говорить о разбиении множества целых чисел Z на непересекающиеся классы эквивалентности.

Теорема 1. (Малая теорема Ферма). Если p – простое число, то (x в степени (p – 1)) = 1 (mod p) для любого х, простого относительно p, и (x в степени p) = х (mod p) для любого х.

Определение 3. Функцией Эйлеpа Ф(n) называется число положительных целых, меньших n и простых относительно числа n.

Теорема 2. Если n = pq, (p и q – отличные друг от друга простые числа), то Ф(n) = (p – 1)(q – 1).

Теорема 3. Если n = pq, (p и q – отличные друг от друга простые числа) и х – простое относительно p и q, то (x в степени Ф(n)) = 1 (mod n).

Следствия:

Если n = pq, (p и q – отличные друг от друга простые числа) и е – пpостое число относительно Ф(n), то отображение Е(e,n): x -> (x в степени e) (mod n) является взаимно однозначным на алгебраическом кольце вычетов Z(n).

Если е – пpостое число относительно Ф(n), то существует целое число d, такое, что e\*d = 1 (mod Ф(n)).

Пусть n = pq, где p и q – различные простые числа. Если e и d удовлетворяют уравнению (см. следствие 2), то отображения Е(e,n) и Е(d,n) являются инверсиями на кольце Zn.

Как Е(e,n), так и Е(d,n) легко рассчитываются, когда известны e, d, p, q.

Если известны e и n, но p и q неизвестны, то Е(e,n) представляет собой однонаправленную функцию; нахождение Е(d,n) по заданному n равносильно разложению n на простые сомножители.

Если p и q – достаточно большие простые числа, то разложение n – достаточно сложная вычислительная операция.

Это и заложено в основу системы шифрования RSA.

Пользователь i выбирает пару различных простых p(i) и q(i) и рассчитывает пару целых (e(i), d(i)), которые являются простыми относительно Ф(n(i)), где n(i) = p(i)\*q(i).

Итак, в реальных системах RSA реализуется следующим образом:

Каждый пользователь выбирает два больших простых числа p и q, и в соответствии с описанным выше алгоритмом выбирает два простых числа e и d; как результат умножения первых двух чисел устанавливается n. После этого {e, n} образует открытый ключ, а {d, n} – секретный (хотя можно взять и наоборот).

Открытый ключ публикуется и доступен каждому, кто желает послать владельцу ключа сообщение, которое зашифровывается указанным алгоритмом. После шифрования, сообщение невозможно дешифровать с помощью открытого ключа. Владелец же секретного ключа без труда может расшифровать принятое сообщение.

**Решение 3 варианта**

1. Дано два простых числа **p = 11** и **q = 101**
2. Вычисляется произведение **n = p\*q**, в нашем задании **n = 11\*101 = 1111**

Вычисляется функция Эйлера **φ(n)**

**φ(n) = (p-1) \* (q-1)**

В нашем задании **φ(n) = (11** **-1) \* (101-1) = 1000**. Функция Эйлера определяет количество целых положительных чисел, не превосходящих **n** и взаимно простых с **n**.

Целые числа называются взаимно простыми, если они не имеют никаких общих делителей, кроме 1.

1. Выбирается произвольное целое **0 < e < n** взаимно простое с значением функции Эйлера **φ(n)**. Возьмём **e = 3**. Пара чисел **(e, n)** объявляется открытым ключом шифра. В нашем примере **(e, n) = (3, 1111)**
2. Вычисляется целое число **d** (обратное число по модулю от е) из соотношения

**(d\*e) mod φ(n) = 1**.

Операция **mod** вычисляет остаток от целочисленного деления двух чисел.

Это соотношение означает, что результатом деления произведения чисел **e** и **d** на значение функции Эйлера должно быть число 1. Поэтому **d** можно рассчитать по формуле

http://altaev-aa.narod.ru/security/images/im7.png,

d = 3.

при **k = 1**, **d** – не целое, при **k =2**, **d =667**. Пара чисел **(d, n)** будет закрытым ключом шифра. В нашем задании **(d, n) = (667, 1111)**.

RSA-шифрование сообщения **T** выполняется с помощью открытого ключа получателя **(e, n)** по формуле

http://altaev-aa.narod.ru/security/images/im9.png,

где **Ti** и **Ci** числовые эквиваленты символов исходного и зашифрованного сообщений (см. табл. 1).

Таблица 1. Числовые эквиваленты русских букв, цифр и символа пробела

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** | **14** | **15** | **16** | **17** | **18** | **19** | **20** | **21** | **22** | **23** |
| А | Б | В | Г | Д | Е | Ё | Ж | З | И | Й | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **24** | **25** | **26** | **27** | **28** | **29** | **30** | **31** | **32** | **33** | **34** | **35** | **36** | **37** | **38** | **39** | **40** | **41** | **42** | **43** | **44** |
| Ц | Ч | Ш | Щ | Ъ | Ы | Ь | Э | Ю | Я | пробел | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |

Таблица 2. Числовые эквиваленты латинских букв, цифр и символа пробела

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **65** | **66** | **67** | **68** | **69** | **70** | **71** | **72** | **73** | **74** | **75** | **76** | **77** | **78** | **79** | **80** | **81** | **82** | **83** | **84** | **85** | **86** | **87** | **88** | **89** | **90** |
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |

Зашифруем сообщение «CDA» с помощью открытого ключа (3, 1111) (см. табл. 3).

Таблица 3. Вычисление шифрограммы

|  |  |  |
| --- | --- | --- |
| Символы исходного сообщения, Ti | Коды символов Ti(табл. 1) | Зашифрованные коды символов Ci |
| C | 67 | 673 mod 1111 = 793 |
| D | 68 | 683 mod 1111 = 19 |
| A | 65 | 653mod 1111 = 208 |

Таким образом, мы исходное сообщение «CDA» представили в виде шифрограммы «793, 19, 208».

Расшифровка RSA-закодированного сообщения **T** выполняется с помощью закрытого ключа получателя **(d, n)** по формуле

http://altaev-aa.narod.ru/security/images/im10.png

Теперь восстановим исходное сообщение. Восстановим исходное сообщение, применив закрытый ключ **(d, n) = (667, 1111)** той же пары (см. табл. 4).

Таблица 4. Восстановление сообщения

|  |  |  |
| --- | --- | --- |
| Зашифрованные коды символов Ci | Дешифрованные коды символов Ti(табл. 4.1) | Символы исходного сообщения,Ti |
| 793 | 793 667mod 1111 = 67 | C |
| 19 | 19667mod 1111 = 68 | D |
| 208 | 208667 mod 1111 = 65 | A |

Таким образом, мы восстановили исходное сообщение «CDA».

**Вывод**: на этом практическом занятии мы научились зашифровывать и расшифровывать данные с помощью ключей RSA.

**Практическое занятие №9**

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

Цель: Изучить основные положения авторского права и смежных прав.

Авторское право распространяется на произведения науки, литературы и искусства, являющиеся результатом творческой деятельности, независимо от назначения и достоинства произведения, а также от способа его выражения.

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

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).

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.

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. 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.

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

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

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.

Наиболее распространенные виды авторских договоров:

* издательский договор;
* постановочный договор;
* сценарный договор;
* договор о депонировании рукописи;
* договор художественного искусства;
* договор об использовании в промышленности произведений декоративно-прикладного искусства. Договор, предусматривающий способы использования произведения (конкретные права, передаваемые по данному договору); срок, на который передается право, и территорию, на которую распространяется действие этого права на указанный срок; размер вознаграждения и (или) порядок определения размера вознаграждения за каждый способ использования произведения, порядок и сроки его выплаты, а также другие условия, которые стороны сочтут необходимыми.

**Вывод:** На практическом занятии я изучила основы авторского права и смежных прав; имущественные и неимущественные права; субъекты авторского права; разобрала основы написания авторского договора.

**Практическое занятие №10**

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

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

Основные составляющие описания изобретения:

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

Описание начинается с названия изобретения и указания индекса или индексов рубрики действующей редакции международной патентной классификации, к которой относится заявляемое изобретение. Названия разделов в тексте описания не указываются. Не допускается замена раздела «Описание» в целом или его части отсылкой к источнику, в котором находятся необходимые сведения. В разделе «Уровень техники» приводятся сведения об аналогах и прототипах.

Заявка подается в трех экземплярах и должна содержать:

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

На изобретение:

Заявка на выдачу патента на изобретение подается автором изобретения, нанимателем, если изобретение служебное. Заявка подается в трех экземплярах. Вместе с заявкой или не позднее 2-х месяцев с даты ее подачи в одном экземпляре предоставляется документ, подтверждающий уплату пошлины в установленном размере.

Заявка на выдачу патента:

В данном разделе необходимо указать состав заявки, сколько экземпляров заявки необходимо подавать в патентный орган, а также на каких языках оформляется заявка. Временная правовая охрана заявленному изобретению предоставляется с даты публикации заявки до даты публикации сведений о патенте. Заявку на полезную модель преобразовать в заявку на изобретение возможно до даты получения решения о выдаче патента на полезную модель.

Заявка на полезную модель:

Заявка на полезную модель должна относиться к одной полезной модели или гpyппу полезных моделей, связанных между собой так, что они образуют единый творческий замысел. До даты получения заявителем решения о выдаче патента на полезную модель, а в случае принятия решения об отказе в выдаче патента - до момента истечения срока его обжалования, возможно преобразование заявки на полезную модель в заявку на изобретение.

Патент на полезную модель действует в течение пяти лет, считая с даты подачи заявки в патентный орган.

Патентно-лицензионная деятельность, регистрация объектов интеллектуальной собственности (ОИС), изобретения, полезные модели, промышленные образцы, товарные знаки и знаки обслуживания, топологии интегральных микросхем, компьютерные программы, оценка объектов интеллектуальной собственности (ОИС), процедура получения охранных документов.

Топологии интегральной микросхемы, товарные знаки, программы , базы данных.

**Вывод:** в течение практического занятия я овладела навыками составления и оформления заявок на объекты промышленной собственности, закрепила их на практике, изучила на какие объекты промышленной собственности можно оформлять патент, как оформляются заявки, какие существуют правила.

**Практическое занятие №11**

**Тема «Патентные исследования»**

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

**Теоретическое введение**

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

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

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

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 КЛАССИФИКАЦМЯ (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:

1. инструментом для упорядоченного хранения патентных документов, что облегчает доступ к содержащейся в них технической и правовой информации;
2. основой для избирательного распределения информации среди потребителей патентной информации;
3. основой для определения уровня техники в отдельных областях;
4. 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).

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  | | --- | --- | --- | --- | --- | | 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:

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

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

Отчет о патентных исследованиях должен содержать:

1. титульный лист;
2. список исполнителей;
3. содержание;
4. перечень сокращений, условных обозначений, символов, единиц, терминов;
5. общие данные об объекте исследования;
6. основную (аналитическую) часть;
7. заключение;
8. приложения.

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

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

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

1. оценку состояния выполнения работы, составной частью которой являются патентные исследования, и ее соответствие планам программ, перспективным целям деятельности предприятия (организации);
2. 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 |

**Ход выполнения:**

В результате проведения исследовательских работ по увеличению точности и расширения эксплуатационных возможностей производства, было предложено конструктивное выполнение механизма для обеспечения линейного перемещения исследуемых препаратов, внешний вид которого представлен на рисунке 1.

рис5

Рисунок 1 – механизм для обеспечения линейного перемещения исследуемых препаратов

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

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

В качестве существенных признаков при патентовании предполагаемого изобретения, выносится конструктивный признак: взаимное расположение перемещающихся элементов.

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

1. объект – *механизм для обеспечения линейного перемещения исследуемых препаратов;*
2. страна поиска – *Республика Беларусь*;
3. источники информации – *патентные*;
4. ретроспективность – *5 лет*;

информационная база - *Афiцыйны бюлетэнь «Вынаходствы, карысныя мадэлi, прамысловыя узоры» Нацыянальнага цэнтра iнтэлектуальная уласнасцi Рэспублiкi Беларусь, каталог МПК.* [http://www.belgospatent.org.by](http://www.belgospatent.org.by/)

Для проведения патентного поиска необходимо определить классификационную рубрику предполагаемого изобретения, которая в данном случае, классифицируется по разделу **«**Физика**»**, класс **«G12B 1/00 Чувствительные элементы, способные производить движение или перемещение, применение которых не ограничивается целями измерения; передаточные механизмы, связанные с ними».**

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Таблица 6 – Патентная документация | | | | |
| Предмет поиска (объект исследования, его составные части) | Страна выдачи, вид и номер охранного документа. Классификационный индекс | Заявитель (патентообладатель), страна. Номер заявки, дата приоритета, конвенционный приоритет, дата публикации | Название изобретения (полезной модели, промышленного образца) | Сведения о действии охранного документа или причина его аннулирования (только для анализа патентной чистоты) |
| Механизм линейного перемещения, Устройство перемещения держателя объекта, Привод перемещения координатного устройства для подачи | Патент РБ  № 6634  МПК 7G 12B 1/00 | ОАО «Пеленг»  Заявка a 20010103 от  2001.02.08, опубл.  2002.09.30 | «Механизм линейного перемещения» | Действует |
| Патент РБ  № 20689  МПК B23Q 5/22 | Государственное научное учреждение «Объединенный институт машиностроения Национальной академии наук Беларуси»  Заявка a 20130583 от  2013.05.03, опубл.  2014.12.30 | «Привод перемещения координатного устройства для подачи инструмента» | Действует |
| Патент РБ  № 2439  МПК  6 G 02B 21/26 | Санников П. А., М., Казеев Ю. И. Заявка 960025 от 1998.12.30, опубл. 1997.09.30 | «Устройство перемещения держателя объекта» | Не действует |

**Патент РБ № 2439 «Устройство перемещения держателя объекта»**

Изобретение относится к точному приборостроению и может быть использовано в контрольно-измерительной техники, в частности в микроскопах сравнения и стереоскопических микроскопах. Задачей изобретения является разработка устройства, обеспечивающая шесть степеней свободы держателя объекта с возможность определения величины линейного и углового перемещения по всем направлениям.

**Патент РБ № 6634 «Механизм линейного перемещения»**

рис5

Рисунок 2 - Механизм линейного перемещения

Изобретение относится к области приборостроения и может быть использовано для перемещения узла в двух взаимно-перпендикулярных направлениях. Изобретение направлено на повышение точности и расширения эксплуатационных возможностей.

Это обеспечивается за счет того, что механизм линейного перемещения содержит корпус, площадку для размещения юстируемого изделия и два регулировочных узла.

**Патент РБ № 20689 «Привод перемещения координатного устройства для подачи инструмента»**

Привод перемещения координатного устройства для подачи режущего инструмента содержащий с основание с направляющей, на которой установлена подвижная каретка, основной электродвигатель, с редуктором, соединенным с расположенным вдоль направляющей бесконечным ремнем, связанным с указанной кареткой, установленный вдоль направляющей линейный дополнительный электродвигатель, якорь которого жестко связан с кареткой, статор – с основанием , а также программируемый программный модуль управления перемещением каретки, выходы которого связны с входами управления указанных электродвигателей.

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

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

**Практическое занятие №12**

**Тема «**Патентный поиск**»**

Цель: освоить навыки проведения патентного поиска по заданной тематике.

**Теоретическое введение**

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

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

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

Национальный центр интеллектуальной собственности [http://www.belgospatent.org.by](http://www.belgospatent.org.by/)

Российское агентство но патентам и товарным знакам (Роспатент) предоставляет доступ к патентным материалам на страницах своего сайта:

http://www1.fips.ru/wps/wcm/connect/content\_ru/ru/inform\_resources/inform\_retrieval\_system

Евразийские патенты – http://www.eapo.org

Бесплатный поиск по патентам США возможно проводить с 1790 г по сайту компании United States Patent and Trademark Office [http://www.uspto.gov](http://www.uspto.gov/patft/)

Европейский патентный офис [http://www.epo.org](http://www.epo.org/)

Патентное бюро Японии. Поиск по серверу Японского патентного ведомства (ЯПВ) необходимо начинать со страницы [www.jpo.go.jp](http://www.jpo.go.jp)

**Ход работы:**

#### Провести патентный поиск по теме дипломного проекта, в соответствии с номером варианта.

|  |  |
| --- | --- |
| 2. | Программное приложение для контроля географического местоположения мобильных объектов на платформе Android. |

### Passive area geographic information acquiring system based on Android platform and method thereof

# Patent №: CN104833995 (A) ― 2015-08-12

**Classification:[G01S19/48](https://worldwide.espacenet.com/publicationDetails/biblio?DB=EPODOC&II=1&ND=3&adjacent=true&locale=en_EP&FT=D&date=20150812&CC=CN&NR=104833995A&KC=A)  
Applicant(s): UNIV SOUTHEAST**

The invention discloses a passive area geographic information acquiring system based on an Android platform and a method thereof, which belongs to the technical field of GPS positioning. The passive area geographic  information acquiring system comprises the components of a GPS positioning module which acquires latitude and longitude coordinates of an active point, a ranging module which measures distance information between target positioning points, an MEMS sensor module which measures a coordinate direction angle between the target positioning points, a controller module, a wireless transmitting module, a wireless receiving module and a data processing module which operates on the Android platform. The method comprises the steps of establishing a passive point set by distance information and direction angle information, determining the latitude and longitude coordinates of the target positioning point after the GPS signal is stable, determining a coordinate correction amount by means of a conversion relationship between a passive coordinate system and a geodetic coordinate system, converting the passive coordinate of the target positioning point to the geodetic coordinate according to the coordinate correction amount, and converting the geodetic coordinate to the latitude and longitude coordinates. The passive area geographic information acquiring system is provided with a wireless GPS positioning system which operates on the Android moving platform and realizes accurate acquisition for the passive area geographic information.

### Система получения географической информации с пассивной областью на основе платформы Android и ее особенностей

# Патент №: CN104833995 (A) ― 2015-08-12

**Классификация:**[**G01S19/48**](https://worldwide.espacenet.com/publicationDetails/biblio?DB=EPODOC&II=1&ND=3&adjacent=true&locale=en_EP&FT=D&date=20150812&CC=CN&NR=104833995A&KC=A) **Заявитель: UNIV SOUTHEAST**

Изобретение раскрывает области географической информационной системы на основе Android платформы и способу, который принадлежит к технической области позиционирования GPS. Географическая система получения информации пассивной области включает компоненты модуля определения местоположения GPS, которая приобретает координаты широты и долготы активной точки, в пределах модуля, который измеряет информацию о расстоянии между точками целевого позиционирования, модулем датчика MEMS, который измеряет координатный угол направления между целевая точку позиционирования, модуль контроллера, беспроводной передающий модуль, беспроводной модуль приема и модуль обработки данных, который работает на Android платформы. Способ включает в себя этапы создания пассивного точки, установленной информацией о расстоянии и информации угла направления, определение широты и долготы координаты точки целевого позиционирования после того, как сигнал GPS стабильна, определение координат величину коррекции с помощью отношений преобразования между а пассивная система координат и геодезическая система координат, преобразование пассивной координаты точки мишени позиционирования к геодезическим координатам в соответствии с величиной коррекции координат, и преобразования координат геодезического в координаты широты и долготы.

Географическая система получения информации пассивной площади предоставляются беспроводной системой позиционирования GPS, который работает на Android подвижной платформу и реализует точное приобретение для пассивной области географической информации.

# GPS navigation system based on Android platform

# Patent №: CN105066987 (A) ― 2015-11-18

**Classification:** [**G01C21/00**](https://worldwide.espacenet.com/publicationDetails/biblio?DB=EPODOC&II=0&ND=3&adjacent=true&locale=en_EP&FT=D&date=20151118&CC=CN&NR=105066987A&KC=A)

**Applicant(s): UNIV BINZHOU; LIU MING**

# The invention relates to the technical field of navigation, in particular to a GPS navigation system based on an Android platform. The GPS navigation system comprises a mobile device and a Baidu map server. The mobile device enables a GPRS wireless transmission technology, a GPS positioning technology and a geographic information system (GIS) to be combined together to achieve the GPS navigation system. The mobile device is connected with a mobile phone GPS module, a GPRS module, a touch screen and a display. The mobile phone GPS module is connected with a GPS navigation satellite. The mobile device is wirelessly connected with the Baidu map server through the GPRS module to obtain map services. The mobile device is provided with a current position positioning module, a specified address query module, a longitude and latitude query module, a position information service module, a route navigation module, a specified address tracking module and a system setting module. The GPS navigation system is combined with humanized user interface (UI) design of a mobile phone client to provide convenience for all Android mobile phone users.

# Система GPS навигации на платформе Android

# Патент №: CN105066987 (A) ― 2015-11-18

**Классификация:** [**G01C21/00**](https://worldwide.espacenet.com/publicationDetails/biblio?DB=EPODOC&II=0&ND=3&adjacent=true&locale=en_EP&FT=D&date=20151118&CC=CN&NR=105066987A&KC=A)

**Заявители: UNIV BINZHOU; LIU MING**

# Изобретение относится к области навигации, в частности, к системе GPS навигации на основе Android. Система GPS навигации содержит мобильное устройство и серверную карту Baidu. Мобильное устройство предоставляет технологию беспроводной передачи данных GPRS, технологию позиционирования GPS и географической информационной системы (ГИС), которые могут быть объединены вместе для создания GPS навигационной системы. Мобильное устройство соединено с мобильным модулем телефона GPS, модулем GPRS, сенсорным экраном и дисплеем. Мобильный телефон GPS модуль связан с GPS навигацией спутника. Мобильное устройство беспроводное соединение с картой сервера Baidu через модуль GPRS для получения картографических сервисов. Мобильное устройство снабжено модулем текущего позиционирования, модулем запроса адреса, модуль долготы и широты запроса, модуль службы информации о положении, маршрут навигационный модуль, указанный модуль отслеживания адреса и модуля настройки системы. Система GPS навигации в сочетании с очеловеченным пользовательским интерфейсом (UI) конструкцией клиента мобильного телефона, чтобы обеспечить удобство для всех Android пользователей мобильных телефонов.

### Mobile object monitor system based on Android operation system

# Patent №: CN204086967 (U) ― 2015-01-07

**Classification:** [**G05B19/418**](https://worldwide.espacenet.com/publicationDetails/biblio?DB=EPODOC&II=3&ND=3&adjacent=true&locale=en_EP&FT=D&date=20150107&CC=CN&NR=204086967U&KC=U)

**Applicant(s): SUN XIUYNG**

# The utility model discloses a mobile object monitor system based on an Android operation system. The mobile object monitor system comprises a plurality of monitor terminals that are respectively disposed on each mobile object. The monitor terminals collect the monitor data of the mobile objects in a real-time manner. The monitor data comprises mobile object geographic coordinate data, mobile object driving state data and mobile object monitor video data. The mobile object monitor system further comprises a communication server that is in communication connection with the monitor terminals and connected to a public communication network through a wireless network gateway. The mobile object monitor system also comprises a plurality of mobile terminals utilizing the Android operation system. Each mobile terminal obtains the monitor data transmitted by the communication server through the public communication network. The mobile object monitor system enables remote wireless monitor of mobile objects with unattended operation, achieve good monitor mobility, and is advantaged by being simple in structure, easy to realize and low in cost.

### Система отслеживания мобильных объектов на базе ОС Android

# Патент№: CN204086967 (U) ― 2015-01-07

**Классификация:** [**G05B19/418**](https://worldwide.espacenet.com/publicationDetails/biblio?DB=EPODOC&II=3&ND=3&adjacent=true&locale=en_EP&FT=D&date=20150107&CC=CN&NR=204086967U&KC=U)

**Заявитель: SUN XIUYNG**

# Полезная модель раскрывает мобильную систему отслеживания на основе операционной системы Android. Система отслеживания мобильного объекта содержит множество отслеживающих терминалов, которые соответственно расположены на каждом подвижном объекте. Отслеживающие терминалы собирают данные о подвижных объектах в режиме реального времени. Данные слежения включают в себя координатные данные мобильного объекта, данные о состоянии движения подвижного объекта и видеоданные подвижного объекта. Система мобильного слежения дополнительно содержит коммуникационный сервер, который находится в соединении связи с терминалами монитора, подключено к сети связи общего пользования через беспроводной шлюз сети. Система мобильного слежения за объектaми также содержит множество мобильных датчиков, использующих систему Android. Каждый мобильный терминал получает данные слежения, передаваемые на сервер связи через сеть общего пользования. Система мобильного отслеживания объекта позволяет осуществлять дистанционный беспроводной мониторинг мобильных объектов с работой без присмотра, достижение хорошей мобильности.

# Navigation vehicle information management system based on Android system

# Patent №: CN102323883 (A) ― 2012-01-18

**Classification:** [**G06F9/44**](https://worldwide.espacenet.com/publicationDetails/biblio?DB=EPODOC&II=6&ND=3&adjacent=true&locale=en_EP&FT=D&date=20120118&CC=CN&NR=102323883A&KC=A)**;**[**H04M1/725**](https://worldwide.espacenet.com/publicationDetails/biblio?DB=EPODOC&II=6&ND=3&adjacent=true&locale=en_EP&FT=D&date=20120118&CC=CN&NR=102323883A&KC=A)

**Applicant(s): GUAGNDONG DONGNA SOFTWARE TECHNOLOGY CO LTD**

# The invention discloses a navigation vehicle information management system based on an Android system, which comprises a system framework, a navigation information service module, a GIS (Geographic Information System) navigation engine, a JNI (Java Native Interface) module and a user interface module, wherein communication and cooperation among all modules are realized and managed by using the system framework, the navigation information module is a background module for enabling third party software to request navigation information, and the JNI module is used for scheduling the GIS navigation engine. According to the system, a user can conveniently and efficiently complete navigation tasks without additionally purchasing a navigator; meanwhile, the system also can provide the navigation information for the third party software, thus practical applicability of the Android mobile phone system is greatly enhanced.

# Система управления транспортно-навигационной информацией на базе Android

# Патент №: CN102323883 (A) ― 2012-01-18

**Классификация:** [**G06F9/44**](https://worldwide.espacenet.com/publicationDetails/biblio?DB=EPODOC&II=6&ND=3&adjacent=true&locale=en_EP&FT=D&date=20120118&CC=CN&NR=102323883A&KC=A)**;**[**H04M1/725**](https://worldwide.espacenet.com/publicationDetails/biblio?DB=EPODOC&II=6&ND=3&adjacent=true&locale=en_EP&FT=D&date=20120118&CC=CN&NR=102323883A&KC=A)

**Заявитель: GUAGNDONG DONGNA SOFTWARE TECHNOLOGY CO LTD**

# Изобретение раскрывает систему управления информацией навигации транспортного средства на основе Android системы, которая включает в себя структуру системы, модуль обслуживания навигационной информации, ГИС (географическая информационная система) Навигационная двигатель, JNI (Java Native Interface) модуль и модуль пользовательского интерфейса , в котором связь и сотрудничество между всеми модулями реализуются и управляются с помощью рамки системы, навигационной информации модуль представляет собой справочный модуль для включения стороннего программного обеспечения для запроса навигационной информации, а модуль JNI используется для планирования ГИСА навигации двигателя. Согласно системе, пользователь может легко и эффективно выполнять задачи навигации без дополнительного приобретения навигатора; Между тем, система также может предоставить навигационную информацию для стороннего программного обеспечения, таким образом, практическая применимость Android системы мобильного телефона значительно усиливается.

### Android platform-based big dipper and GPS dual-mode on-line positioning method

**Patent №:** **CN105005058 (A) ―2015-10-28**

**Classification:** [**G01S19/33**](https://worldwide.espacenet.com/publicationDetails/biblio?DB=EPODOC&II=2&ND=3&adjacent=true&locale=en_EP&FT=D&date=20151028&CC=CN&NR=105005058A&KC=A)

**Applicant(s): LIZHOU BAISIDE INFORMATION TECHNOLOGY CO LTD**

The invention relates to an Android platform-based big dipper and GPS dual-mode on-line positioning method, which comprises a mobile positioning terminal capable of receiving the information sent by a satellite, a remote cloud server, a mobile webpage client, and an Android handset client. The mobile positioning terminal is connected with the remote cloud server through the internet. The remote cloud server is respectively connected with the mobile webpage client and the Android handset client through the internet. A mobile platform of the Freescale i.MX 6q series is operated based on the Android system, so that the real-time location information of a Big Dipper/GPS dual-mode module can be received in real time. Therefore, problems in the prior art that in some remote areas, corresponding services cannot be supplied to people or enterprise and public institutions in need due to the bare coverage of communication base stations and the large transmission difficulty of information can be solved.

### Двухрежимный метод онлайн позиционирования на платформе Android, основанный на GPS-системы и большой медведицы.

**Патент №:** **CN105005058 (A) ―2015-10-28**

**Классификация:** [**G01S19/33**](https://worldwide.espacenet.com/publicationDetails/biblio?DB=EPODOC&II=2&ND=3&adjacent=true&locale=en_EP&FT=D&date=20151028&CC=CN&NR=105005058A&KC=A)

**Заявитель: LIZHOU BAISIDE INFORMATION TECHNOLOGY CO LTD**

Изобретение относится к Android платформы на основе большой медведицы и GPS с двухрежимным онлайн способом позиционирования, который включает мобильный терминал позиционирования, способный принимать информацию, передаваемую со спутника, удаленным облачным сервером, мобильным клиентам посредством веб-страницы, Android-пользователям. Мобильный терминал позиционирования соединен с удаленным облачным сервером через Интернет. Удаленный облачный сервер соответственно соединен с мобильным клиентом веб-страницы и пользователями Android телефонов через Интернет. Мобильная платформа Freescale. серии 6Q MX работает на основе Android системы, так что информация о местоположении можно получить в режиме реального времени. Таким образом, могут быть решены отсутствия связи в некоторых отдаленных районах.

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

**Практическое занятие №13**

Тема «Регистрация компьютерных программ в Национальном центре интеллектуальной собственности»

Цель: Овладеть навыками подготовки документации для регистрации компьютерных программ.

**Теоретическое введение**

Регистрация компьютерных программ осуществляется Национальным центром интеллектуальной собственности в порядке оказания услуг заинтересованным лицам по их инициативе (обращению) на основе представляемых ими сведений (материалов, подтверждающих создание компьютерной программы и принадлежность исключительного права на такую компьютерную программу конкретному лицу).

Лицам, заинтересованным в получении услуг по регистрации компьютерных программ, важно понимать, что осуществляемая со стороны НЦИС регистрация не является основанием или условием возникновения и осуществления авторского права на компьютерную программу. Регистрация производится исключительно в порядке оказания услуги заинтересованному лицу (автору или иному правообладателю, далее – заявителю) по его инициативе для целей предоставления ему независимого подтверждения факта его собственного заявления о создании компьютерной программы и принадлежности исключительного права на данный объект.

Ввиду ограниченности организационно-технических ресурсов и в целях минимизации собственных затрат, связанных с оказанием данного вида услуг, НЦИС заключен договор о сотрудничестве со специализированной организацией – ООО «Интеллектуальные медиа технологии» (далее – регистратор), на которую возложены функции по практической реализации действий, связанных с осуществлением регистрации компьютерных программ.

Проведение процедуры по регистрации компьютерной программы осуществляется в рамках договора, заключаемого заявителем с регистратором. Основанием для заключения договора является обращение заявителя (заявка), оформляемое в соответствии с [установленной формой](http://www.belgospatent.org.by/russian/docs/2016/zayv_comp.doc) и подаваемое в НЦИС лично (через уполномоченного представителя) или по почте с приложением [материалов](http://www.belgospatent.org.by/russian/docs/2016/perech_mat_comp_prog.pdf), необходимых для принятия решения о возможности осуществления регистрации компьютерной программы. Дальнейшая процедура регистрации компьютерной программы определяется договором, для заключения которого НЦИС передает поступившую заявку регистратору. Регистратор, заключив договор с заявителем, осуществляет необходимую обработку заявки и представленных материалов, обеспечивает в интересах заявителя сопровождение регистрационной процедуры.

В результате проведения процедуры регистрации компьютерной программы:

* заявитель получает свидетельство НЦИС о регистрации компьютерной программы,
* данные о компьютерной программе вносятся в реестр НЦИС и размещаются на сайте НЦИС,
* материалы компьютерной программы депонируются в НЦИС и могут впоследствии быть использованы для подтверждения от имени НЦИС необходимых заявителю обстоятельств.

**Ход выполнения:**

|  |  |
| --- | --- |
| В Национальный центр  интеллектуальной собственности  220034, г. Минск, ул. Козлова, 20 | дата поступления и рег. № (присваивается при необходимости): |
|  |

**ЗАЯВКА**

**на оказание услуг по регистрации компьютерной программы**

|  |  |  |
| --- | --- | --- |
| 1. Заявитель   /ФИО физического лица, полное наименование юридического лица/ | Сураго Дмитрий Александрович | |
| просит Национальный центр интеллектуальной собственности оказать услуги по регистрации компьютерной программы в соответствии с нижеприведенными данными | | |
| 1. Вид услуг   /отметить знаком «Х» нужное/ | Х | Стандартная регистрационная процедура (заявитель является автором) |
|  | Стандартная регистрационная процедура (заявитель не является автором) |
|  | Ускоренная регистрационная процедура  (заявитель является автором) |
|  | Ускоренная регистрационная процедура  (заявитель не является автором) |
|  | Оформление дополнительного экземпляра свидетельства |
|  | Оформление дополнительного экземпляра свидетельства на английском языке |
|  | Оформление изменений в отношении ранее зарегистрированной компьютерной программы |
| 1. Название компьютерной программы | Приложение «Студенты университета». | |
| 1. Год создания компьютерной программы | 2020 | |
| 1. Авторы компьютерной программы   /ФИО автора(ов), дата (число/месяц/год) рождения/ | Сураго Дмитрий Александрович 21.03.2001 | |
| 1. Правообладатель компьютерной программы   /ФИО физического лица, полное наименование юридического лица/ | Сураго Дмитрий Александрович | |
| 1. Основание принадлежности исключительного права на компьютерную программу   /отметить знаком «Х» нужное/ | X | Создание компьютерной программы |
|  | Переход исключительного права в порядке служебного произведения |
|  | Приобретение исключительного права по договору |
|  | Правопреемство (в т.ч. наследование) в отношении исключительного права |
| 1. Данные для заключения договора на оказание услуг по регистрации компьютерной программы   /полный (юридический) адрес, банковские реквизиты Заявителя; для организаций – лицо (ФИО и должность), уполномоченное на заключение договора (ссылка на документ); данные о лице, уполномоченном на ведение дел по договору - ФИО контактные данные – тел., эл. почта/ | Адрес: г. Минск, ул. Бобруйская 25  Телефон: +375(44) 734-71-56 (Life)  Эл. Почта: dmitriysuraho@mail.ru | |
| 1. Перечень прилагаемых материалов (с указанием носителя, кол-ва листов и т.д.)   /**обязательно** – экземпляр компьютерной программы, описание компьютерной программы, документы (заверенные копии), подтверждающие принадлежность исключительного права, при подаче Заявки через представителя – документ, подтверждающий полномочия представителя, **дополнительно** – на усмотрение заявителя/ | 1) Экземпляр программы  2) Описание программы  3) Заверенные копии документов | |
| Заявитель подтверждает свое понимание того, что регистрация компьютерной программы, о проведении которой просит Заявитель: 1) не является основанием или условием возникновения и осуществления авторского права на компьютерную программу, 2) осуществляется по инициативе Заявителя на основании предоставляемых им сведений (материалов), 3) в случае предоставления Заявителем для целей регистрации компьютерной программы недостоверных данных НЦИС или ассоциируемые с ним лица не могут рассматриваться ответственными за произведенную регистрацию компьютерной программы | | |
| 1. Дата Заявки и подпись Заявителя   /дата оформления заявки, подпись Заявителя либо уполномоченного представителя, ФИО, должность, печать – при наличии/ | 15 мая 2020 | |

**Описание программы**

**Назначение программы и область применения:**

Это игровое приложение хорошо подходит для развития логического мышления, обучая в игровой форме выстраивать взаимосвязанные логические цепочки, еще подходит для обогащения словарного запаса и повышения грамотности.

Игровое приложение «4 картинки 1 слово» имеет:

• возможность сохранения и модификации рабочей информации в централизованной базе данных;

• возможность изменения настроек интерфейса;

• уровневую структуру приложения;

• систему логирования;

• систему запросов;

• экспорт и импорт информации в базу данных;

Приложение создано на языке программирования С#. При разработке приложения были использованы:

* интегрированная среда разработки Microsoft Visual Studio Ultimate 2013 (Версия 12.0.21005.1 REL);
* программная платформа .NET Framework 4.6;
* язык программирования C#;
* расширяемый язык разметки XAML;
* технология WPF;
* ADO.NET

Приложения построено на технологии Windows Presentation Foundation. Для создания базы данных был выбран Microsoft SQL Server 2012.

Приложение спроектировано таким образом, что каждый класс выполняет свои функции и практически не зависит от других.

**Язык программирования:** С#

**Вид и версия операционной системы:** Windows 10 x64

**Объем программы:** 11,2 Мб

**Вывод:** в ходе данного практического занятия я овладела навыками подготовки документации для регистрации компьютерных программ.