Учреждение образование «Белорусский государственный технологический университет»

Кафедра информационных систем и технологий

Основы защиты информации

Электронная тетрадь

Студент:

Жаворонок Павел Евгеньевич

Вариант 10

Преподаватель:

Бракович Андрей Игоревич

Минск 2015

**Практическое занятие №1**

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

1. Что такое информационная безопасность?

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

1. Перечислить основные национальные интересы в информационной сфере?

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.

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

* нарушение функционирования критически важных объектов информатизации;
* недостаточные масштабы и уровень внедрения передовых информационно-коммуникационных технологий;
* снижение или потеря конкурентоспособности отечественных информационно-коммуникационных технологий, информационных ресурсов и национального контента;

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

В информационной сфере внутренними источниками угроз национальной безопасности являются:

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

В информационной сфере внешними источниками угроз национальной безопасности являются:

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

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

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 системах, используемых в инфраструктуре, являющейся жизненно важной для страны, отказ или разрушение которой может оказать существенное отрицательное воздействие на национальную безопасность.

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.

**Практическое занятие №2**

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

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 *Е0*. Несанкционированный доступ к объекту уменьшает полезный эффект от его функционирования (нарушается нормальная работа, наносится ущерб из-за утечки информации и т.д.) на величину *ΔЕ*. Тогда эффективность функционирования объекта с учетом воздействия несанкционированного доступа:

|  |  |
| --- | --- |
|  | (1) |





Относительная эффективность:

|  |  |
| --- | --- |
|  | (2) |



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:

|  |  |
| --- | --- |
|  | (4) |



Тогда получим что:

|  |  |
| --- | --- |
|  | (5) |

|  |  |
| --- | --- |
|  | (6) |

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

|  |  |
| --- | --- |
|  | (7) |

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

|  |  |
| --- | --- |
|  | (8) |

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

|  |  |
| --- | --- |
|  | (9) |



Вывод: в итоге при расходе в 900 на использование средств защиты, мы имеем прибыль в дополнительные 1600 или чуть больше 9% от общего дохода.

При расходе допустимых средств на защиту своего продукта от взлома или различного рода воздействия, мы можем увеличить свой доход и получить максимальную эффективность в условиях несанкционированного доступа. Но чтобы понять стоит ли защищать свой продукт для начала необходимо посчитать стоимость защиты. Так же если на ваш продукт возлагаются ответственные задачи для которых несанкционированный доступ влечет катастрофические потери эффективности их функционирования, влиянием стоимости средств защиты на эффективность можно пренебречь.

Учреждение образование

«Белорусский государственный технологический университет»

Кафедра информационных систем и технологий

Основы защиты информации

Политика информационной безопасности

оператора сотовой связи OAO «Мобилка»

Выполнил:

Жаворонок Павел Евгеньевич

Проверил:

Бракович Андрей Игоревич

Минск 2015

**Оглавление**

[Введение 3](#_Toc414366021)

[1. Общие положения 3](#_Toc414366022)

[1.2 Структура компании и организация связи 4](#_Toc414366023)

[1.3 Возможные угрозы и их анализ 5](#_Toc414366024)

[2.1 Исследование политики безопасности предприятия 8](#_Toc414366025)

[2.2 Организационный элемент защиты информации на OAO «Мобилка» 9](#_Toc414366026)

[2.3 Нормативно-правовой элемент защиты информации на предприятии OAO «Мобилка» 10](#_Toc414366027)

[2.4 Инженерно-технический элемент защиты информации на OAO «Мобилка» 11](#_Toc414366028)

[3. Политики информационной безопасности 12](#_Toc414366029)

[3.1 Политика предоставления доступа к информационному ресурсу 12](#_Toc414366030)

[3.2 Политика учетных записей 12](#_Toc414366031)

[3.3 Политика архивирования, резервного копирования и восстановления данных 13](#_Toc414366032)

[3.4 Политика реализации антивирусной защиты 13](#_Toc414366033)

[3.5 Политика защиты АРМ 14](#_Toc414366034)

[3.6 Политика пользования электронной почтой 15](#_Toc414366035)

[3.7. Методы и механизмы защиты в глобальной сети. 16](#_Toc414366036)

[Заключение 18](#_Toc414366037)

[Список используемой литературы 19](#_Toc414366038)

## Введение

Потоки информации, циркулирующие в окружающем нас мире, огромны. В этих потоках имеются документы, содержащие самую разнообразную информацию. Поэтому без решения задач информационной безопасности не может продолжать работу ни одно из предприятий. В любой организации, как большой, так и маленькой, возникает проблема безопасного хранения, передачи, использования информации.

Компания ОАО «Мобилка» хранит персональные данные своих клиентов, сотрудников. Компания вкладывает немалые средства в обеспечение своей защиты и защиты клиентов.

Исследование проблемы информационной безопасности на предприятиях связи становится наиболее актуальным с течением времени, т.к. развиваются и появляются новые операторы сотовой связи, преумножается количество клиентов, пользующихся услугами сотовой связи. Ведь любое несанкционированное вмешательство может повредить работу системы, вплоть до невозможности ее функционирования, что неизбежно повлечет за собой финансовые убытки для компании.

Защита документооборота и баз данных хранящих практически всю информацию о клиентах и сотрудниках является сложной, но обязательной задачей, без решения которой невозможно нормальное функционирование мобильного оператора.

## 1. Общие положения

Информация является ценным и жизненно важным ресурсом OAO «Мобилка» (далее – Компания). Настоящая политика информационной безопасности предусматривает принятие необходимых мер в целях защиты активов от случайного или преднамеренного изменения, раскрытия или уничтожения, а также в целях соблюдения конфиденциальности, целостности и доступности информации, обеспечения процесса автоматизированной обработки данных в Компании.

Ответственность за соблюдение информационной безопасности несет каждый сотрудник Компании, при этом первоочередной задачей является обеспечение безопасности всех активов Компании. Это значит, что информация должна быть защищена не менее надежно, чем любой другой основной актив Компании. Главные цели Компании не могут быть достигнуты без своевременного и полного обеспечения сотрудников информацией, необходимой им для выполнения своих служебных обязанностей.

1.2 Структура компании и организация связи

Основным документом, регламентирующим [корпоративное управление](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D1%80%D0%BF%D0%BE%D1%80%D0%B0%D1%82%D0%B8%D0%B2%D0%BD%D0%BE%D0%B5_%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5) в ОАО «Мобилка», является его устав[[75]](https://ru.wikipedia.org/wiki/%D0%9C%D0%BE%D0%B1%D0%B8%D0%BB%D1%8C%D0%BD%D1%8B%D0%B5_%D0%A2%D0%B5%D0%BB%D0%B5%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D1%8B#cite_note-75). Согласно уставу, высшим органом управления общества является [общее собрание акционеров](https://ru.wikipedia.org/wiki/%D0%9E%D0%B1%D1%89%D0%B5%D0%B5_%D1%81%D0%BE%D0%B1%D1%80%D0%B0%D0%BD%D0%B8%D0%B5_%D0%B0%D0%BA%D1%86%D0%B8%D0%BE%D0%BD%D0%B5%D1%80%D0%BE%D0%B2), которое проводится не реже раза в год. Общее руководство ОАО «Мобилка» в части вопросов, не отнесённых к компетенции общего собрания, осуществляется [советом директоров](https://ru.wikipedia.org/wiki/%D0%A1%D0%BE%D0%B2%D0%B5%D1%82_%D0%B4%D0%B8%D1%80%D0%B5%D0%BA%D1%82%D0%BE%D1%80%D0%BE%D0%B2), в состав которого входят девять человек, включая трёх независимых членов. В состав исполнительных органов Мобилки входят коллегиальный исполнительный орган — правление и единоличный исполнительный орган — президент.

****

Рисунок 1 – Структура управления ОАО «Мобилка»

В компании действует «матричная» система управления: стратегические и операционные функции поделены между корпоративным центром, бизнес-единицами, макрорегионами и филиалами.. В ОАО «Мобилка» приняты кодекс этических норм и кодекс корпоративного поведения.

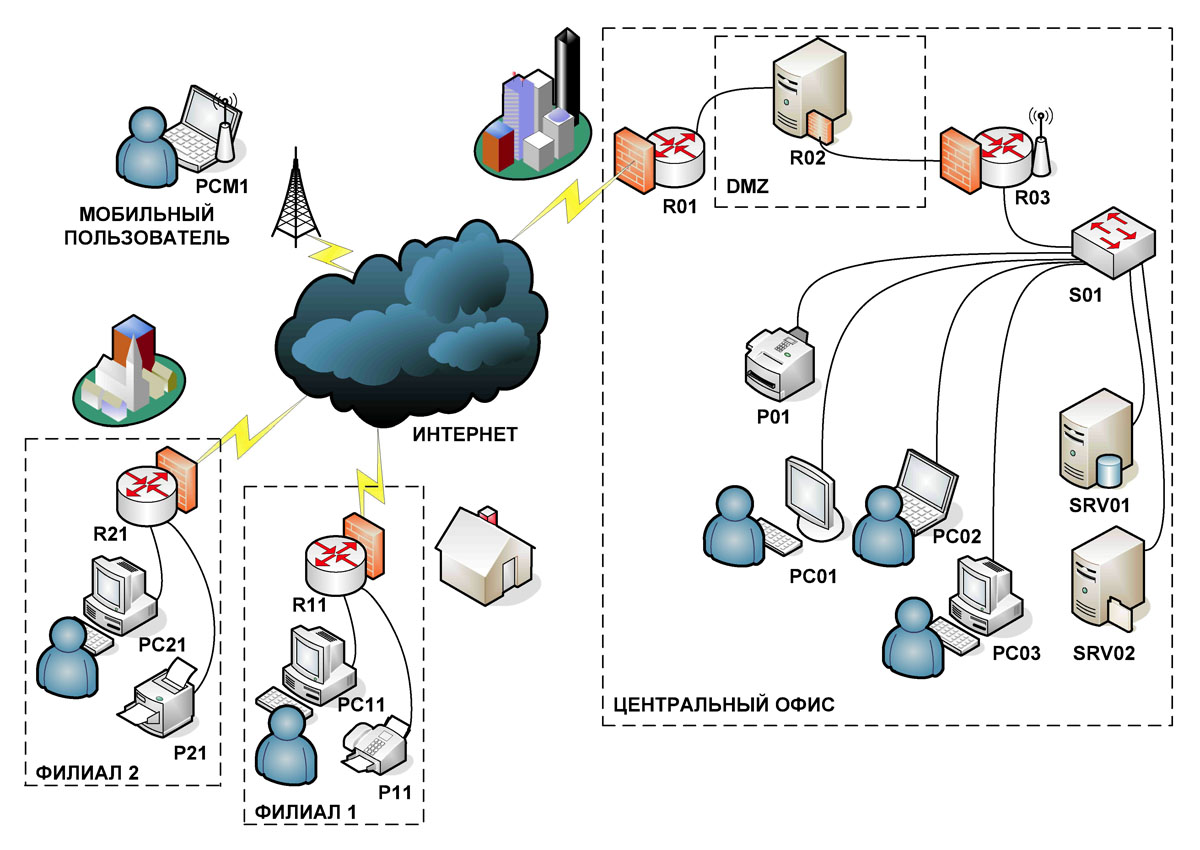


Рисунок 2 – Схема информационной сети ОАО «Мобилка»

Информационные системы, на которых работает компания, в данном случае, образуются совокупностью оборудования сетей центрального офиса, филиалов, домашних и мобильных пользователей.

## 1.3 Возможные угрозы и их анализ

Угроза безопасности - потенциальное нарушение безопасности, любое обстоятельство или событие, которое может явиться причиной нанесения ущерба предприятию в целом.

Все множество потенциальных угроз по природе их возникновения разделяется на два класса: естественные (объективные) и искусственные (субъективные).

Естественные угрозы - это угрозы, вызванные воздействиями на предприятие объективных физических процессов или стихийных природных явлений, независящих от человека.

Искусственные угрозы - это угрозы предприятию, вызванные деятельностью человека. Среди них, исходя из мотивации действий, можно выделить:

* непреднамеренные (неумышленные, случайные) угрозы, вызванные ошибками в проектировании, ошибками в программном обеспечении, ошибками в действиях персонала и т.п.;
* преднамеренные (умышленные) угрозы, связанные с корыстными, идейными или иными устремлениями людей (злоумышленников).
* Источники угроз по отношению к предприятию могут быть внешними или внутренними (составляющие самой организации - её аппаратура, программы, персонал, конечные пользователи).

Основные непреднамеренные искусственные угрозы предприятию (действия, совершаемые людьми случайно, по незнанию, невнимательности или халатности, из любопытства, но без злого умысла):

* неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы (неумышленная порча оборудования, удаление, искажение файлов с важной информацией или программ, в том числе системных и т.п.);
* неправомерное отключение оборудования или изменение режимов работы устройств и программ;
* неумышленная порча носителей информации;
* запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы (зависания или зацикливания) или осуществляющих необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и т.п.);
* нелегальное внедрение и использование неучтенных программ (игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения нарушителем своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);
* заражение компьютера вирусами;
* неосторожные действия, приводящие к разглашению конфиденциальной информации, или делающие ее общедоступной;
* разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);
* проектирование архитектуры системы, технологии обработки данных, разработка прикладных программ, с возможностями, представляющими опасность для работоспособности системы и безопасности информации;
* игнорирование организационных ограничений (установленных правил) при работе в системе;
* вход в систему в обход средств защиты (загрузка посторонней операционной системы со сменных магнитных носителей и т.п.);
* некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности;
* пересылка данных по ошибочному адресу абонента (устройства);
* ввод ошибочных данных;
* неумышленное повреждение каналов связи.

Основные возможные пути умышленной дезорганизации работы, вывода системы из строя, проникновения в систему и несанкционированного доступа к информации:

* физическое разрушение системы (путем взрыва, поджога и т.п.) или вывод из строя всех или отдельных наиболее важных компонентов компьютерной системы (устройств, носителей важной системной информации, лиц из числа персонала и т.п.);
* отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и т.п.);
* действия по дезорганизации функционирования системы (изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных радиопомех на частотах работы устройств системы и т.п.);
* внедрение агентов в число персонала системы (в том числе, возможно, и в административную группу, отвечающую за безопасность);
* вербовка (путем подкупа, шантажа и т.п.) персонала или отдельных пользователей, имеющих определенные полномочия;
* применение подслушивающих устройств, дистанционная фото- и видео-съемка и т.п.;
* перехват побочных электромагнитных, акустических и других излучений устройств и линий связи, а также наводок активных излучений на вспомогательные технические средства, непосредственно не участвующие в обработке информации (телефонные линии, сели питания, отопления и т.п.);
* перехват данных, передаваемых по каналам связи, и их анализ с целью выяснения протоколов обмена, правил вхождения в связь и авторизации пользователя и последующих попыток их имитации для проникновения в систему;
* хищение носителей информации (магнитных дисков, лент, микросхем памяти, запоминающих устройств и целых ПЭВМ);
* несанкционированное копирование носителей информации;
* хищение производственных отходов (распечаток, записей, списанных носителей информации и т.п.);
* чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
* чтение информации из областей оперативной памяти, используемых операционной системой (в том числе подсистемой зашиты) или другими пользователями, в асинхронном режиме используя недостатки мультизадачных операционных систем и систем программирования;
* незаконное получение паролей и других реквизитов разграничения доступа (агентурным путем, используя халатность пользователей, путем подбора, путем имитации интерфейса системы и т.д.) с последующей маскировкой под зарегистрированного пользователя («маскарад»);
* несанкционированное использование терминалов пользователей, имеющих уникальные физические характеристики, такие как номер рабочей станции в сети, физический адрес, адрес в системе связи, аппаратный блок кодирования и т.п.;
* вскрытие шифров криптозащиты информации;
* внедрение аппаратных «спецвложений», программных «закладок» и «вирусов» («троянских коней» и «жучков»), то есть таких участков программ, которые не нужны для осуществления заявленных функций, но позволяющих преодолевать систему защиты, скрытно и незаконно осуществлять доступ к системным ресурсам с целью регистрации и передачи критической информации или дезорганизации функционирования системы;
* незаконное подключение к линиям связи с целью работы «между строк», с использованием пауз в действиях законного пользователя от его имени с последующим вводом ложных сообщений или модификацией передаваемых сообщений;
* незаконное подключение к линиям связи с целью прямой подмены законного пользователя путем его физического отключения после входа в систему и успешной аутентификации с последующим вводом дезинформации и навязыванием ложных сообщений.

Следует заметить, что чаще всего для достижения поставленной цели злоумышленник использует не один, а некоторую совокупность из перечисленных выше путей.

**2. Исследование процессов защиты информации на предприятии OAO «Мобилка»**

## 2.1 Исследование политики безопасности предприятия

Политика безопасности - это документ «верхнего» уровня, в котором должно быть указано:

* ответственные лица за безопасность функционирования фирмы;
* полномочия и ответственность отделов и служб в отношении безопасности;
* организация допуска новых сотрудников и их увольнения;
* правила разграничения доступа сотрудников к информационным ресурсам;
* организация пропускного режима, регистрации сотрудников и посетителей;
* использование программно-технических средств защиты;
* другие требования общего характера.

Таким образом, политика безопасности - это организационно-правовой и технический документ одновременно. При ее составлении надо всегда опираться на принцип разумной достаточности и не терять здравого смысла.

Например, в политике может быть указано, что все прибывающие на территорию фирмы сдают мобильные телефоны вахтеру (такие требования встречаются в некоторых организациях). Будет ли кто-нибудь следовать этому предписанию? Как это проконтролировать? К чему это приведет с точки зрения имиджа фирмы? Ясно, что это требование нежизнеспособное. Другое дело, что можно запретить использование на территории мобильных телефонов сотрудникам фирмы, при условии достаточного количества стационарных телефонов.

Особое внимание в политике безопасности надо уделить разграничению зоны ответственности между службой безопасности и IT-службой предприятия. Зачастую сотрудники службы безопасности, в силу низкой технической грамотности, не осознают важности защиты компьютерной информации. С другой стороны, IT-сотрудники, являясь «творческими» личностями, как правило, стараются игнорировать требования службы безопасности. Кардинально решить эту проблему можно было бы, введя должность CEO по информационной безопасности, которому бы подчинялись обе службы.

В политике безопасности не надо детализировать должностные обязанности каких бы то ни было сотрудников. Эти обязанности должны разрабатываться на основе политики, но не внутри нее.

Для защиты информации на предприятии OAO «Мобилка» разработана система защиты информации (СЗИ). Выделяют следующие элементы СЗИ:

* Организационный элемент ЗИ - включает регламентацию производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающую или ослабляющую нанесение, какого-либо ущерба исполнителям. На данном предприятии имеется шлагбаум при въезде на территорию, въезд осуществляется только по пропускам, на окнах первого этажа имеются решетки, ведется видеонаблюдение за всей территорией предприятия;
* Нормативно-правовой элемент ЗИ - это специальные законы, другие нормативные акты, правила, процедуры и мероприятия. Обеспечивающие защиту информации на правовой основе. На данном предприятии существуют: ветеринарно-санитарные правила, правила пожарной безопасности, правила внутреннего распорядка;
* Инженерно-технический элемент ЗИ - это использование различных инженерно-технических средств, препятствующих нанесению ущерба защищаемой информации;
* Программно-аппаратный элемент ЗИ - это все программные и автоматизированные системы обработки данных обеспечивающие сохранность и конфиденциальность информации.

## 2.2 Организационный элемент защиты информации на OAO «Мобилка»

Организационная защита информации на предприятии - регламентация производственной деятельности и взаимоотношений субъектов (сотрудников предприятия) на нормативно-правовой основе, исключающая или ослабляющая нанесение ущерба данному предприятию.

Организационная защита информации:

* Организация работы с персоналом;
* Организация внутриобъектового и пропускного режимов и охраны;
* Организация работы с носителями сведений;
* Комплексное планирование мероприятий по защите информации;
* Организация аналитической работы и контроля.
* Основные принципы организационной защиты информации:
* принцип комплексного подхода - эффективное использование сил, средств, способов и методов защиты информации для решения поставленных задач в зависимости от конкретной складывающейся ситуации и наличия факторов, ослабляющих или усиливающих угрозу защищаемой информации;
* принцип оперативности принятия управленческих решений (существенно влияет на эффективность функционирования и гибкость системы защиты информации и отражает нацеленность руководства и персонала предприятия на решение задач защиты информации);
* принцип персональной ответственности - наиболее эффективное распределение задач по защите информации между руководством и персоналом предприятия и определение ответственности за полноту и качество их выполнения.

Среди основных условий организационной защиты информации можно выделить следующие:

* непрерывность всестороннего анализа функционирования системы защиты информации в целях принятия своевременных мер по повышению ее эффективности;
* неукоснительное соблюдение руководством и персоналом предприятия установленных норм и правил защиты конфиденциальной информации.

При соблюдении перечисленных условий обеспечивается наиболее полное и качественное решение задач по защите конфиденциальной информации на предприятии.

Естественно организационные мероприятия должны четко планироваться, направляться и осуществляться службой информационной безопасности, в состав которой входят специалисты по безопасности.

Таким образом, элемент организационной защиты является основным элементом комплексной СЗИ и во многом от того, каким образом реализован организационный элемент, зависит безопасности организации.

## 2.3 Нормативно-правовой элемент защиты информации на предприятии OAO «Мобилка»

Как известно, право - это совокупность общеобязательных правил и норм поведения, установленных государством в отношении определенных сфер жизни и деятельности.

Правовой элемент системы организации защиты информации на предприятии OAO «Мобилка» основывается на нормах информационного права и имеет юридическое закрепление взаимоотношений фирмы и государства по поводу правомерности использования системы защиты информации, фирмы и персонала по поводу обязанности персонала соблюдать установленные меры защитного характера, ответственности персонала за нарушение порядка защиты информации.

Этот элемент включает:

* наличие в организационных документах фирмы, правилах внутреннего трудового распорядка, трудовых договорах, в должностных инструкциях положений и обязательств по защите конфиденциальной информации;
* формулирование и доведение до сведения всех сотрудников положения о правовой ответственности за разглашение конфиденциальной информации, несанкционированное уничтожение или фальсификацию документов;
* разъяснение лицам, принимаемым на работу, положения о добровольности принимаемых ими на себя ограничений, связанных с выполнением обязанностей по защите информации.

В числе основных подсистем защиты информации в правовом плане можно считать:

* установление на объекте режима конфиденциальности;
* разграничение доступа к информации;
* правовое обеспечение процесса защиты информации;
* четкое выделение конфиденциальной информации как основного объекта защиты.

Опираясь на государственные правовые акты на уровне OAO «Мобилка», разрабатываются собственные нормативно-правовые документы, ориентированные на обеспечение информационной безопасности.

К таким документам относятся:

* Политика Информационной безопасности;
* Положение о коммерческой тайне;
* Положение о защите персональных данных;
* Перечень сведений, составляющих конфиденциальную информацию;
* Инструкция о порядке допуска сотрудников к сведениям, составляющим конфиденциальную информацию;
* Положение о специальном делопроизводстве и документообороте;
* Обязательство сотрудника о сохранении конфиденциальной информации;
* Памятка сотруднику о сохранении коммерческой тайны.

Указанные нормативные акты направлены на предупреждение случаев неправомерного оглашения (разглашения) секретов на правовой основе, и в случае их нарушения должны приниматься соответствующие меры воздействия.

## 2.4 Инженерно-технический элемент защиты информации на OAO «Мобилка»

Инженерно-технический элемент защиты информации предназначен для пассивного и активного противодействия средствам технической разведки и формирования рубежей охраны территории, зданий, помещений и оборудования с помощью комплексов технических средств.

Организация охраны - составная часть общей системы защиты конфиденциальной информации предприятия. Вопросы обеспечения надежной охраны территории предприятия и его объектов неразрывно связаны с задачами организации пропускного режима на предприятии. Силы и средства, участвующие в решении этих задач, являются составными элементами системы охраны предприятия.

От эффективности функционирования системы охраны в полной мере зависят возможность и уровень решения задач пропускного и внутриобъектового режимов. Системы пропускного и внутриобъектового режимов образуют следующие после системы охраны рубежи безопасности, предотвращающие доступ злоумышленника к охраняемой предприятием информации.

Главные цели охраны OAO «Мобилка» следующие:

* предотвращение попыток проникновения посторонних лиц (злоумышленников) на территорию (объекты) предприятия;
* своевременное обнаружение и задержание лиц, противоправно проникших (пытающихся проникнуть) на охраняемую территорию;
* обеспечение сохранности находящихся на охраняемой территории носителей конфиденциальной информации и материальных средств и исключение, таким образом, нанесения ущерба предприятию;
* предупреждение происшествий на охраняемом объекте и ликвидация их последствий.

К основным объектам охраны относятся:

* территория предприятия;
* расположенные на территории предприятия объекты (здания, сооружения);
* носители конфиденциальной информации (документы, изделия);
* материальные ценности.

Особыми объектами охраны являются руководство предприятия персонал, допущенный к конфиденциальной информации. Организация охраны руководства и персонала предприятия регулируются отдельным положением, которое утверждается руководителем предприятия, и, в необходимых случаях согласовывается с территориальными органами внутренних дел и органами безопасности. Основные цели охраны руководства и перевала предприятия - обеспечение их личной безопасности в повседневных условиях и при возникновении чрезвычайных ситуаций, предотвращение возможных попыток завладения злоумышленниками защищаемой информацией путем физического и иного насильственного воздействия на этих лиц, выработка рекомендаций охраняемым лицам по особенностям поведения в различных ситуациях.

1. Политики информационной безопасности
   1. Политика предоставления доступа к информационному ресурсу

Настоящая Политика определяет основные правила предоставления сотрудникам доступа к защищаемым информационным ресурсам Управления.

К работе с информационным ресурсом допускаются пользователи, ознакомленные с правилами работы с информационным ресурсом и ответственностью за их нарушение, а также настоящей политикой.

Каждому сотруднику Управления, допущенному к работе с конкретным информационным ресурсом, должно быть сопоставлено персональное уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать в ИС.

В случае необходимости некоторым сотрудникам могут быть сопоставлены несколько уникальных имен (учетных записей). Использование несколькими сотрудниками при работе в Управлении одного и того же имени пользователя («группового имени») ЗАПРЕЩЕНО.

3.2 Политика учетных записей

Настоящая политика определяет основные правила присвоения учетных записей пользователям информационных активов компании.

Регистрационные учетные записи подразделяются на:

* пользовательские – предназначенные для идентификации/аутентификации пользователей информационных активов Управления;
* системные – используемые для нужд операционной системы;
* служебные – предназначенные для обеспечения функционирования отдельных процессов или приложений.

Каждому пользователю информационных активов Управления назначается уникальная пользовательская регистрационная учетная запись. Допускается привязка более одной пользовательской учетной записи к одному и тому же пользователю (например, имеющих различный уровень полномочий).

В общем случае запрещено создавать и использовать общую пользовательскую учетную запись для группы пользователей. В случаях, когда это необходимо, ввиду особенностей автоматизируемого бизнес-процесса или организации труда (например, посменное дежурство), использование общей учетной записи должно сопровождаться отметкой в журнале учета машинного времени, которая должна однозначно идентифицировать текущего владельца учетной записи в каждый момент времени. Одновременное использование одной общей пользовательской учетной записи разными пользователями запрещено.

Системные регистрационные учетные записи формируются операционной системой и должны использоваться только в случаях, предписанных документацией на операционную систему.

Служебные регистрационные учетные записи используются только для запуска сервисов или приложений.

Использование системных или служебных учетных записей для регистрации пользователей в системе категорически запрещено.

* 1. Политика архивирования, резервного копирования и восстановления данных

Требования к архивированию, резервному копированию и восстановлению данных определяется уровнем риска сервиса, требованием к доступности сервиса и устанавливаются следующие:

Режим работы сервиса Интернет круглосуточный, время восстановления 2 часа (не по вине провайдера, предоставляющего доступ к сети)

Режим работы электронной почты круглосуточный, время восстановления 4 часа (не по вине провайдера, предоставляющего доступ к сети)

Режим работы файлового архива круглосуточный, время восстановления 4 часа.

Режим работы системы по управлению предприятием круглосуточный, время восстановления 4 часа. Полное ежедневное копирование базы данных и хранение в течение 30 дней. 2 раза в год полное копирование и хранение в течение 5 лет.

* 1. Политика реализации антивирусной защиты

Настоящая Политика определяет основные правила для реализации антивирусной защиты в Управлении.

Антивирусная защита строится на трех уровнях АВЗ.

Первый уровень антивирусной защиты – уровень защиты сети Интернет – шлюза доступа (HTTP, FTP трафика).

Второй уровень антивирусной защиты – уровень защиты почтовых систем (SMTP/POP3 трафика).

Третий уровень антивирусной защиты – уровень защиты файловых серверов и рабочих станций.

Антивирусное программное обеспечение должно быть установлено, настроено и активировано на всех программно-технических средствах, имеющих доступ к информационным активам ОАО «Мобилка», до начала их использования или подключения к информационным ресурсам.

Все возможные каналы поступления вредоносного программного обеспечения в информационно-технологическую инфраструктуру организации должны быть определены, проанализированы и защищены средствами антивирусной защиты.

Контролю на предмет обнаружения вредоносных программ должна подвергаться вся информация, создаваема и обрабатываемая программно-техническими средствами ОАО «Мобилка», а также принимаемая (передаваемая) посредством сменных носителей информации и средствами телекоммуникаций.

С целью эффективной борьбы с новыми видами зловредного программного обеспечения и уменьшения накладных расходов на администрирование должно выполняться централизованное, регулярное обновление всех средств антивирусной защиты, используемых для защиты информационных систем организации.

Для эффективной реализации АВЗ ОАО «Мобилка», необходимо:

* унифицировать антивирусное программное обеспечение с возможностью централизованного управления
* постоянное, своевременное обновление антивирусных баз и программных компонентов

Реализацию данного пункта политики безопасности осуществляет системный администратор, контроль за исполнением обеспечивает заведующий отделом ИТ.

Любые информационные системы, используемые в ЛВС огранизации или подключаемые к ней как локально, так и удаленно, в ходе эксплуатации должны подвергаться непрерывному антивирусному мониторингу и сканированию. К таковым системам относятся сервера и рабочие станции ЛВС организации, а также мобильные и отдельные автономные автоматизированные рабочие места руководства, сотрудников организации, имеющие доступ к информационным активам организации.

* 1. Политика защиты АРМ

Настоящая Политика определяет основные правила и требования по защите персональных данных и иной конфиденциальной информации Управления от неавторизованного доступа, утраты или модификации.

Во время работы с конфиденциальной информацией должен предотвращаться ее просмотр не допущенными к ней лицами.

При любом оставлении рабочего места, рабочая станция должна быть заблокирована, съемные машинные носители, содержащие конфиденциальную информацию, заперты в помещении, шкафу или ящике стола или в сейфе.

Несанкционированное использование печатающих, факсимильных, копировально-множительных аппаратов и сканеров должно предотвращаться путем их размещения в помещениях с ограниченным доступом, использования паролей или иных доступных механизмов разграничения доступа.

Сотрудники получают доступ к ресурсам вычислительной сети после ознакомления с документами, утвержденными стандартами Управления, (согласно занимаемой должности), а именно с инструкциями по обращению с носителями конфиденциальной информации, «Перечень сведений конфиденциального характера».

Доступ к компонентам операционной системы и командам системного администрирования на рабочих станциях пользователей ограничен. Право на доступ к подобным компонентам предоставлено только администратор информационной безопасности. Конечным пользователям предоставляется доступ только к тем командам, которые необходимы для выполнения их должностных обязанностей.

Доступ к информации предоставляется только лицам, имеющим обоснованную необходимость в работе с этими данными для выполнения своих должностных обязанностей.

Пользователям запрещается устанавливать неавторизованные программы на компьютеры.

Конфигурация программ на компьютерах должна проверяться ежемесячно на предмет выявления установки неавторизованных программ.

Техническое обслуживание должно осуществляться только на основании обращения пользователя к системному администратору.

Локальное техническое обслуживание должно осуществляться только в личном присутствии пользователя.

Дистанционное техническое обслуживание должно осуществляться только со специально выделенных автоматизированных рабочих мест, конфигурация и состав которых должны быть стандартизованы, а процесс эксплуатации регламентирован и контролироваться.

При проведении технического обслуживания должен выполняться минимальный набор действий, необходимых для устранения проблемы, явившейся причиной обращения, и использоваться любые возможности, позволяющие впоследствии установить авторство внесенных изменений.

Копирование конфиденциальной информации и временное изъятие носителей конфиденциальной информации (в том числе в составе АРМ) допускаются только с санкции пользователя. В случае изъятия носителей, содержащих конфиденциальную информацию, пользователь имеет право присутствовать при дальнейшем проведении работ.

Программное обеспечение должно устанавливаться со специальных ресурсов или съемных носителей и в соответствии с лицензионным соглашением с его правообладателем.

Конфигурации устанавливаемых рабочих станций должны быть стандартизованы, а процессы установки, настройки и ввода в эксплуатацию - регламентированы.

АРМ, на которых предполагается обрабатывать конфиденциальную информацию, должны быть закреплены за соответствующими сотрудниками Предприятия. Запрещается использование указанных АРМ другими пользователями без согласования с администратором информационной безопасности Предприятия. При передаче указанного АРМ другому пользователю, должна производиться гарантированная очистка диска (форматирование).

Системный администратор вправе отказать в устранении проблемы, вызванной наличием на рабочем месте программного обеспечения или оборудования, установленного или настроенного пользователем в обход действующей процедуры.

## 3.6 Политика пользования электронной почтой

Электронная почта – используется только для выполнения работником его служебных обязанностей

Единственно возможный способ работы с электронной почтой в ОАО «Мобилка» – использование корпоративной электронной почты. Работа с другими сервисами электронной почты, включая, но не ограничиваясь, бесплатными почтовыми серверами, только при согласовании с системным администратором организации.

Запрещается рассылка цепных сообщений, спама, исполняемых файлов, файлов развлекательного характера.

Запрещается использовать корпоративную электронную почту для любой деятельности с целью получения личной материальной выгоды.

Запрещается пересылка и получение электронной почты, содержащей лицензионное программное обеспечение и другие действия, позволяющие обойти лицензионные соглашения или нарушить авторские права

Запрещается посылать письма, содержащие информацию, составляющие коммерческую тайну ОАО «Мобилка». Исключения составляют пользователи, имеющие на это право в соответствии с положением «О коммерческой тайне»

## 3.7. Методы и механизмы защиты в глобальной сети.

На предприятии ОАО «Мобилка» используются различные механизмы защиты в глобальной сети:

* Оконечное шифрование.

В глобальной сети ОАО «Мобилка» должен использоваться механизм оконечного шифрования, который позволяет обеспечивать конфиденциальность данных, передаваемых между двумя прикладными объектами. Другими словами, отправитель зашифровывает данные, получатель - расшифровывает.

* Криптографическая защита данных.

Защита конфиденциальных данных, передаваемых между двумя прикладными объектами, с помощью криптографических преобразований (преобразование данных шифрованием и выработкой имитовставки) - одно из возможных решений проблемы их безопасности. Криптографическая защита данных представляет собой шифрование данных с целью скрыть их смысл. До тех пор, пока пользователь не идентифицирован по ключу, смысл данных ему не доступен.

Зашифрованные данные становятся доступными для того, кто знает ключ, и поэтому похищение зашифрованных данных абсолютно бессмысленно для несанкционированных пользователей.

* Механизмы цифровой подписи.

Механизмы цифровой подписи, которые включают процедуры закрытия блоков данных и проверки закрытого блока данных.

* Электронная цифровая подпись (ЭЦП).

ЭЦП позволяет заменить при безбумажном документообороте традиционные печать и подпись. Цифровая подпись не имеет ничего общего с последовательностью символов, соответствующих печати или подписи, приписанной к документу. При построении подписи вместо обычной связи между печатью или рукописной подписью и листом бумаги выступает сложная математическая зависимость между документом, секретным и общедоступным ключом, а также цифровой подписью. Невозможность подделки ЭЦП опирается на очень большой объём необходимых математических вычислений.

* Механизм контроля доступа.

Осуществляют проверку полномочий сетевого объекта на доступ к ресурсам.

Контроль должен осуществиться при доступе к:

* + оперативной памяти;
  + разделяемым устройствам прямого доступа;
  + разделяемым устройствам последовательного доступа;
  + разделяемым программам и подпрограммам;
  + разделяемым наборам данных.

Основным объектом внимания средств контроля доступа являются используемые наборы данных и ресурсы системы.

* Механизм обеспечения целостности передаваемых данных.

Этот механизм обеспечивает как целостность отдельного блока или поля данных, так и потока данных. Целостность блока данных обеспечивается передающим и принимающим объектами. Передающий объект добавляет к блоку данных признак, значение которого является функцией от самих данных. Принимающий объект также вычисляет эту функцию и сравнивает её с полученной.

* Механизм аутентификации объектов сети.

Для обеспечения аутентификации используются пароли, проверка характеристик объекта, криптографические методы (аналогичные цифровой подписи).

При входе в систему и вводе имени пользователя осуществляется идентификация, при вводе пароля - аутентификация и, если пользователь с данным именем и паролем зарегистрирован в системе, ему разрешается доступ к определённым объектам и ресурсам (авторизация). Однако, при входе в систему существуют отличия при выполнении этих функций. Они обусловлены тем, что в процессе работы система уже имеет информацию о том, кто работает, какие у него полномочия (на основе информации в базе данных защиты) и т.д. и поэтому может адекватно реагировать на запросы субъекта. При входе в систему это всё только предстоит определить. В данном случае возникает необходимость организации «достоверного маршрута» - пути передачи идентифицирующей информации от пользователя к ядру безопасности для подтверждения подлинности. Как показывает практика, вход пользователя в систему - одно из наиболее уязвимых мест защиты: известно множество случаев взлома пароля, входа без пароля, перехват пароля и т.д. Поэтому при входе и пользователь, и система должны быть уверены, что они работают непосредственно друг с другом, между ними нет других программ и вводимая информация истинна.

## Заключение

В последнее время стремительно быстро развиваются новые технологии, так же быстро и появляются новые устройства, методы для кражи информационных ресурсов. У любого предприятия, дорожащего своей репутацией и прибылью, должна быть чётко сформирована система защиты, как информации, так и предприятия в целом. На таком предприятии, как ОАО «Мобилка» утечка данных может привести не только к краху корпорации, но и нанести ущерб клиентам компании, так как в автоматизированной системе организации находятся персональные данные клиентов, включающие паспортные данные, которые должны храниться в секрете от посторонних лиц.

Но, несмотря на всё, в практике компании ОАО «Мобилка» за всю историю существования не было несчастных случаев, связанных с утечкой информации. Даже, несмотря на то, что компания имеет филиалы по всей Европе и связана общей сетью, насчитывает тысячи сотрудников, информация надёжно защищена от несанкционированного доступа.

## Список используемой литературы

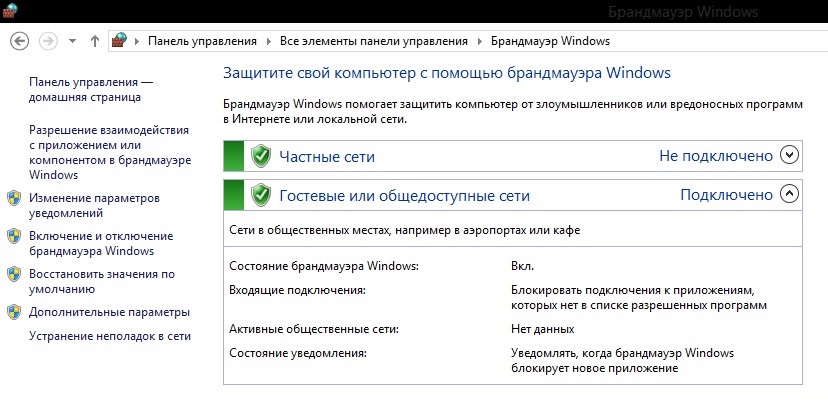
1. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных: Руководящий документ ФСТЭК России 15.02.2008 г. - М.: ГТК РФ, 2008. - 55 с.
2. ГОСТ Р 53110-2008. Система обеспечения информационной безопасности сети связи общего пользования. Общие положения. Введ. 2008 - 03 - 03.: Изд-во стандартов, 2008. - 32 с.
3. Концепция защиты персональных данных в информационных системах персональных данных оператора связи: Концепция от 15 апреля 2009 г. №15 ICU-15-2009-K // Собрание законодательства Российской Федерации. - 2009. - 609 с.
4. Котиков И. Пространство технологий абонентского доступа для оператора связи / И. Котиков // Технологии и средства связи 2008. - №1. - С. 46 - 511
5. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных: Руководящий документ ФСТЭК России 14.02.2008 г. - М.: ГТК РФ, 2008. - 73 с.
6. Мельников Д.А. Информационные процессы в компьютерных сетях / Д.А. Мельников - М.: Кудиц-Образ, 2001. - 250 с.
7. Об информации, информатизации и защите информации Федеральный Закон от 25.01.95 №24-ФЗ // Собрание законодательства Российской Федерации. - 2005. - 609
8. О связи: Федеральный закон от 07.07.2003 №126-ФЗ // Собрание законодательства Российской Федерации. - 2004. - №32. - Ст. 3283.
9. Костров Д.А. Информационная безопасность ЦОД: подходы [Электронный ресурс] // Интернет-журнал Information Security. - 2009. < http://www.itsec.ru/articles2/Oborandteh/>

**Практическое занятие №4**

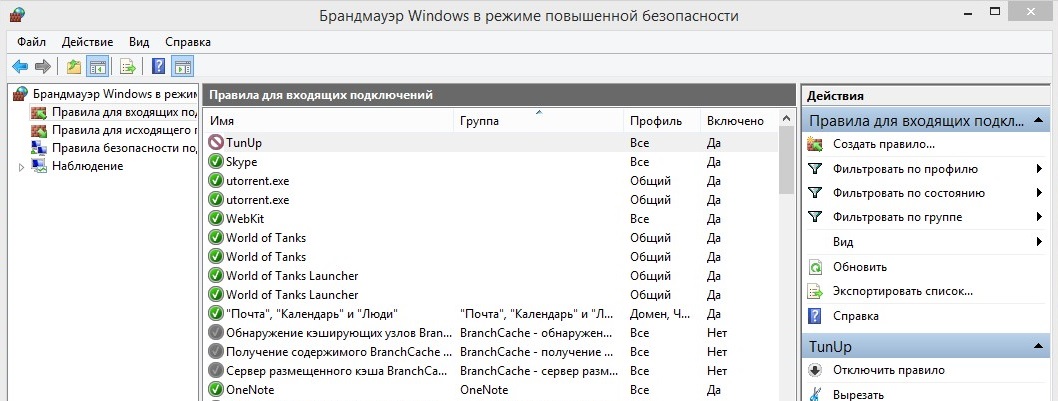
**Тема «**Настройка Брандмауэра Windows**»**

**Выполнение**

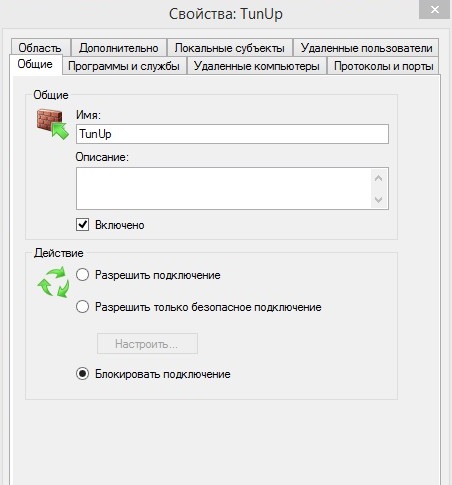
* + 1. Открыли брандмауэр и включили его.



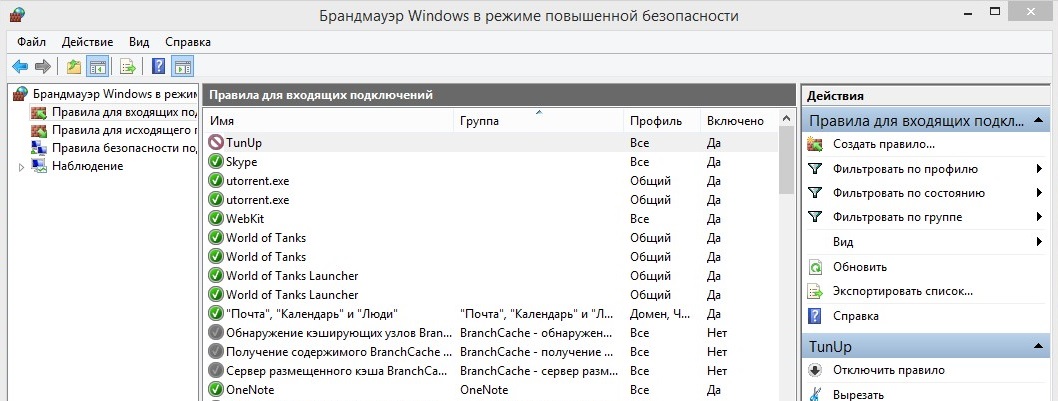
* + 1. Создали правило для входящих подключений запрещающее любой доступ программы TuneUp к сети.



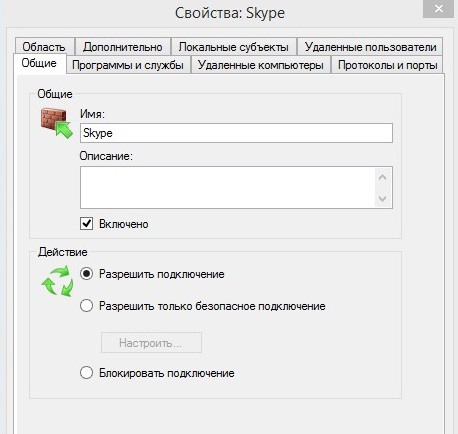
* + 1. Окно свойств правила.



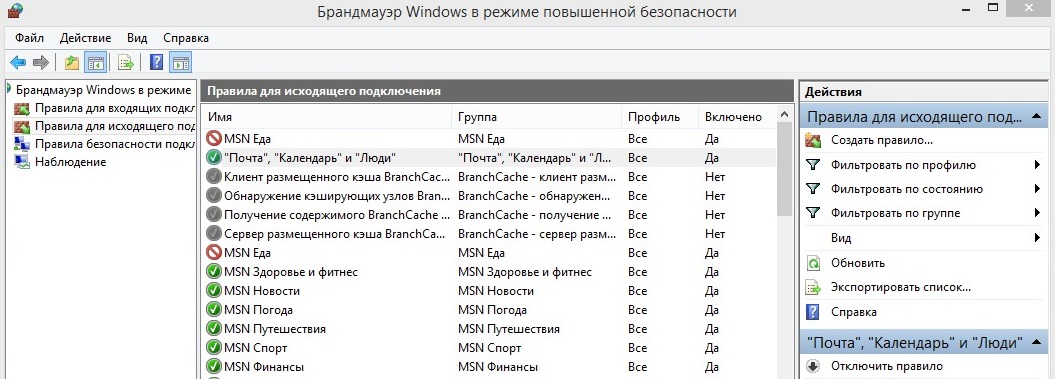
* + 1. Создали правило для всех входящих подключений разрешающее доступ программы Skype для всех подключений.



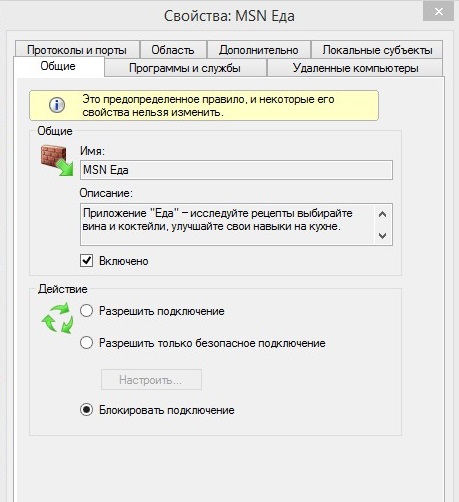
* + 1. Окно свойств правила.



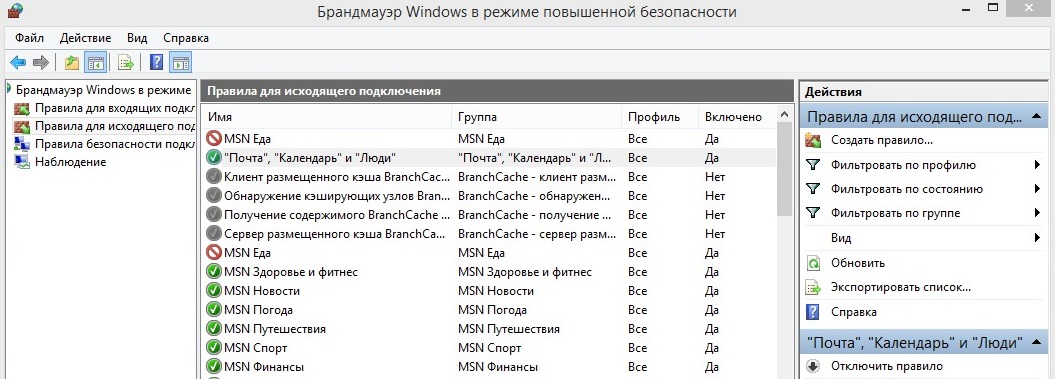
* + 1. Создали правило для всех исходящих подключений запрещающее доступ программы MSN Еда для всех подключений.



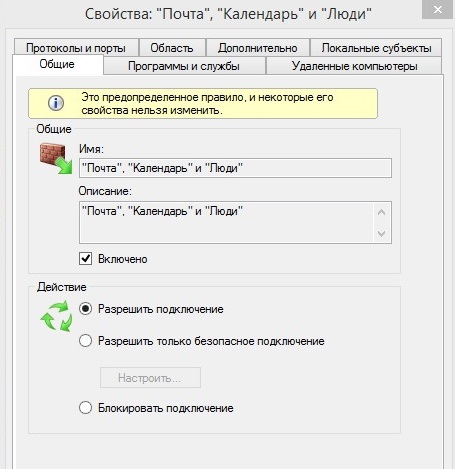
* + 1. Свойство правила MSN Еда



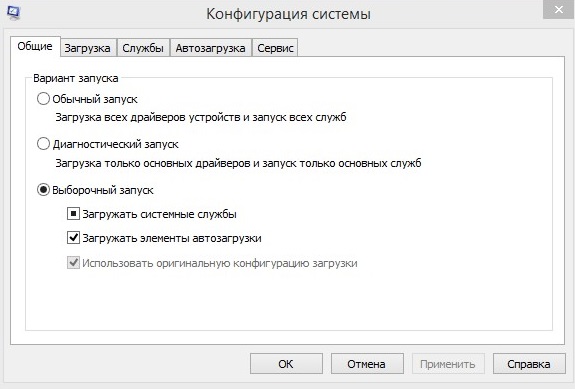
* + 1. Создали правило для всех исходящих подключений разрешающее доступ программы Почта, Календарь и Люди для всех подключений.



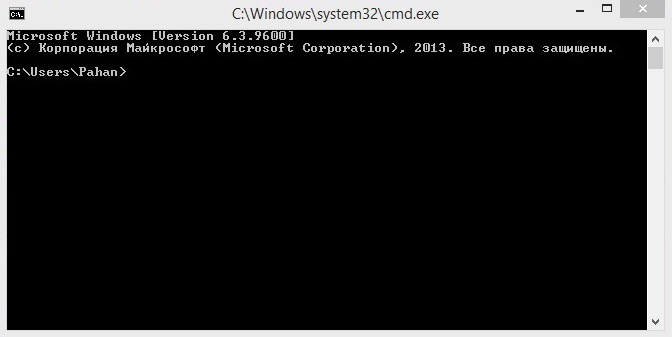
* + 1. Окно свойств правила Почта, Календарь и Люди



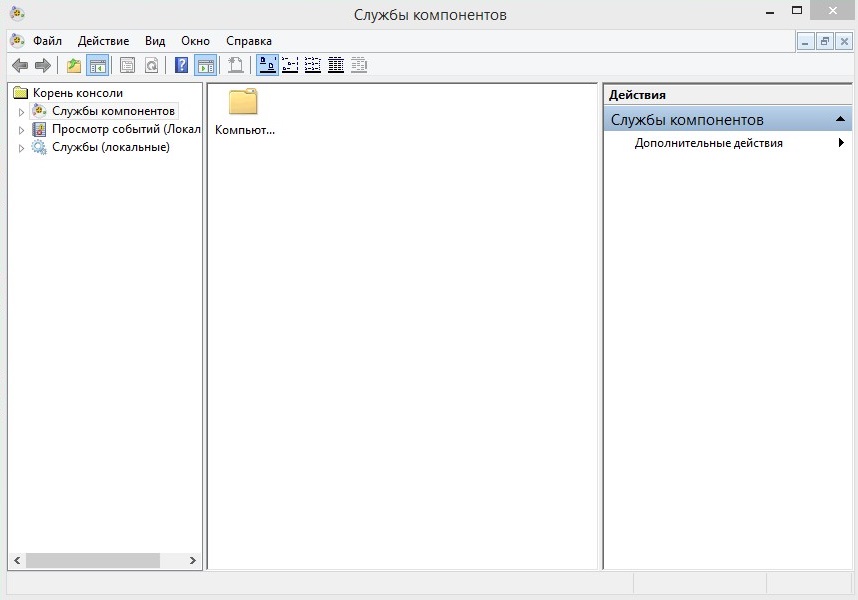
* + 1. Вернул настройки Брандмауэра в исходное состояние до начала выполнения практического задания.
    2. Опробовал команды администратора msconfig



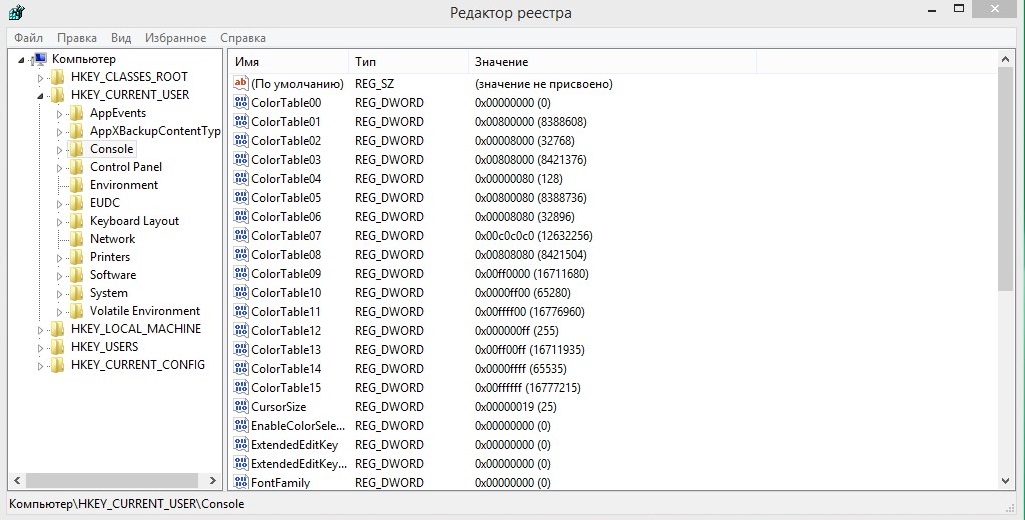
Cmd



Dcomcnfg



Regedit



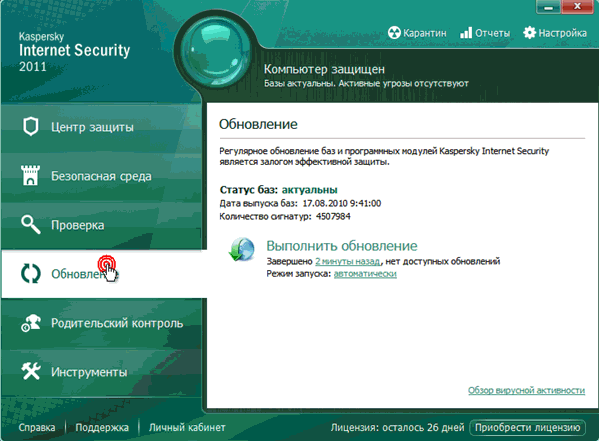
**Вывод**: в процессе выполнения задания ознакомились с брандмауэром Windows, его функциями и попробовали в действии команды администратора.

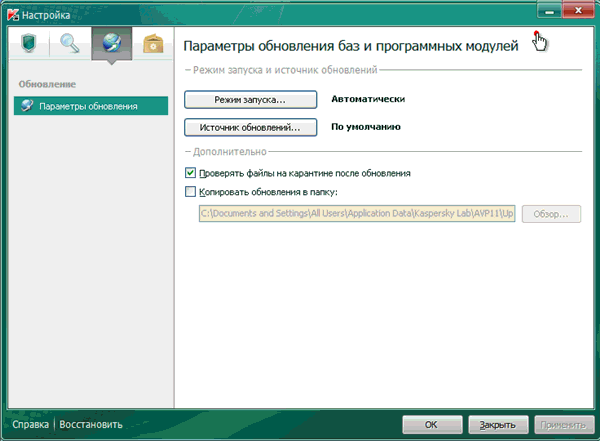
**Практическое занятие №5**

Настройка антивирусов

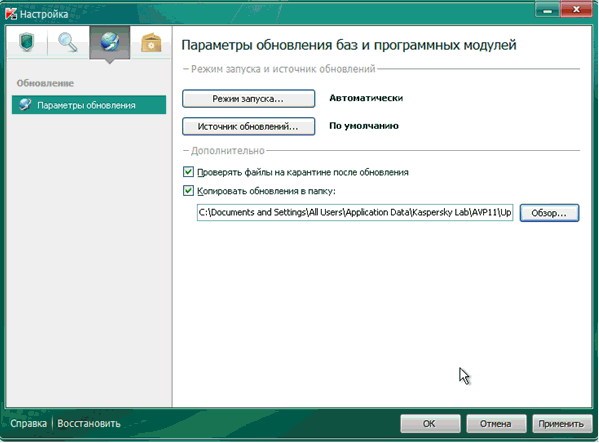
1. Настроить режим фильтрации файервола антивируса (один из описанных в теоретическом введении).
2. Настроить **Оффлайн обновление сигнатур угроз из локальной папки**

Для того чтобы выполнить обновление из папки нужно выполнить действия:

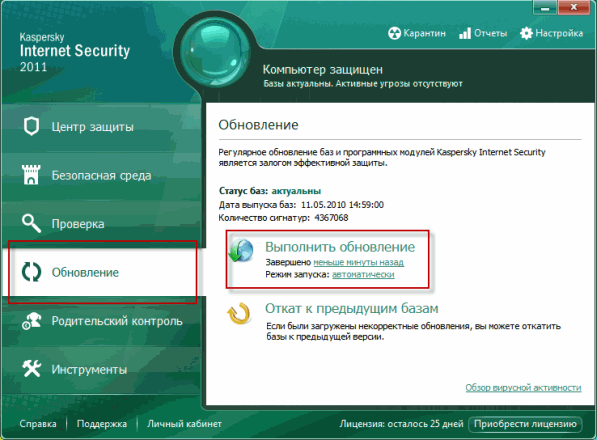
1. Открыть главное окно программы
2. В левой части окна **Kaspersky Internet Security** выбираем раздел **Обновление.**
3. 
4. В правом верхнем углу окна **Kaspersky Internet Security** нажимаем на ссылку **Настройка.**



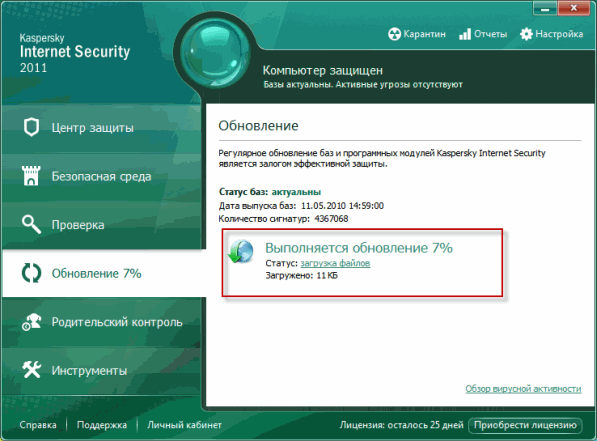
1. В правой части окна в блоке **Дополнительно** ставим флажок **Копировать обновления в папку.**
2. Нажимаем на кнопку **Обзор**, если необходимо указать папку для баз отличную от папки по умолчанию.



1. Настроить **Оффлайн обновление сигнатур угроз из локального сервера**
   1. В главном окне программы переходим на закладку **Обновление**
   2. Нажимаем кнопку **Выполнить обновление**



* 1. Дожидаемся окончания обновления.



**Вывод**: овладели навыками работы с антивирусом Kaspersky Internet Security 2011 и опробовали различные функции (локальное обновление и отключение фаервола).

**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.

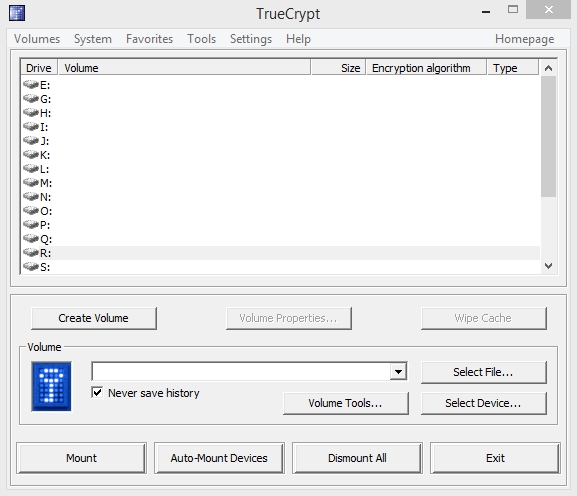
**Порядок работы с программой TrueCrypt**

**Этап  1:**

Установили программу TrueCrypt

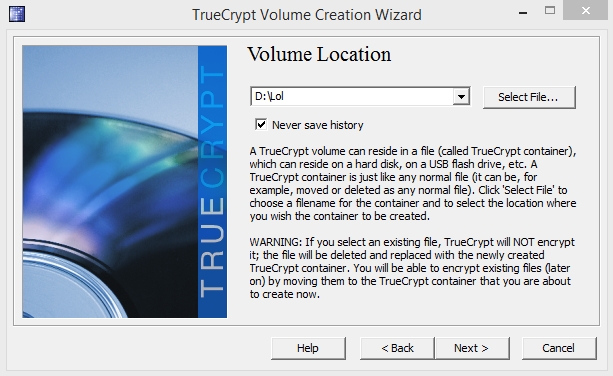
**Этап  2:**

Запустили программу TrueCrypt



**Этап 3:**

Создали раздел и прописали путь к нему



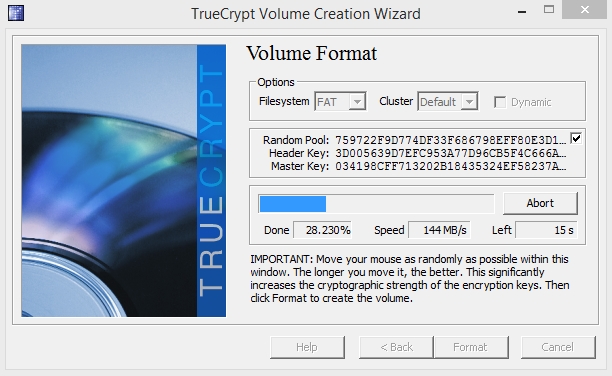
**Этап 4:**

Выбрали алгоритм шифрования и определились с паролем



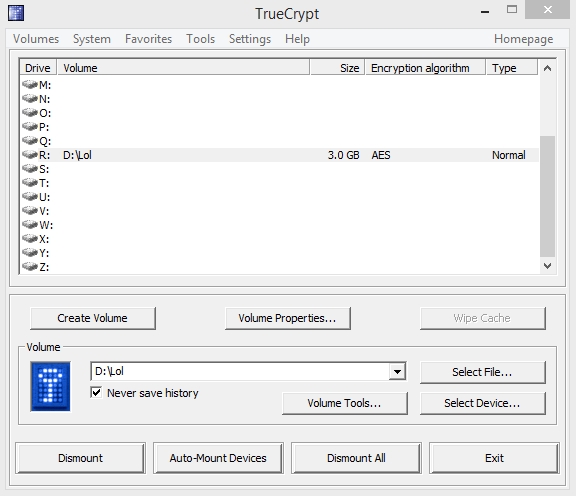
**Этап 5:**

Для увеличения криптографических свойств ключей мы водили мышью по экрану в случайном порядке.



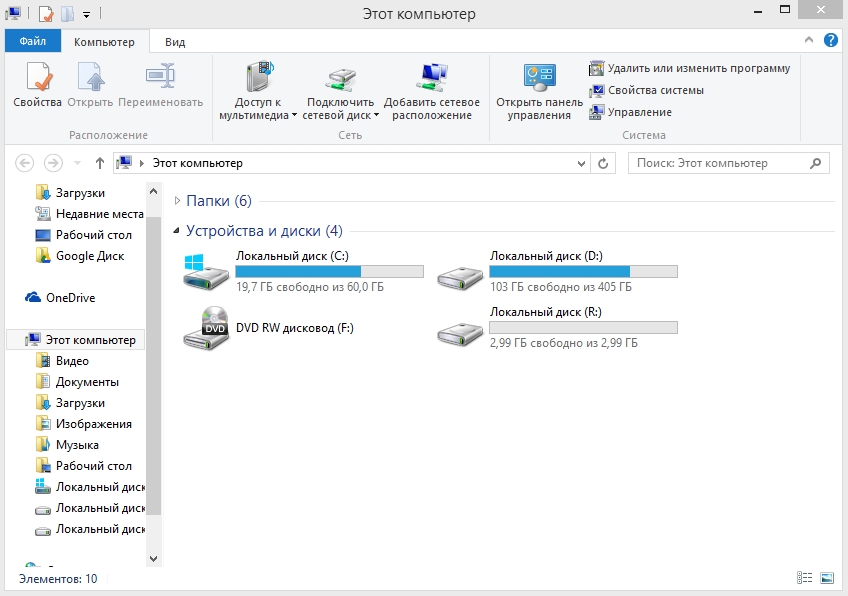
**Этап 6:**

Выбрали имя диска к которому примонтировали наш контейнер и ввели пароль в нашему контейнеру.



**Этап 7:**

Появился новый раздел



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

**Практическое занятие №7**

**Тема «Криптографическая защита информации»**

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

**Теоретическое введение**

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

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

Помимо этого современная криптография включает в себя асимметричные криптосистемы, системы электронной цифровой подписи, хеш-функции, управление ключами, получение скрытой информации, квантовую криптографию.

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

В англоязычной литературе зашифрование / расшифрование – enciphering / deciphering.

Классификация алгоритмов шифрования

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

1.1. Потоковые:

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

· с конечным ключом;

· на основе генератора псевдослучайных чисел.

1.2. Блочные:

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

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

· моноалфавитные;

· полиалфавитные;

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

· Диффи-Хеллман DH (Diffie, Hellman);

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

· Эль-Гамаль (ElGamal).

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

Обмен информацией осуществляется в 3 этапа:

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

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

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

· шифры перестановки (transposition, permutation, P-блоки);

· шифры замены (подстановки, substitution, S-блоки).

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

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

· моноалфавитные (код Цезаря);

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

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



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

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

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

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

Схема обмена информацией такова:

· получатель вычисляет открытый и секретный ключи, секретный ключ хранит в тайне, открытый же делает доступным (сообщает отправителю, группе пользователей сети, публикует);

· отправитель, используя открытый ключ получателя, зашифровывает сообщение, которое пересылается получателю;

· получатель получает сообщение и расшифровывает его, используя свой секретный ключ.

**Алгоритм Диффи-Хелмана**

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

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

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

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

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

**Генерация секретного ключа методом Диффи-Хелмана:**

Ева — криптоаналитик. Она читает пересылку Боба и Алисы, но не изменяет содержимого их сообщений.

g = открытое простое число. g = 7

p = открытое простое число. p = 13

a = секретный ключ Алисы. a = 18

A = открытый ключ Алисы. A = ga mod p

A = 718 mod 13 = 12

b = секретный ключ Боба. b = 10

B = открытый ключ Боба. B = gb mod p

B = 710 mod 13 = 4

S = секретный ключ.

S = Ba mod p

S = 418 mod 13 = 1

**Шифр Цезаря**

Зашифруем слово «хочузачетавтоматом» с помощью шифра Цезаря с ключом 5

А а Б б В в Г г Д д Е е Ё ё Ж ж З з И и Й й К к Л л М м

Н н О о П п Р р С с Т т У у Ф ф Х х Ц ц Ч ч Ш ш Щ щ Ъ ъ

Ы ы Ь ь Э э Ю ю Я я

Первая буква заменяется на букву, отстоящую от нее в латинском алфавите на некоторое число позиций. В данном случае на 5.

И получим «ъуьшмеьйчежчусечус».

Вывод: Овладели навыками работы с компьютерными программами для криптографической защиты информации при передаче и хранении.

**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 относи-тельно 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 pасшифpовать принятое сообщение.

**Пример**

1. Пусть требуется зашифровать сообщение “САВ”.
2. Для простоты будем использовать маленькие числа (на практике применяются гораздо большие). Пошагово проследим процессы шифрования и дешифрования.
3. Выберем p = 3 и q = 11.
4. Определим n = 3 \* 11 = 33.
5. Найдем (p – 1)(q – 1) = 20. Следовательно, в качестве e можно взять число, взаимно простое с 20, напpимеp, e = 3.
6. Выберем число d. * d = e-1mod((p-1)(q-1)).* В качестве такого числа может быть взято любое число, для которого выполняется соотношение (d \* 3) = 1(mod 20), напpимеp 7.
7. Представим шифруемое сообщение как последовательность целых чисел с помощью отображения: А -> 1, В-> 2, С-> 3. Тогда исходное открытое сообщение принимает вид M = (3,1,2). Зашифруем сообщение с помощью ключа {7, 33}:
8. s1 = (3 в степени 7) (mod 33) = 2187 (mod 33) = 9,
9. s2 = (1 в степени 7) (mod 33) = 1 (mod 33) = 1,
10. s3 = (2 в степени 7) (mod 33) = 128 (mod 33) = 29.
11. Зашифрованное сообщение после этого примет вид S = (9, 1, 29).
12. Расшифруем полученное зашифрованное сообщение (9, 1, 29) на основе секретного ключа {3, 33}:
13. m1 = (9 в степени 3) (mod 33) = 729 (mod 33) = 3,
14. m2= (1 в степени 3) (mod 33) = 1 (mod 33) = 1,
15. m3 = (29 в степени 3) (mod 33) = 24389 (mod 33) = 2.
16. Как можем видеть, дешифрование шифртекста S = (9, 1, 29) привело к исходному открытому тексту M = (3, 1, 2).

**Выполнение**

1. Требуется зашифровать сообщение “BBB”.
2. Выберем p = 37 и q = 67.
3. Определим n = 37 \* 67 = 2479.
4. Найдем (p – 1)(q – 1) = 2376, e = 1.
5. Выберем число d. * d = e-1mod((p-1)(q-1)).*В качестве такого числа может быть взято любое число, для которого выполняется соотношение

(d \* 1) (mod 2376), = 1 напpимеp 2377.

1. Представим шифруемое сообщение как последовательность целых чисел с помощью отображения: А -> 1, В-> 2, С-> 3. Тогда исходное открытое сообщение принимает вид M = (2,2,2). Зашифруем сообщение с помощью ключа {1, 2377}:
2. s1 = (1 в степени 1) (mod 2377) = 2 (mod 2377) = 2,
3. s2 = (1 в степени 1) (mod 2377) = 2 (mod 2377) = 2,
4. s2 = (1 в степени 1) (mod 2377) = 2 (mod 2377) = 2,
5. Зашифрованное сообщение после этого примет вид S = (2, 2, 2).
6. Расшифруем полученное зашифрованное сообщение (2, 2, 2) на основе секретного ключа {1, 2377}:
7. m1 = (2 в степени 2) (mod 2377) = 2 (mod 2377) = 2,
8. m2= (2 в степени 2) (mod 2377) = 2 (mod 2377) = 2
9. m3= (2 в степени 2) (mod 2377) = 2 (mod 2377) = 2
10. Как можем видеть, дешифрование шифртекста S = (2, 2, 22) привело к исходному открытому тексту M = (2, 2, 2).

Вывод: Овладели навыками работы с известными криптографическими алгоритмами.

**Практическое занятие №9**

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

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

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

Авторское право распространяется 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- фаж дан других государств (и их правопреемников), обнародованные (либо необнародованные, но находящиеся в какой-либо объективной форме) за пределами РБ - в соответствии с международными договорами РБ.

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

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

Личные неимущественные права:

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

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

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

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

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

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

Авторское право на составные произведения:

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

1. **Каков срок действия авторского права?**

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

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

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

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

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

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

Но недееспособные, став субъектами авторского права, не 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.

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

Если произведение обнародовано либо не обнародовано, но существует на территории РБ в какой-либо объективной форме, то авторское право распространяется на такое произведение независимо от гражданства автора.

За гражданами других государств, обнародовавшими свои произведения за пределами РБ, авторское право признается в соответствии с международными договорами РБ.

Лицо, обозначенное в качестве автора на оригинале или экземпляре произведения, считается его автором, если отсутствует доказательство иного.

При обнародовании произведения анонимно или под псевдонимом (за исключением случаев, когда псевдоним автора не вызывает сомнения в его личности), издатель имя или наименование которого обозначено на произведении, при отсутствии доказательств иного, считается представителем автора и имеет право защищать права автора и обеспечивать их осуществление. Это положение действует до тех пор, пока автор не раскроет свою личность и не заявит о своем авторстве.

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

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

Недействительным является соавторство, навязанное автору лицам, от которого так или иначе зависит использование произведения.

Оказание автору технической помощи соавтора не порождает. При соавторстве должно быть творческое участие лиц в создании произведения.

В юридической литературе выделяют два вида соавторства: нераздельное и раздельное.

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

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

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

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

Особенности наследования авторских прав следующие:

Прежде всего, по наследству к наследникам переходят не все авторские права, а только их часть. В законе указывается, что по наследству не переходят право авторства, право на авторское имя и право на защиту репутации автора.

Однако и в отношении этих прав к наследникам переходят нрава на защиту названных прав от нарушений со стороны третьих лиц, если только автор не назначил для этих целей специальное лицо.

В отличие от прав на произведения самих авторов, которые носят пожизненный характер, авторские права наследников ограничены установленным законом сроком. Авторские права наследников действуют в течение 50 лет после смерти автора, считая с 1 января года, следующего за годом смерти.

Из этого общего правила есть ряд исключений:

а) если произведение создано в соавторстве, то 50-летний срок исчисляется после смерти последнего из соавторов;

б) если произведение впервые выпущено в свет после смерти автора, то авторское право действует в течение 50 лет после выпуска его в свет;

в) если автор был репрессирован и реабилитирован посмертно, то произведение охраняется 50 лет после реабилитации;

г) если автор воевал или работал во время Великой Отечественной войны, то срок охраны увеличивается на четыре года и т.д.

Важной особенностью наследования авторских прав является то, что авторские нрава переходят к наследнику в бездолевом порядке, как единое целое, не подлежащее ни выделу, ни разделу. Это означает, что распоряжаться перешедшими по наследству авторскими правами наследники должны совместно и по взаимному согласию, а в случае спора - по решению суда.

Помимо наследников авторские права могут переходить к иным правопреемникам. В их роли выступают издательства, театры киностудии и другие организации, занимающиеся использованием произведений. Они приобретают авторские права на основании заключенных с авторами и наследниками авторских договоров.

Становясь обладателями авторских прав, эти организации используют произведения и распоряжаются ими такими способами, которые предусмотрены конкретными авторскими договорами, и в установленных ими пределах.

Субъекты смежных прав: исполнители, производители фонограмм, организации эфирного или кабельного вещания.

Сфера действия смежных прав: исполнители граждане и не граждане РБ, исполнения которых имеют место на территории РБ, или включены в фонограммы, или не записаны на стенограмму, но содержатся в передачах организаций эфирного или кабельного вещания, охраняемые в соответствии с Законом.

Права исполнителя: на имя; на защиту репутации; на использование исполнения в любой форме, включая право на получение вознаграждения за каждый вид использования исполнения.

Исключительное право на использование: передавать в эфир или сообщать для всеобщего сведения по кабелю исполнение; записывать ранее не записанное исполнение; воспроизводить запись исполнения; передавать в эфир или по кабелю запись исполнения; распространять оригинал или экземпляры исполнения, записанного на фонограмму; сдавать в прокат оригинал или экземпляры записанного на фонограмму исполнения; сообщать для всеобщего сведения исполнение, записанное на фонограмму, по проводам или средствами беспроволочной связи.

Права производителя фонограммы: на использование ее в любой форме, включая право на получение вознаграждения за каждый вид использования фонограммы: воспроизводство; переработку; распространение; импортирование; сдача в прокат; доведение до всеобщего сведения.

Использование фонограммы, опубликованной в коммерческих целях: публичное исполнение фонограммы; передача фонограммы в эфир; иное сообщение фонограммы для всеобщего сведения.

Права организаций эфирного вещания.

Права организаций кабельного вещания.

Ограничения прав исполнителей, производителей фонограмм, организаций эфирного или кабельного вещания.

Допускается воспроизведение фонограмм: для включения в обзор о текущих событиях отрывков из исполнения, фонограммы, передачи организации эфирного или кабельного вещания; исключительно в целях обучения или научного исследования; для цитирования в форме отрывков из исполнения.

Защита авторского права и смежных прав в установленном порядке в судебных и других органах в соответствии с их компетенцией.

Способы обеспечения исков по делам о нарушении авторского права и смежных прав через суд: определение о запрещении, о наложении ареста и изъятии.

Коллективное управление имущественными правами обладателей авторского права и смежных прав в случаях, когда их трудно практически осуществить в индивидуальном порядке, могут осуществлять организации, порядок создания и деятельности которых определяется законодательством РБ.

1. **Что такое авторский договор?**

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

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

В зависимости от степени готовности произведения выделяют:

1) авторский договор заказа;

2) авторский договор на готовое произведение.

Также выделяют:

1) авторский договор на обнародованное произведение;

2) авторский договор на необнародованное произведение.

В зависимости от характера передаваемых прав выделяют:

1) авторский договор о передаче исключительных прав;

2) авторский договор о передаче неисключительных прав.

В зависимости от способа использования произведения выделяют:

1) издательский авторский договор;

2) постановочный авторский договор;

3) сценарный авторский договор;

4) авторский договор о депонировании рукописи;

5) авторский договор художественного заказа;

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

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

1. **Основные составляющие авторского договора?**

В авторском договоре должны быть предусмотрены:

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

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

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

Немаловажное значение имеет соглашение о размере вознаграждения.

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

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

Важными элементами, например, в договоре заказа с участием иностранных лиц, будут условия, определяющие:

* аванс, размер которого определяется соглашением;
* язык, на котором будет написано произведение;
* порядок представления [рукописи](http://baza-referat.ru/%D0%A0%D1%83%D0%BA%D0%BE%D0%BF%D0%B8%D1%81%D1%8C)(полностью или частями);
* примерный объем произведения, который может быть определен в границах «от — до»;
* жанр;
* композицию;

—название и др.

Срок создания и представления произведения автором по договору заказа имеет важное значение. Помимо этого стороны предусматривают сроки для устранения замечаний, сроки рассмотрения представленного произведения.

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

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

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

**Практическое занятие №10**

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

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

1. **Основные составляющие описания изобретения?**

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

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

1. **Правила оформления описания изобретения?**

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

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

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

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

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

Особенности изложения описания устройства

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

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

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

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

Особенности изложения описания способа

Сведение подтверждающие возможность описания изобретения относящегося к способу включают указания на последовательность действий (приемов, операций) над материальным объектом, а также на условия проведения действий, конкретные режимы (температура, давление и т. д.), используемые при этом устройства.

Если в формуле изобретения в качестве отличительных признаков приведены параметры режима, например указан интервал температуры нагревания, и этот интервал сравнительно велик от -20 до +60°С, то следует привести конкретные обоснования граничных значений интервала и привести по одному примеру на оптимальный и граничные значения этого интервала с подробным указанием достигаемого технического результата. Если интервал параметров режима не велик, то достаточно привести один пример с оптимальным параметром. При отсутствии параметров режима приводится один пример.

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

Заявка подается в трех экземплярах и должна содержать:

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

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

Вместе с заявкой или не позднее 2-х месяцев с даты ее подачи в одном экземпляре предоставляется документ, подтверждающий уплату пошлины в установленном размере или освобождение от уплаты, либо наличие оснований для уменьшения ее размера.

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

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

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

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

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

Алгоритм патентования:

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

Рассмотрим подробно каждый из перечисленных этапов, хотя их содержание не всегда можно четко разграничить.

1. **На какие ОПС выдаются патенты?**

Изобретению может быть предоставлена правовая охрана, если оно:

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

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

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

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

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

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

Не признаются патентоспособными:

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

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

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

Товарным знаком и знаком обслуживания (далее — товарный знак) признается обозначение, способствующее отличию товаров или услуг одного лица от однородных товаров или услуг других лиц. Правовая охрана товарного знака на территории Республики Беларусь осуществляется на основании его регистрации в патентном органе в порядке, установленном законодательством о товарных знаках и знаках обслуживания, или в силу международных договоров Республики Беларусь.  
Право на товарный знак охраняется государством и удостоверяется свидетельством. Свидетельство на товарный знак удостоверяет приоритет товарного знака, исключительное право владельца на товарный знак в отношении товаров, указанных в свидетельстве, и содержит изображение товарного знака. Владелец товарного знака имеет исключительное право использовать товарный знак и распоряжаться им, а также право запрещать использование товарного знака другим лицам. Географическим указанием признается обозначение, которое идентифицирует товар как происходящий с территории страны либо из региона или местности на этой территории, где определенные качество, репутация или другие характеристики товара в значительной степени связываются с его географическим происхождением. Понятие «географическое указание» включает в себя понятия «наименование места происхождения товара» и «указание происхождения товара». Наименованием места происхождения товара признается название страны, населенного пункта, местности или другого географического объекта, используемое для обозначения товара, особые свойства которого исключительно или главным образом определяются характерными для этого географического объекта природными условиями или иными факторами либо сочетанием природных условий и этих факторов. Наименованием места происхождения товара может являться историческое название географического объекта.  
Не признается наименованием места происхождения товара обозначение, хотя и представляющее собой название географического объекта или содержащее название географического объекта, но вошедшее в Республике Беларусь во всеобщее употребление как обозначение товара определенного вида, не связанное с местом его изготовления.  
Указанием происхождения товара признается обозначение, прямо или косвенно указывающее на место действительного происхождения или изготовления товара.  
Указание происхождения товара может быть представлено в виде названия географического объекта или изображения. Правовая охрана наименования места происхождения товара в Республике Беларусь предоставляется на основании его регистрации в патентном органе или в силу международных договоров Республики Беларусь.  
На основании регистрации выдается свидетельство на право пользования наименованием места происхождения товара.

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

**Практическое занятие №11**

**Тема «**Патентный поиск**»**

Цель: изучить содержание, порядок проведения и оформления результатов патентных исследований.

*Задание.* Изобретение относится к области приборостроения и может быть использовано для перемещения узла в двух взаимно перпендикулярных направлениях. Изобретение направлено на повышение точности и расширение эксплуатационных возможностей. Это обеспечивается за счет того, что механизм линейного перемещения содержит корпус, площадку для размещения юстируемого изделия и два регулировочных узла.

|  |  |
| --- | --- |
| http://img.findpatent.ru/img_data/84/847211.gif | Наличие предполагаемых существенных признаков и планируемый выпуск продукции являются предпосылками для патентования разработки.  Необходимо выполнить экспертизу патентной чистоты разработанного конструктивного решения (ОПС). |
| Рисунок 1 – Конструкция механизма для обеспечения линейного перемещения исследуемых препаратов, отличающаяся взаимным расположением перемещающихся элементов. |

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

* объект – *механизма для обеспечения линейного перемещения исследуемых препаратов, отличающаяся взаимным расположением перемещающихся элементов.*
* страна поиска – *Республика Беларусь*;
* источники информации – *патентные*;
* ретроспективность – *5 лет*;

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

Для проведения патентного поиска необходимо определить классификационную рубрику предполагаемого изобретения, которая в данном случае, классифицируется по разделу **«ФИЗИКА»**, класс **«G12В1 Чувствительные элементы, способные производить движение или перемещение, применение которых не ограничивается целями измерения; передаточные механизмы, связанные с ними».**

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

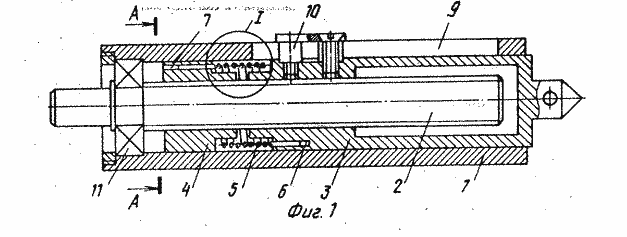


Рисунок 2 - Механизм линейного перемещения

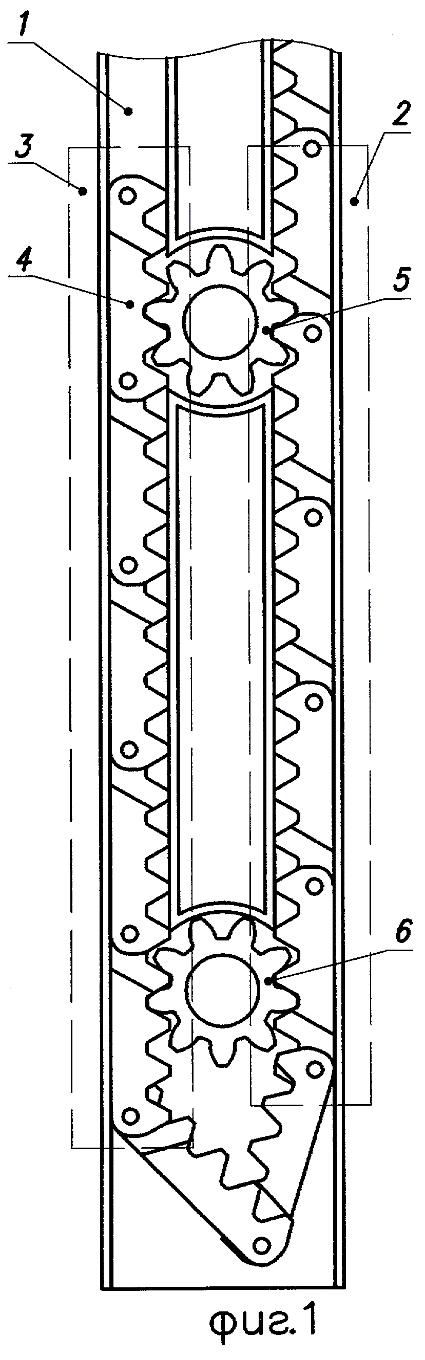


Рисунок 3- Механизм перемещения

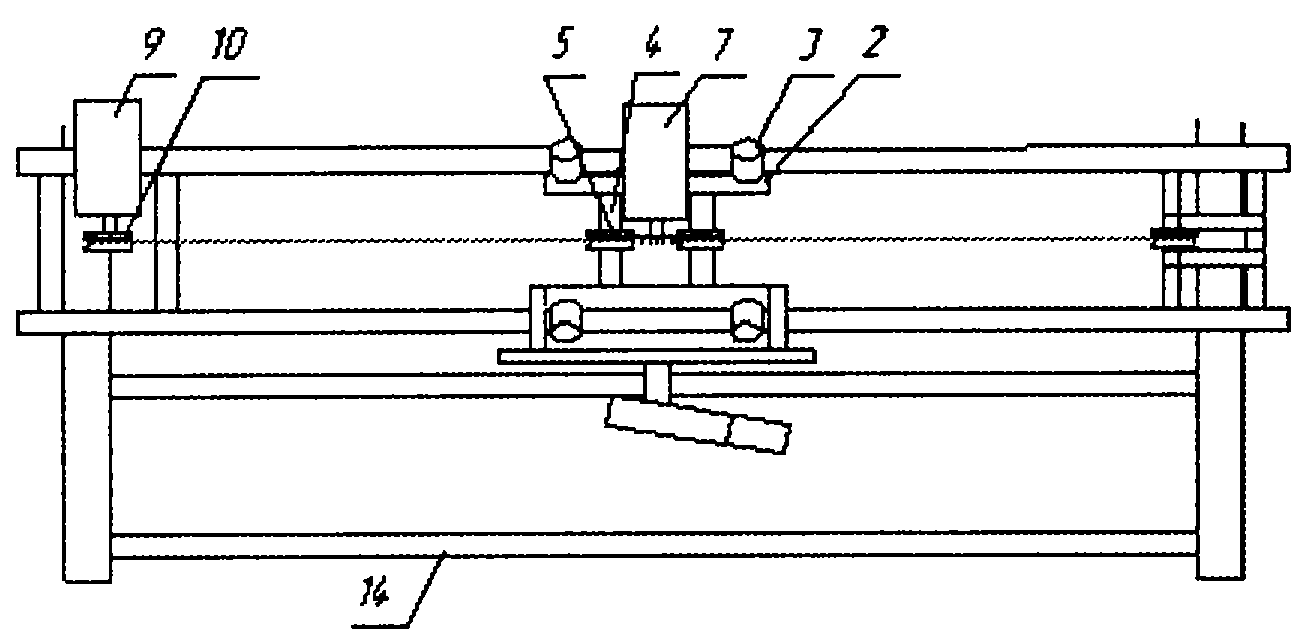


Рисунок 4 - Механизм линейного перемещения плазмотрона

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Таблица 1 – Патентная документация | | | | |
| Предмет поиска (объект исследования, его составные части) | Страна выдачи, вид и номер охранного документа. Классификационный индекс | Заявитель (патентообладатель), страна. Номер заявки, дата приоритета, конвенционный приоритет, дата публикации | Название изобретения (полезной модели, промышленного образца) | Сведения о действии охран-ного документа или причина его аннулирования (только для анализа патентной чистоты) |
| Механизм для обеспечения линейного перемещения исследуемых препаратов | Патент СССР  № 1783205  МПК F16H25/20. | Каменский, Федоров Заявка SU 1783205 A1  Опубликовано: 23.12.1992 | «Механизм линейного перемещения» | Не действует |
| Патент РФ  № 2107857  МПК F16H25/20 | Кочетков В.М.  Номер заявки: 96103527/28  Дата публикации: 27.03.1998 | «Механизм линейного перемещения» | Действует |
| Патент РФ  № 2004108076/11  МПК F16H7/06. | Горелкин И. В,  Пушин А. Г.  Опубликовано: 20.06.2006  Заявка: 2004108076/11, | «Механизм перемещения» | Действует |
| Патент РФ  № 38668  МПК B25J | Барвинок В.А. (RU), Богданович В.И. (RU), Докукина И.А. (RU), Ивашин А.С. (RU), Ананьева Е.А. (RU), Сыроватка Д.В. (RU) Заявка 850372 от 3 Февраля, 2004 опубл.  10 Июля, 2004 | «Устройство для линейного перемещения плазмотрона» | Действует |

Изобретение относится к области приборостроения и может быть использовано для перемещения узла в двух взаимно перпендикулярных направлениях.

Известен механизм линейного перемещения, содержащий корпус, подпружиненную подвижную площадку для юстируемого элемента и регулировочные узлы, каждый из которых состоит из двух пар сухарей в форме трапеции, соединенных регулировочными винтами, и расположенного между ними валика. Данная конструкция обладает невысокой надежностью и не обеспечивает устойчивое положение подвижной площадки с юстируемым элементом.

Наиболее близким аналогом по совокупности признаков является механизм линейного перемещения подвижного элемента в двух взаимно перпендикулярных направлениях. Механизм линейного перемещения содержит корпус, состоящий из верхнего и нижнего оснований, между которыми зажата с возможностью плоского перемещения подвижная площадка с юстируемым элементом, и два регулировочных узла. Каждый регулировочный узел выполнен в виде валика и зубчато-реечной передачи, зубчатые колеса которой размещены на валике по двум противоположным сторонам площадки с юстируемым элементом. Валики установлены в подвижной площадке с возможностью вращения во взаимно перпендикулярных направлениях, а рабочие профили реек зубчато-реечной передачи каждого регулировочного узла выполнены на внутренних поверхностях оснований во взаимно перпендикулярных направлениях. Данный механизм линейного перемещения обладает недостаточной точностью из-за использования зубчато-реечной передачи в регулировочных узлах и имеет ограниченные эксплуатационные возможности из-за замкнутой формы корпуса механизма линейного перемещения.

Задачей изобретения является повышение точности и расширение эксплуатационных возможностей механизма линейного перемещения.

Поставленная задача достигается тем, что в механизм линейного перемещения, содержащем корпус, площадку для размещения юстируемого изделия и два регулировочных узла, в отличие от прототипа, введены две направляющие, каждая из которых выполнена в виде плоской пластины с прямоугольным пазом, причем эти две направляющие расположены под прямым углом друг к другу с образованием прямоугольного окна и с образованием общей плоскости скольжения, а площадка для размещения юстируемого изделия состоит из двух оснований, выполненных с возможностью размещения в образованном прямоугольном окне и при этом соединенных между собой с зазором, в котором размещены направляющие с возможностью скольжения друг относительно друга в общей плоскости скольжения, обеспечивая при этом перемещение площадки для размещения юстируемого изделия, регулировочные узлы выполнены в виде двух передач винт-гайка, винты которых являются частью взаимно перпендикулярных валов, установленных в корпусе с возможностью вращения, а гайки неподвижно закреплены на соответствующих направляющих.

Для компенсации зазора между площадкой и обеими направляющими используются два упругих элемента.

Такая конструкция обеспечивает устойчивое положение площадки для размещения юстируемого изделия практически в любых условиях эксплуатации и не может быть выведена из этого устойчивого равновесия (например динамическими воздействиями), а может лишь, будучи расположенной внутри прямоугольного окна, образованного двумя взаимно перпендикулярными подвижными направляющими, совершать линейные перемещения посредством регулировочных узлов, выполненных в виде передачи винт-гайка, в одной из двух направляющих совместно с другой направляющей и это всегда обеспечивается их взаимным скольжением в общей плоскости.

Выполнение регулировочного узла в виде передачи винт-гайка и обеспечение возможности перемещения площадки в прямоугольном окне, образованном двумя направляющими, позволяют повысить точность линейного перемещения.

Механизм линейного перемещения (см.фиг.1) имеет две направляющие 1 и 2, каждая из которых выполнена в виде плоской пластины с прямоугольным пазом, имеющие общую взаимную плоскость скольжения А и развернутые в этой плоскости на прямой угол с образованием прямоугольного окна, в котором размещена площадка 3 для размещения юстируемого изделия, площадка 3 охватывает направляющие 1 и 2 с возможностью их скольжения друг относительно друга и имеет возможность перемещения в пазах пластин этих направляющих; два регулировочных узла, каждый из которых выполнен в виде передачи винт-гайка. Гайки 4 и 5 неподвижно закреплены соответственно на направляющих 1 и 2, в которых могут вращаться винты, являющиеся частью взаимно перпендикулярных валов 6 и 7, которые имеют по две опоры вращения 8 и 9, расположенные в корпусе 10. Конструкция корпуса может быть любой формы. В предложенной реализации устройства корпус имеет незамкнутую форму. В каждой паре винт-гайка при вращении двух взаимно перпендикулярных валов 6 и 7 положение винтов остается неизменным в пространстве, а каждая гайка 4 и 5 имеет возможность относительного перемещения вдоль оси ответного винта.

Площадка 3 для размещения юстируемого изделия (см. фиг.2) выполнена из двух оснований 11 и 12, соединенных между собой посредством винтов 13 и гаек 14 с образованием между собой зазора, в котором размещены направляющие 1 и 2 с возможностью скольжения друг относительно друга в общей плоскости скольжения. При этом основания 11 и 12 выполняют роль крышек и выполняют функцию каретки, которая может перемещаться в одной из двух взаимно перпендикулярных направляющих.

Площадка 3 может быть дополнена двумя упругими элементами 15, расположенными на боковых поверхностях во взаимно перпендикулярных направлениях для компенсации зазора между подвижной площадкой и обеими направляющими 1, 2 соответственно.

Механизм линейного перемещения работает следующим образом. При вращении вала 6 профиль резьбы винта входит в зацепление с резьбой гайки 4, которая закреплена на направляющей 1, и вызывает совместное поступательное перемещение направляющей 1 с подвижной площадкой 3 вдоль направляющей 2, что соответствует линейному перемещению площадки 3 вдоль оси У-У. Аналогично, при вращения вала 7 с расположенным на нем винтом за счет взаимодействия винта с гайкой 5, гайка поступательно перемещается с направляющей 2 совместно с площадкой 3, что соответствует линейному перемещению площадки вдоль оси Х-Х.

Задавая различные законы вращения валов 6 и 7 регулировочных узлов, предложенный механизм позволяет обеспечивать линейное перемещение площадки 3 с юстируемым изделием по любой траектории по заданному закону движения.

Применение предложенной конструкции позволяет повысить точность и значительно расширить эксплуатационные возможности за счет обеспечения возможности установки сменных юстируемых изделий. Конструкция направляющих позволяет устанавливать в них площадку с юстируемыми элементами и изделиями различного размера и формы, а также позволяет применять механизм в оптических трактах с плотным расположением оптических элементов и ограниченным (щелевым) радиальным подходом. Кроме того, эксплуатационные возможности расширяются за счет постоянного положения в пространстве двух взаимно перпендикулярных валов 6, 7 с расположенными на них винтами и их совместного расположения, невынесенного далеко за пределы оптической трубы. Механизм линейного перемещения может быть использован в автоматизированных устройствах.

Такая конструкция обеспечивает устойчивое положение площадки с юстируемым элементом практически в любых условиях эксплуатации, и площадка не может быть выведена из этого равновесия, а может лишь линейно перемещаться в одной плоскости в прямоугольных направляющих в двух взаимно перпендикулярных направлениях с помощью регулировочных узлов через передачу винт-гайка.

Формула изобретения

1. Механизм линейного перемещения, содержащий корпус, площадку для размещения юстируемого изделия и два регулировочных узла, отличающийся тем, что введены две направляющие, каждая из которых выполнена в виде плоской пластины с прямоугольным пазом, причем эти две направляющие расположены под прямым углом друг к другу с образованием прямоугольного окна и с образованием общей плоскости скольжения, а площадка для размещения юстируемого изделия состоит из двух оснований, выполненных с возможностью размещения в образованном прямоугольном окне и при этом соединенных между собой с зазором, в котором размещены направляющие с возможностью скольжения друг относительно друга в общей плоскости скольжения, обеспечивая при этом перемещение площадки для размещения юстируемого изделия, регулировочные узлы выполнены в виде двух передач винт-гайка, винты которых являются частью взаимно перпендикулярных валов, установленных в корпусе с возможностью вращения, а гайки неподвижно закреплены на соответствующих направляющих.

Механизм линейного перемещения по п.1, отличающийся тем, что для компенсации зазора между площадкой и обеими направляющими используются два упругих элемента.

Вывод: изучили содержание, порядок проведения и оформления результатов патентных исследований

**Практическое занятие №12**

**Тема «**Патентный поиск**»**

Цель: освоить навыки проведения патентного поиска по заданной тематике.

Тема: Модуль создания аналитических отчетов для платформы бизнес анализа Pentaho

* 1. **Информационно-аналитическая система для моделирования рациональной бизнес-системы компании.**

Авторы патента: Скубченко А.И.

Информационно-аналитическая система для моделирования рациональной бизнес-системы компании (RU 2171498):

G06N1 - Компьютерные системы, не отнесенные к группам G06N 3/00-G06N 7/00

G06F17 - Устройства или методы цифровых вычислений или обработки данных, специально предназначенные для специфических функций

Вледельцы патента: Скубченко Андрей Иванович.

Изобретение относится к вычислительной технике и может быть использовано для управления производственными предприятиями. Техническим результатом является расширение функциональных возможностей. Устройство содержит компьютерное устройство концептуального описания бизнеса компании, компьютерное устройство факторного анализа внешней среды, рабочее место оператора, компьютерное устройство моделирования бизнес-системы действующей компании, компьютерное устройство моделирования оптимальной структуры бизнес-системы компании, компьютерное устройство тестирования бизнес-системы компании, компьютерное устройство аналитического мониторинга бизнес-системы компании и компьютерное устройство реинжиниринга. 4 ил.

Изобретение относится к системам и способам вычислений и обработки данных, специально предназначенным для коммерческих и управленческих специфических функций учета и отчетности, и может быть использовано для моделирования с последующим внедрением в производство бизнес-систем.

* 1. **Система для формирования структуры товарного выпуска продукции промышленного предприятия**

Авторы патента:

Виер Игорь Владимирович (RU), Песин Александр Моисеевич (RU), Шмаков Владимир Иванович (RU), Жлудов Виктор Владиславович (RU), Салганик Виктор Матвеевич (RU), Сеничев Геннадий Сергеевич (RU)

Система для формирования структуры товарного выпуска продукции промышленного предприятия (RU 2321884):

G06N1 - Компьютерные системы, не отнесенные к группам G06N 3/00-G06N 7/00

G06F17 - Устройства или методы цифровых вычислений или обработки данных, специально предназначенные для специфических функций

Вледельцы патента:

Закрытое акционерное общество "Патентные услуги" (RU).

Изобретение относится к системам обработки данных, предназначенным для коммерческих и управленческих функций учета и отчетности. Техническим результатом является повышение надежности системы при формировании выпуска товаров, за счет реализации аппаратных средств программными блоками. Система содержит: блок памяти данных о производительностях и доступных фондах времени агрегатов, блок памяти данных об объемах спроса и ценах на выпускаемую продукцию, блок анализа загрузки агрегатов, блок памяти данных о переменных затратах по видам товарной продукции, блок памяти данных о долгосрочных заказах на выпускаемую продукцию, блок определения и анализа прибыльности, блок ранжирования, блок анализа и фиксации долгосрочных договоров, блок сравнения доступного и требуемого фондов времени, блок формирования структуры товарного выпуска, оптимизационный блок. 1 ил.

* 1. **Вычислительная система и способ формирования аналитических данных, относящиеся к способу обработки проектных предложений и заявок**

Авторы патента: КАЛЛЕН Эндрю А. III (US), ДАНИЛОВ Иван (US), ЗИЛЬБЕРМАН Леонид (US)

Вычислительная система и способ формирования аналитических данных, относящиеся к способу обработки проектных предложений и заявок (RU 2329538):

G06Q90 - Вычисление; счет (счетные устройства для подсчета очков при играх A63B 71/06,A63D 15/20,A63F 1/18; комбинации счетных устройств с пишущими приспособлениями B43K 29/08)

G06F9 - Устройства для программного управления, например блоки управления (программное управление для периферийных устройств G06F 13/10)

Вледельцы патента:

ВОЛЬТ ИНФОРМЕЙШН САЙЕНСИЗ, ИНК. (US)

Предложены комплексная вычислительная система с поддержкой сетью Интернет и соответствующий способ, обеспечивающие формирование аналитических данных, относящихся к системе управления предложениями для проекта. Данные транзакций, относящиеся к предложению и проекту, вводят в вычислительную систему посредством оперативных процессов предложения, заявок по проекту и оплаты. При использовании данных транзакций, сохраняемых в системе, может быть сформирован фактически любой вид аналитических данных, связанных с одиночными проектами или множеством проектов, выполняемыми одним или несколькими продавцами для одного или нескольких покупателей.

Вывод: освоили навыки проведения патентного поиска по заданной тематике.