Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Электронная тетрадь**

по Основам Защиты Информации

Студент: Матюх А. А.

ФИТ 2 курс 4 группа

Преподаватель: Берников В. О.

Минск 2019

**Практическое занятие №1**

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

Национальная безопасность ­–­­­­­­­­­ состояние защищенности национальных интересов Республики Беларусь от внутренних и внешних угроз;

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

Информационная безопасность состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз 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.

Основные угрозы национальной безопасности, связанные с ИТ-сферой:

* навязывание Республике Беларусь политического курса, не отвечающего ее национальным интересам, вмешательство извне во внутриполитические процессы;
* рост преступных и иных противоправных посягательств против личности и собственности, коррупционные проявления;
* проявления социально-политического, религиозного, этнического экстремизма и расовой вражды на территории Республики Беларусь;
* дезорганизация системы государственного управления, создание препятствий функционированию государственных институтов;
* деструктивное информационное воздействие на личность, общество и государственные институты, наносящее ущерб национальным интересам;
* нарушение функционирования критически важных объектов информатизации;
* утрата значительной частью граждан традиционных нравственных ценностей и ориентиров, попытки разрушения национальных духовно-нравственных традиций и необъективного пересмотра истории, затрагивающие данные ценности и традиции;
* резкое либо масштабное снижение доверия граждан к основным государственным институтам;
* снижение или потеря конкурентоспособности отечественных информационно-коммуникационных технологий, информационных ресурсов и национального контента;

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.

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»**

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

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

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

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

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

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

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

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

Относительная эффективность:

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

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

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

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

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

где К≥1.

Выражения (2.2) и (2.4) примут вид:

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

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

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

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

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

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

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

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

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

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

или

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

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

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

**Задание на выполнение**

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

Таблица 2.1. Исходные данные

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № варианта | *E*0 | *E* | *K* | *C* |
| 2 | 100000 | 90000 | 50 | 5000 |

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:



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:

Относительная эффективность:

Уменьшение эффективности функционирования объекта приводит к материальному ущербу для владельца объекта. Тогда снижение эффективности функциональности объекта при наличии средств защиты равно:

Выражение для эффективности и относительной эффективности примут вид:

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

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

**Практическое занятие №3**

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

Цель: разработать проект политики информационной безопасности института.

**Введение**

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

В развитии компьютерной техники и программного обеспечения очень важную роль сыграли научные учреждения и высшие учебные заведения. В частности, в ВУЗах разрабатываются, испытываются и внедряются передовые проекты в сфере IT. С ростом киберпреступности защита конфиденциальной информации и научных разработок в учебных учреждениях становится особенно актуальной.

Под политикой информационной безопасности компании понимается «формальное изложение правил поведения лиц, получающих доступ к конфиденциальным данным в корпоративной информационной системе». При этом различают общую стратегическую политику безопасности компании, взаимоувязанную со стратегией развития бизнеса и ИТ-стратегией компании, и частные тактические политики безопасности, детально описывающие правила безопасности при работе с соответствующими ИТ-системами и службами компании.

Политика безопасности определяется как совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов.

При разработке и проведении ее в жизнь целесообразно руководствоваться следующими принципами: невозможность миновать защитные средства, усиление самого слабого звена, многообразие защитных средств, минимизация привилегий, разделение обязанностей, невозможность перехода в небезопасное состояние, достаточность всеобщей поддержки мер безопасности, простота в управлении информационной системой.

В первую очередь для разработки политики информационной безопасности ВУЗа экономического профиля необходимо рассмотреть его цель, функции, задачи и структуру.

Цель: институт как государственное высшее учреждение образования и науки определяет главенствующую роль в национальной системе образования, удовлетворяет потребности граждан в приобретении профессиональных знаний и умений в экономической сфере деятельности, в интеллектуальном, культурном и нравственном развитии личности, в удовлетворении потребностей общества в квалифицированных специалистах с высшим экономическим образованием.

Задачи института:

* проведение профессиональной ориентации, довузовской подготовки и конкурсного отбора учащихся;
* обучение студентов;
* проведение последипломной подготовки и повышения квалификации;
* осуществление подготовки и аттестации научно-педагогических кадров высшей квалификации в соответствии с учебно-научным профилем института;
* разработка новых методов и технологий подготовки кадров, обеспечивающих эффективную интеграцию в мировое сообщество.

Институт в соответствии с порядком, установленным действующим законодательством, выполняет следующие функции:

* определяет перечень специализаций и специальностей, а также направлений научных исследований по профилю института во взаимодействии с заинтересованными ведомствами и министерствами, организациями и предприятиями на основе изучения потребностей народного хозяйства в специалистах;
* разрабатывает и реализует целевые программы в области высшего образования, науки и техники в соответствии со своими профилем совместно с заинтересованными ведомствами и министерствами, организациями и предприятиями;
* проводит инновационную политику в области технологий обучения, направленную на эффективную реализацию целей высшего, послевузовского профессионального и соответствующего дополнительного образования, развитие творческой активности научно-педагогических работников и студентов.

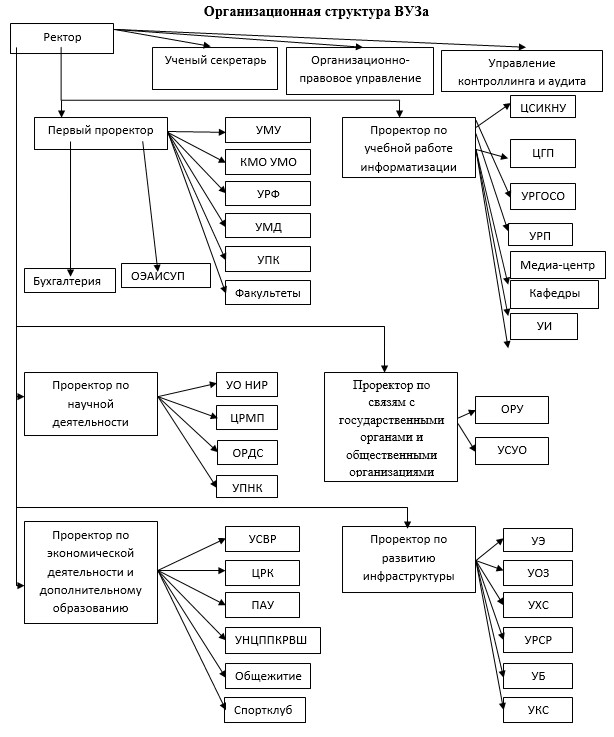


Рисунок 3.1 - Организационная структура ВУЗа

Ниже представлены расшифровки аббревиатур типовых подразделений высшего учебного заведения:

* УМУ - Учебно-методическое управление;
* КМО УМО - Координационно-методический отдел УМО;
* УПК - Управление приемной комиссии;
* УРф - Управление по работе с филиалами;
* УМД - Управление международной деятельности;
* УРП - Управление по работе с персоналом;
* УИ - Управление по информатизации;
* ЦСИКНУ - Центр сохранения историко-культурного наследия института;
* УРГОСО - Управление по работе с государственными органами и связям с общественностью;
* ЦГП - Центр гуманитарной подготовки;
* УО НИР - Управление организации НИР;
* ЦРМП - Центр развития молодежного предпринимательства;
* УПНК - Управление подготовки научных кадров;
* ОРДС - Отдел по работе с диссертационными советами;
* УСВР - Управление по социальной и воспитательной работе;
* ЦРК - Центр развития карьеры;
* УНЦППКРВШ - Учебно-научный центр по переподготовке и повышению квалификации работников высшей школы;
* ПАУ - Прогнозно-аналитическое управление;
* УОЗ - Управление организации закупок;
* УКС - Управление капитального строительства;
* УРСР - Управление ремонтно-строительных работ;
* УЭ - Управление эксплуатации;
* УХС - Управление хозяйственной службы;
* УБ - Управление безопасности;
* ОРУ - Операционно-расчетное управление;
* УСУО - Управление сводного учета и отчетности;
* ОПУ - организационно-правовое управление;
* УКА - управление контроллинга и аудита.
  1. **Специфика образовательных учреждений**

В современном вузе хранится и обрабатывается огромное количество различных данных, связанных не только с обеспечением учебного процесса, но и с научно-исследовательскими и проектно-конструкторскими разработками, персональные данные студентов и сотрудников, служебная, коммерческая и иная конфиденциальная информация.

Рост количества преступлений в сфере высоких технологий диктует свои требования к защите ресурсов вычислительных сетей учебных заведений и ставит задачу построения собственной интегрированной системы безопасности. Ее решение предполагает наличие нормативно-правовой базы, формирование концепции безопасности, разработку мероприятий, планов и процедур по безопасной работе, проектирование, реализацию и сопровождение технических средств защиты информации (СЗИ) в рамках образовательного учреждения. Эти составляющие определяют единую политику обеспечения безопасности информации в вузе.

Специфика защиты информации в образовательной системе заключается в том, что вуз – публичное заведение с непостоянной аудиторией, а также место повышенной активности «начинающих киберпреступников».

Основную группу потенциальных нарушителей в вузе составляют студенты, ряд из них имеют достаточно высокий уровень подготовки. Возраст (от 18 до 23 лет) и юношеский максимализм побуждают таких людей блеснуть знаниями перед сокурсниками: устроить вирусную эпидемию, получить административный доступ и «наказать» преподавателя, заблокировать выход в Интернет и т. д. Достаточно вспомнить, что первые компьютерные правонарушения родились именно в вузе (червь Морриса) [4].

Особенности вуза как объекта информатизации связаны также с многопрофильным характером деятельности, обилием форм и методов учебной работы, пространственной распределенностью инфраструктуры (филиалы, представительства). Сюда же можно отнести и многообразие источников финансирования, наличие развитой структуры вспомогательных подразделений и служб (строительная, производственная, хозяйственная деятельность), необходимость адаптации к меняющемуся рынку образовательных услуг, потребность в анализе рынка труда, отсутствие общепринятой формализации деловых процессов, необходимость электронного взаимодействия с вышестоящими организациями, частое изменение статуса сотрудников и обучаемых.

Несколько облегчает проблему то, что вуз представляет собой стабильную, иерархическую по функциям управления систему, обладающую всеми необходимыми условиями жизнедеятельности и действующую на принципах централизованного управления (последнее означает, что в управлении задачами информатизации может активно использоваться административный ресурс).

Указанные выше особенности обусловливают необходимость соблюдения следующих требований:

* комплексная проработка задач информационной безопасности, начиная с концепции и заканчивая сопровождением программно-технических решений;
* привлечение большого числа специалистов, владеющих содержательной частью деловых процессов;
* использование модульной структуры корпоративных приложений, когда каждый модуль покрывает взаимосвязанную группу деловых процедур или информационных сервисов при обеспечении единых требований к безопасности;
* применение обоснованной последовательности этапов в решении задач информационной безопасности;
* документирование разработок на базе разумного применения стандартов, что гарантирует создание успешной системы;
* использование надежных и масштабируемых аппаратно-программных платформ и технологий различного назначения, обеспечивающих необходимый уровень безопасности.

С точки зрения архитектуры в корпоративной информационной среде можно выделить три уровня, для обеспечения безопасного функционирования которых необходимо применять различные подходы:

* оборудование вычислительной сети, каналов и линий передачи данных, рабочих мест пользователей, системы хранения данных;
* операционные системы, сетевые службы и сервисы по управлению доступом к ресурсам, программное обеспечение среднего слоя;
* прикладное программное обеспечение, информационные сервисы и среды, ориентированные на пользователей.

При создании комплексной информационной сети (КИС) необходимо обеспечить межуровневое согласование требований по безопасности к выбираемым решениям или технологиям. Так, на втором уровне архитектура КИС многих вузов представляет собой разрозненные и слабо связанные подсистемы с разными операционными средами, согласованные друг с другом только на уровне закрепления IP-адресов или обмена сообщениями. Причинами плохой системной организации КИС является отсутствие утвержденной архитектуры КИС, наличие нескольких центров ответственности за развитие технологий, которые действуют несогласованно. Проблемы начинаются с нежелания управлять выбором операционных сред в подразделениях, когда ключевые технологические решения полностью децентрализованы, что резко снижает уровень безопасности системы.

Вузы, имеющие четкую стратегию развития информационных технологий, единые требования к информационной инфраструктуре, политику информационной безопасности и утвержденные регламенты на основные компоненты КИС, отличаются, как правило, сильным административным ядром в управлении и высоким авторитетом руководителя ИТ-службы.

В таких вузах могут, конечно, использоваться различные операционные среды или системы среднего слоя, но это обусловлено организационно-техническими или экономическими причинами и не препятствует развертыванию КИС вуза и внедрению унифицированных принципов безопасного доступа к информационным ресурсам.

Состояние развития в вузах третьего уровня архитектуры КИС можно охарактеризовать следующим образом: в основном завершен переход от локальных программных приложений, автоматизирующих отдельный деловой процесс и опирающихся на локальный набор данных, к корпоративным клиент-серверным информационным системам, обеспечивающим доступ пользователей к оперативным базам данных вуза. В том или ином виде решена задача интеграции данных, порожденных различными информационными системами, что позволяет усовершенствовать бизнес-процессы, повысить качество управления и принятия решений.

Если в начале 90-х гг. XX в. был высокий спрос на бухгалтерское программное обеспечение и программное обеспечение управленческого учета (учет кадров, отчетность и т. д.), то в настоящее время этот спрос в большей части удовлетворен. В настоящее время стоит задача обеспечить достоверными данными о деятельности образовательного учреждения не только управленческий персонал, но и каждого преподавателя и студента, т. е. задача эффективного управления данными, циркулирующими в КИС, что, в свою очередь, делает задачу обеспечения информационной безопасности в таких сетях еще более актуальной.

* 1. **Информационная безопасность корпоративных сетей вузов**

Активное внедрение Интернета и новых информационных технологий в образовательный процесс и систему управления вузом создало предпосылки к появлению корпоративных сетей.

Корпоративная сеть вуза – это информационная система, включающая в себя компьютеры, серверы, сетевое оборудование, средства связи и телекоммуникации, систему программного обеспечения, предназначенную для решения задач управления вузом и ведения образовательной деятельности.

Корпоративная сеть обычно объединяет не только структурные подразделения вуза, но и их региональные представительства. Ранее недоступные для вуза, в настоящее время эти сети стали активно внедряться в образовательные структуры в связи с массовым распространением Интернета и его доступностью.

Комплексная информационная безопасность вуза – система сохранения, ограничения и авторизованного доступа к информации, содержащейся на серверах в корпоративных сетях вузов, а также передаваемая по телекоммуникационным каналам связи в системах дистанционного обучения.

В более широком смысле термин «комплексная информационная безопасность вуза» включает в себя два аспекта: систему защиты интеллектуальной информационной собственности вуза от внешних и внутренних агрессивных воздействий и систему управления доступом к информации и защиты от агрессивных информационных пространств. В последнее время, в связи с неконтролируемым массовым развитием Интернета, последний аспект безопасности становится особенно актуальным.

Под термином «информационное пространство» понимается информация, содержащаяся на серверах в корпоративных сетях учебных заведений, учреждений, библиотек и в глобальной сети Интернет, на электронных носителях информации, а также передаваемая по телевизионным каналам связи или по телевидению.

Агрессивное информационное пространство – это информационное пространство, содержание которого может вызвать проявления агрессии у пользователя как сразу же после информационного воздействия, так и через некоторое время (отдаленный эффект).

Проблемы комплексной информационной безопасности корпоративных сетей вузов гораздо шире, разнообразнее и острее, чем в других системах. Это связано со следующими особенностями:

* корпоративная сеть вуза строится обычно на концепции «скудного финансирования» (оборудование, кадры, нелицензионное программное обеспечение);
* как правило, корпоративные сети не имеют стратегических целей развития. Это значит, что топология сетей, их техническое и программное обеспечение рассматриваются с позиций текущих задач;
* в одной корпоративной сети вуза решаются две основные задачи: обеспечение образовательной и научной деятельности и решение задачи управления образовательным и научным процессами. Это означает, что одновременно в этой сети работает несколько автоматизированных систем или подсистем в рамках одной системы управления (АСУ «Студент», АСУ «Кадры», АСУ «Учебный процесс», АСУ «Библиотека», АСУ «НИР», АСУ «Бухгалтерия» и т. д.);
* корпоративные сети гетерогенны как по оборудованию, так и по программному обеспечению в связи с тем, что создавались в течение длительного времени для разных задач;
* планы комплексной информационной безопасности, как правило, либо отсутствуют, либо не соответствуют современным требованиям.

В такой сети возможны как внутренние, так и внешние угрозы безопасности информации:

* попытки несанкционированного администрирования баз данных;
* исследование сетей, несанкционированный запуск программ по аудиту сетей;
* удаление информации, в том числе библиотек;
* запуск игровых программ;
* установка вирусных программ и троянских коней;
* попытки взлома АСУ «ВУЗ»;
* сканирование сетей, в том числе других организаций, через Интернет;
* несанкционированная откачка из Интернета нелицензионного софта и установка его на рабочие станции;
* попытки проникновения в системы бухгалтерского учета;
* поиск «дыр» в OC, firewall, Proxy-серверах;
* попытки несанкционированного удаленного администрирования ОС;
* сканирование портов и т. п.
  1. **Анализ угроз, их источников и рисков**

Источниками возможных угроз информации являются:

* компьютеризированные учебные аудитории, в которых проходит учебный процесс;
* Интернет;
* рабочие станции неквалифицированных в сфере информационной безопасности работников вуза.

Анализ информационных рисков можно разделить на следующие этапы:

* классификация объектов, подлежащих защите, по важности;
* определение привлекательности объектов защиты для взломщиков;
* определение возможных угроз и вероятных каналов доступа на объекты;
* оценка существующих мер безопасности;
* определение уязвимостей в обороне и способов их ликвидации;
* составление ранжированного списка угроз;
* оценка ущерба от несанкционированного доступа, атак в отказе обслуживании, сбоев в работе оборудования. Основные объекты, нуждающиеся в защите от несанкционированного доступа:
* бухгалтерские ЛВС, данные планово-финансового отдела, а также статистические и архивные данные;
* серверы баз данных;
* консоль управления учетными записями;
* www/ftp-серверы;
* ЛВС и серверы исследовательских проектов.

Как правило, связь с Интернетом осуществляется сразу по нескольким линиям связи (оптоволоконная магистраль, спутниковые и радиоканалы). Отдельные каналы предоставляются для связи с другими институтами или для безопасного обмена данными.

Чтобы исключить риски, связанные с утечкой и порчей передаваемой информации, такие сети не должны подключаться к глобальным сетям и общей сети института.

Критически важные узлы для обмена данными института (например, бухгалтерская ЛВС) также должны существовать отдельно.

* 1. **Рубежи защиты**

Первый рубеж обороны от атак извне (Интернет) – роутер (маршрутизатор). Он применяется для связи участков сети друг с другом, а также для более эффективного разделения трафика и использования альтернативных путей между узлами сети. От его настроек зависит функционирование подсетей и связь с глобальными сетями (WAN). Его главная задача в плане безопасности – защита от распределенных атак в отказе обслуживания (DDOS).

Вторым рубежом может служить межсетевой экран (МСЭ): аппаратно-программный комплекс Cisco PIX Firewall.

Затем следует демилитаризованная зона (DMZ). В этой зоне необходимо расположить главный прокси-сервер, dns-сервер, www/ftp, mail-серверы. Прокси-сервер обрабатывает запросы от рабочих станций учебного персонала, серверов, не подключенных напрямую к роутеру, и фильтрует трафик. Политика безопасности на этом уровне должна определяться блокированием нежелательного трафика и его экономией (фильтрация мультимедиаконтента, iso-образов, блокировка страниц нежелательного/нецензурного содержания по ключевым словам). Чтобы не происходило скачивания информации, зараженной вирусами, на этом сервере оправдано размещение антивирусных средств.

Информация от прокси-сервера должна параллельно отсылаться на сервер статистики, где можно посмотреть и проанализировать деятельность пользователей в Интернете. На почтовом сервере обязательно должен присутствовать почтовый антивирус, например Kaspersky AntiVirus for Mail servers.

Так как эти серверы связаны непосредственно с глобальной сетью, аудит программного обеспечения, установленного на них, – первоочередная задача инженера по информационной безопасности вуза. Для экономии средств и гибкости настраивания желательно применять opensource ОС и программное обеспечение.

Одни из самых распространенных ОС – FreeBSD и GNU Linux. Но ничто не мешает использовать и более консервативную Open BSD или даже сверхстабильную ОС реального времени – QNX.

Для централизованного управления антивирусной деятельностью необходим продукт с клиент-серверной архитектурой, такой как Dr.Web Enterprise Suite. Он позволяет централизованно управлять настройками и обновлением антивирусных баз с помощью графической консоли и предоставлять удобочитаемую статистику о вирусной деятельности, если таковая присутствует.

Для большего удобства работников вуза можно организовать доступ к внутренней сети института с помощью технологии VPN.

Некоторые институты имеют свой пул дозвона для выхода в Интернет и используют каналы связи учреждения. Во избежание использования этого доступа посторонними лицами в незаконных целях работники учебного заведения не должны разглашать телефон пула, логин, пароль.

Степень защищенности сетей и серверов большинства вузов оставляет желать лучшего. Причин тому много, но одна из главных – плохая организация мер по разработке и обеспечению политики информационной безопасности и недооценка важности этих мероприятий. Вторая проблема заключается в недостаточном финансировании закупок оборудования и внедрения новых технологий в сфере информационной безопасности.

* 1. **Структура системы комплексной информационной безопасности вуза**

Система комплексной информационной безопасности должна включать в себя выработку следующих политик.

Прежде всего, это финансовая политика развертывания, развития и поддержания в актуальном состоянии корпоративной сети вуза. Она является доминирующей и ее можно разделить на три направления: скудное финансирование, финансирование с разумной достаточностью и приоритетное финансирование.

Вторая политика определяется уровнем организации развертывания и сопровождения корпоративной сети вуза.

Третья политика относится к кадровому составу информационного центра. Для вуза она особенно актуальна в связи с повышенной востребованностью опытных сисадминов.

Политика программного обеспечения в настоящее время – один из затратных факторов развития корпоративной сети. Рациональные подходы к его решению в условия монопольного рынка ОС и программных продуктов MicroSoft – это отдельный вопрос, требующий внимательного рассмотрения.

Политика технического обеспечения, может быть, не вполне актуальна в условиях достаточного финансирования. Но всегда существует проблема обновления устаревшего оборудования.

Наконец, последняя политика связана с формирование морально-этических норм толерантного поведения в информационных системах и разумного ограничения от посещений агрессивных информационных пространств. Недооценка этих направлений будет компенсироваться повышенными финансовыми затратами на сопровождение корпоративных сетей вузов.

На основе анализа деятельности подразделений ВУЗа, а также самого института в целом, составлен перечень типов информации, наиболее нуждающейся в защите:

* персональные данные студентов и сотрудников (отдел кадров, бухгалтерия, отдел эксплуатации АИС учебного процесса, факультеты, кафедры);
* информация об информационных технологиях, корпоративной сети, вычислительной сети, программном обеспечении, разработках в области информационных технологий, информационной системе института (управление по информатизации);
* бизнес-идеи студентов и сотрудников;
* сведения о техническом обслуживании объектов и инженерных сетей (управление эксплуатации);
* политика безопасности, результаты конфиденциальных совещаний (управление по безопасности).

Подлежащая защите информация хранится как в электронном, так и в бумажном виде на серверах института, на персональных компьютерах сотрудников отделов и в архиве документов; с информацией работают сотрудники указанных отделов, и, соответственно, только сотрудники отделов имеют доступ к соответствующей информации.

Следующим этапом после определения информации, подлежащей защите, является разработка модели злоумышленника.

Модель злоумышленника - абстрактное (формализованное или неформализованное) описание нарушителя правил разграничения доступа.

Модель злоумышленника включает в себя 4 основных пункта:

* Цель злоумышленника;
* Портрет злоумышленника;
* Направления атаки;
* Инструменты атаки.

Модель злоумышленника разрабатывается исходя из 4 видов угроз информации:

1. Блокирование.

При блокировании целью злоумышленника является создание условий для отсутствия или ограничения доступа пользователей информационной системы для последующего получения как материальной, так и нематериальной выгоды.

2.Копирование.

При копировании целью злоумышленника является нарушение конфиденциальности информации для последующего оглашения, использования в личных целях или продажи заинтересованным лицам.

3.Модификация.

При модификации целью злоумышленника является изменение информации в системе для причинения ущерба, получения выгоды либо иных личных интересов.

4.Уничтожение.

При уничтожении целью злоумышленника является невозможность восстановления информации ее владельцем для причинения материального и нематериального ущерба.

Для полного описания модели злоумышленника необходимо определить категорию нарушителя: внутренний или внешний злоумышленник.

Внутренним злоумышленником может быть лицо из следующих категорий сотрудников института:

* сотрудники факультетов и кафедр;
* сотрудники отдела кадров;
* сотрудники Управления информатизации;
* сотрудники Управления безопасности;
* руководители различных уровней.

Категории лиц, которые могут быть внешними нарушителями:

* уволенные сотрудники;
* технический персонал, обслуживающий здания (уборщицы, электрики, сантехники и другие сотрудники, имеющие доступ в здания и помещения, где расположена информация);
* посетители (приглашенные представители организаций, представители фирм, поставляющих технику, программное обеспечение, услуги и т.п.);
* члены преступных организаций, сотрудники спецслужб или лица, действующие по их заданию;
* лица, умышленно проникшие в сети института из внешних (по отношению к ней) сетей телекоммуникации (хакеры).

Сотрудники Управления информатизации и Управления безопасности имеют наиболее широкие возможности по осуществлению несанкционированных действий, вследствие наличия у них определенных полномочий по доступу к ресурсам и хорошего знания технологии обработки информации и защитных мер. Действия этой группы лиц напрямую связаны с нарушением действующих правил и инструкций. Особую опасность эта группа нарушителей представляет при взаимодействии с криминальными структурами или спецслужбами.

Уволенные сотрудники могут использовать для достижения целей свои знания о технологии работы, защитных мерах и правах доступа. Полученные знания и опыт выделяют их среди других источников внешних угроз.

Конкуренты и криминальные структуры представляют наиболее агрессивный источник внешних угроз. Для осуществления своих замыслов эти структуры могут идти на открытое нарушение закона и вовлекать в свою деятельность сотрудников ВУЗа всеми доступными им силами и средствами.

Профессиональные хакеры имеют наиболее высокую техническую квалификацию и знания о слабостях программных средств, используемых в институте. Наибольшую угрозу представляют криминальные структуры и уволенные сотрудники при взаимодействии с ныне работающими.

Внешние информационные посредники (организации, занимающиеся разработкой, поставкой и ремонтом оборудования, информационных систем) представляют внешнюю угрозу в силу того, что эпизодически имеют непосредственный доступ к информационным ресурсам. Конкуренты, криминальные структуры и спецслужбы могут использовать эти организации для временного устройства на работу своих членов с целью доступа к защищаемой информации.

Предлагается принять следующие ограничения и предположения о характере действий возможных нарушителей:

* работа по подбору кадров и специальные мероприятия исключают возможность создания коалиций нарушителей, т.е. объединения (сговора) и целенаправленных действий двух и более нарушителей - сотрудников института по преодолению системы защиты;
* нарушитель скрывает свои несанкционированные действия от других сотрудников ВУЗа;
* несанкционированные действия могут быть следствием ошибок, как сотрудников факультетов, кафедр, так и сотрудников Управления информатизации, а также вследствие несовершенства и недостатков принятой технологии обработки, хранения и передачи информации;
* в своей противоправной деятельности вероятный нарушитель может использовать любое имеющееся средство перехвата информации, воздействия на информацию и информационные системы, а также адекватные финансовые средства для подкупа персонала, шантаж и другие средства и методы для достижения стоящих перед ним целей.

**Вывод:** из вышесказанного следует, что при разработке политики информационной безопасности учреждения, в том числе и ВУЗа, необходимо учитывать модель злоумышленника. Чем адекватнее будет модель, тем более полно будет организована защита конфиденциальных данных. Таким образом, построение модели злоумышленника является существенным звеном в организации политики безопасности информационной безопасности на предприятии.

**Практическое занятие №4**

**Тема «Настройка Брандмауэра Windows»**

Брандмауэр - аппаратный или программный комплекс, позволяющий фильтровать входные и выходные потоки данных, проходящие через интернет или сеть. В случаи нарушения политики безопасности компьютера, брандмауэр блокирует эти данные.

Большая часть проблем с информационной безопасностью сетей связана с особенностью открытой платформы и среды, что сказалось на реализации протоколов обмена данными и политики информационной безопасности. Вследствие этого ряд Internet-служб и совокупность сетевых протоколов имеет "бреши" в защите.

К числу таких служб и протоколов относятся:

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

**Задание**

1. Создать правила для входящих подключений:
   1. Для 1 программы (по выбору) на блокировку подключения:
   2. Для 1 программы (по выбору) на разрешение подключения;

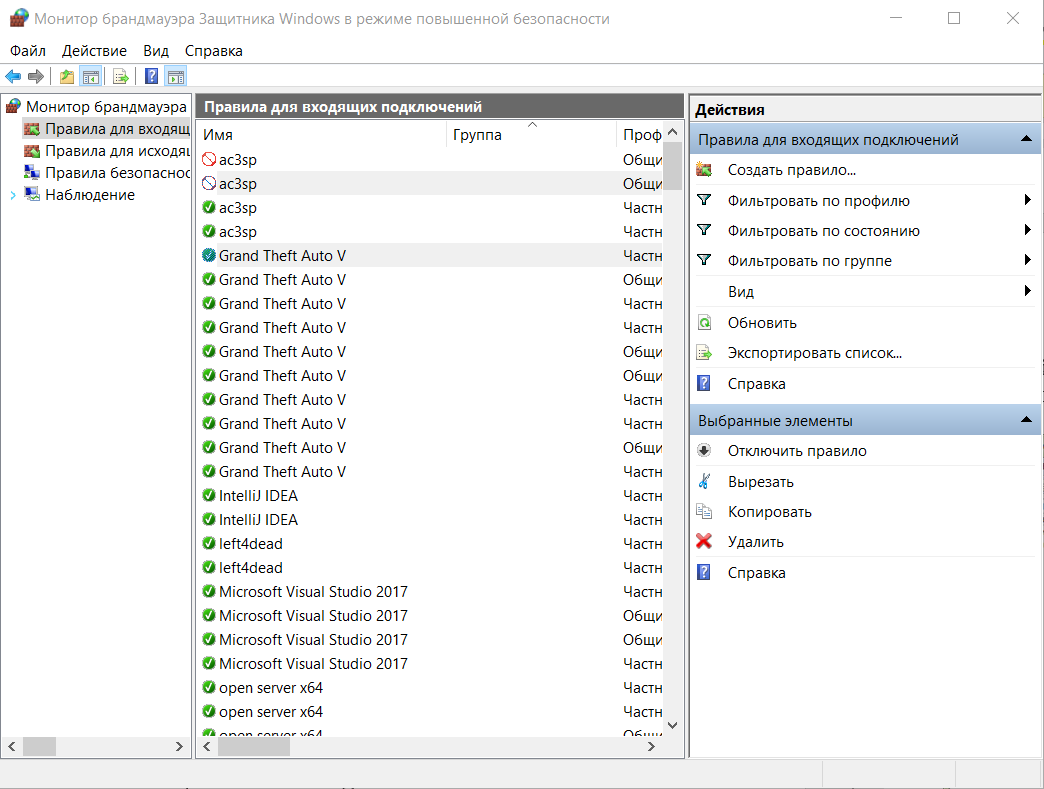


Рисунок 4.1 – Блокировка и разрешение входящих подключений

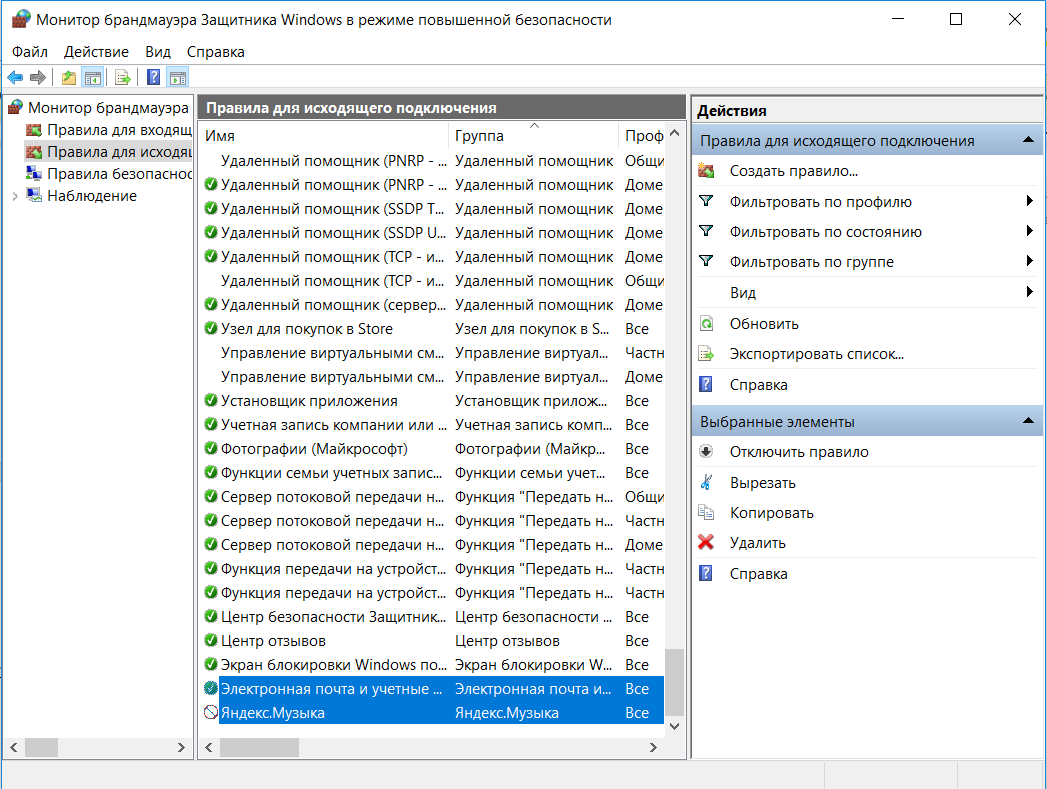


Рисунок 4.2 - Блокировка и разрешение исходящих подключений

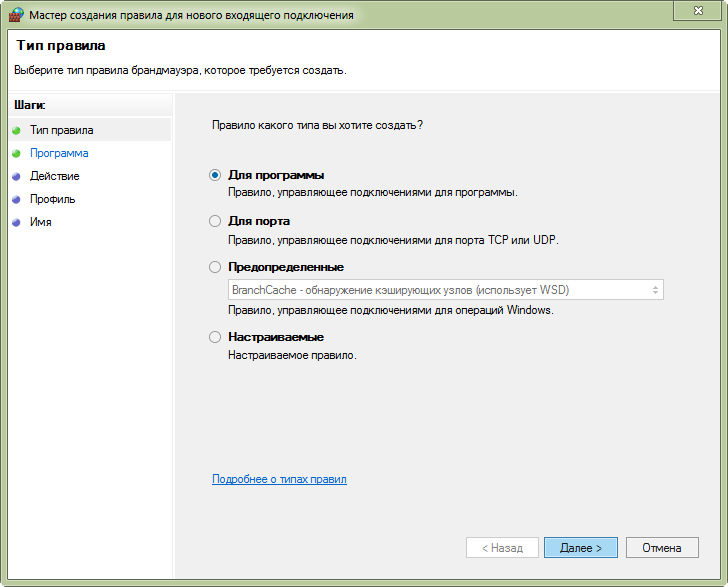


Рисунок 4.3 - Блокировка и разрешение исходящих подключений

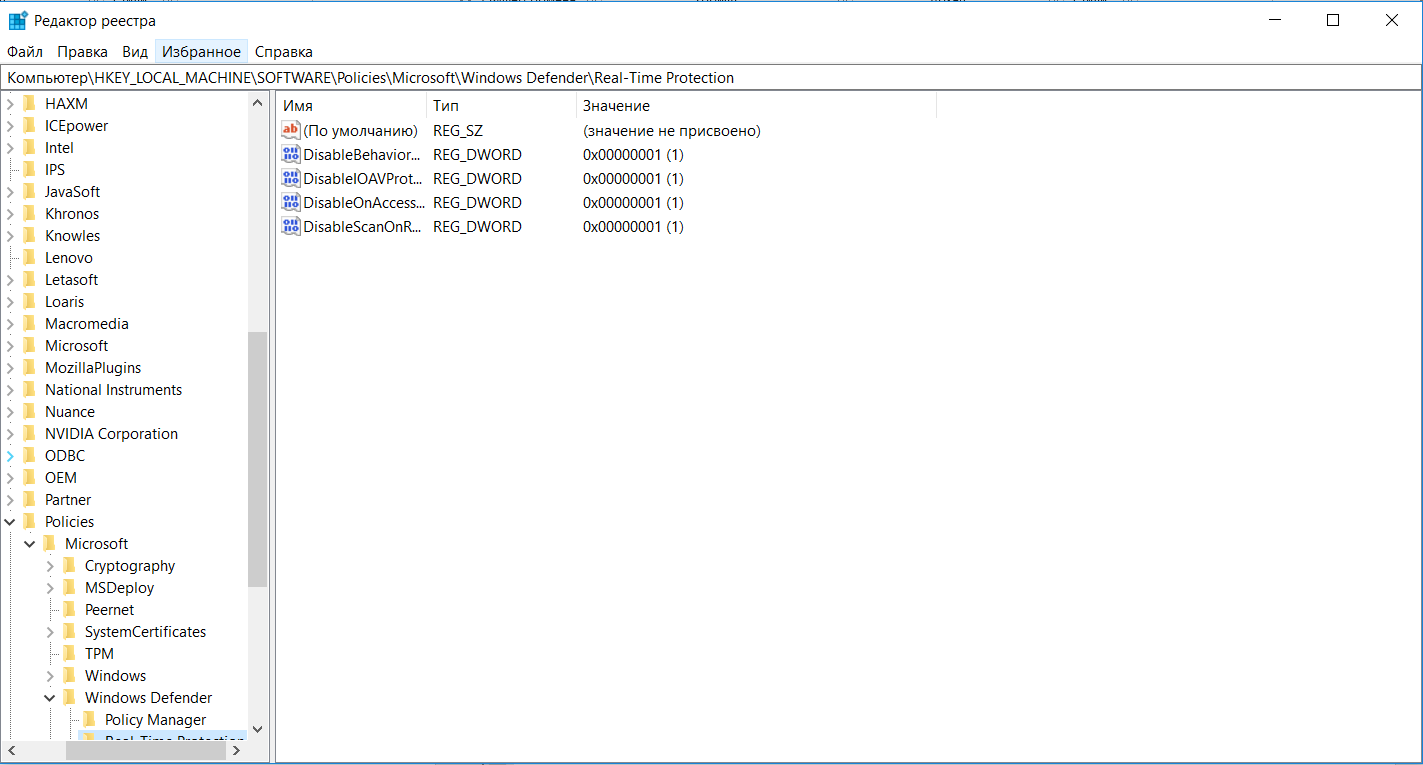


Рисунок 4.4 – Вызов реестра (regedit)

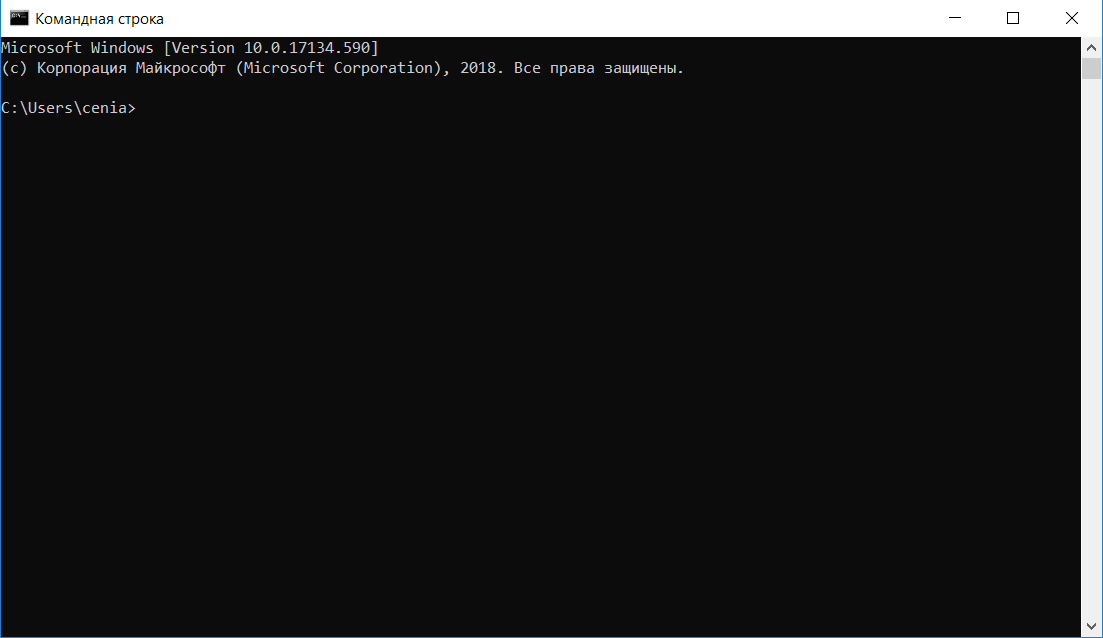


Рисунок 4.5 – Вызов командной строки (cmd)

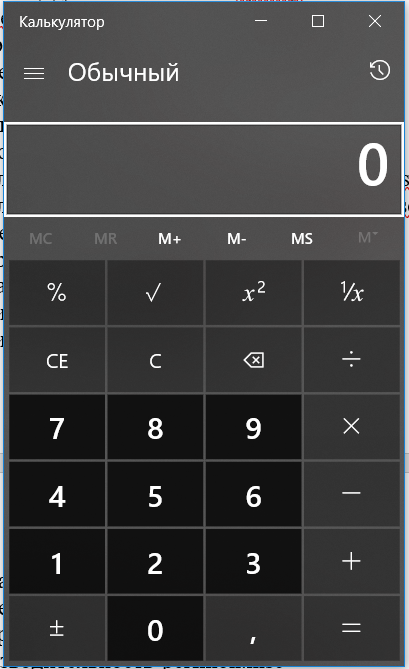


Рисунок 4.6 – Вызов калькулятора (calc)

**Вывод:** Брандмауэр одно из наиболее эффективных средств для закрытия дыр в информационной защите операционной системы. Он фильтрует входящие и исходящие потоки данных из сети, препятствуя снижению информационной защиты аппаратного средства.

**Практическое занятие №5**

**Тема «Настройка антивирусов»**

При заражении компьютера вредоносными программами важно их обнаружить. Для этого следует знать об основных признаках проявления вредоносных программ. К ним можно отнести следующие:

* прекращение работы или неправильная работа ранее успешно функционировавших программ:
* медленная работа компьютера;
* невозможность загрузки операционной системы;
* исчезновение файлов и каталогов или искажение их содержимого;
* изменение размеров файлов;
* неожиданное значительное увеличение количества файлов на диске;
* частые зависания и сбои в работе компьютера.

Персональный файервол – это устройство, выполняющее функции драйвера сетевого трафика и управляющее взаимодействием в рамках локальной сети или Интернета. При помощи правил файервол анализирует это взаимодействие и принимает решение о его разрешении или запрете. Основная функция файервола – защита частных сетей или компьютеров от вторжения со стороны внешних сетей и компьютеров.

Настройка **режима фильтрации файервола антивируса**:

Откроем дополнительные настройки, нажав на клавишу «F5» **-** «Персональный файервол». В раскрывающемся меню справа **Режим фильтрации** выбрать нужный режим фильтрации и нажать **OK.**

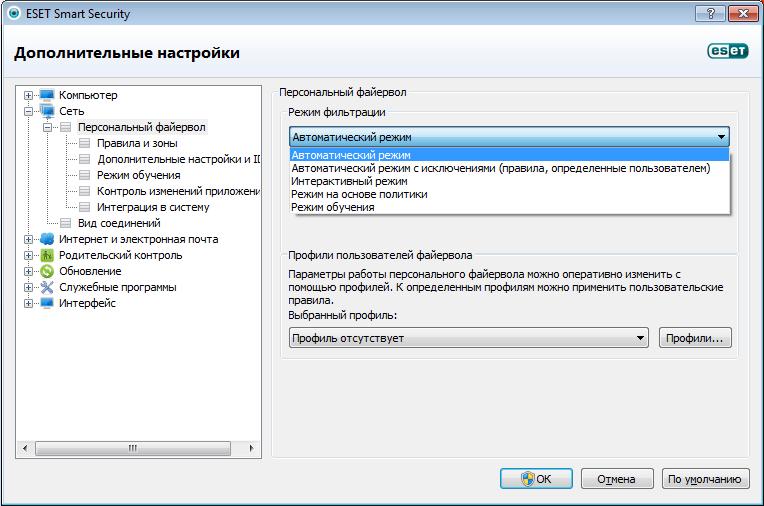


Рисунок 5.1 –Выбор режима фильтрации

Настройка **оффлайн обновления сигнатур угроз из локальной папки:**

1. Скачиваем архив с обновлениями на сайте антивируса.   
   Сохраняем его на компьютере. Распаковываем архив;
2. Запускаем ESET NOD32;
3. Нажать клавишу «F5», далее перейти на вкладку «Обновление»;

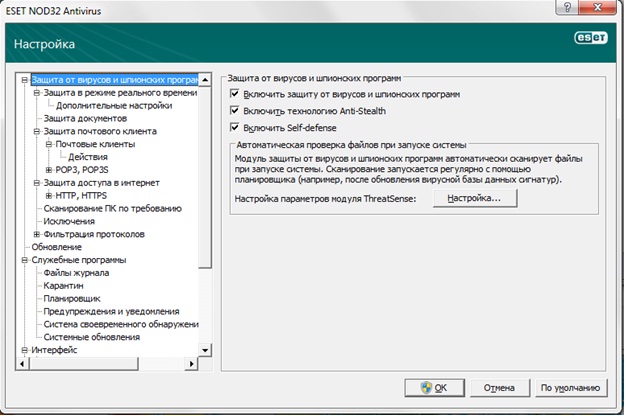


Рисунок 5.2 – Вкладка настройки

1. В строке «Сервер обновлений» нажать «Изменить»;

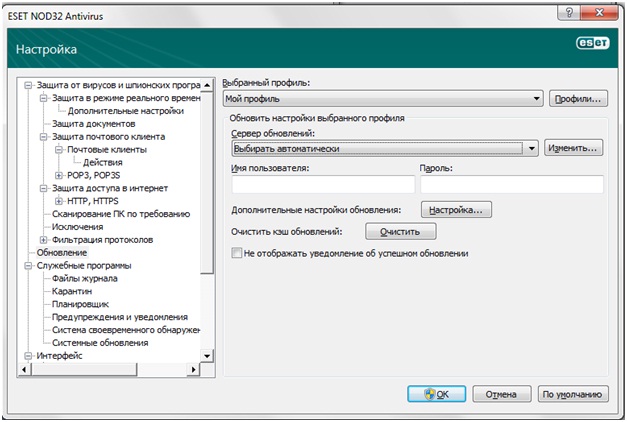


Рисунок 5.3 – Вкладка Обновления

1. В строке «Серверы обновлений» указать путь к папке с обновлениями, далее нажать «Добавить» и «OК»;

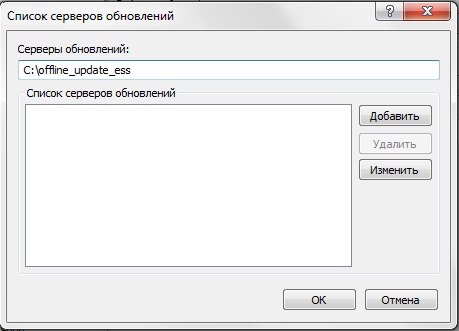


Рисунок 5.4 – Список обновлений

1. В главном окне программы выбрать «Обновление», далее «Обновить версию базы данных сигнатур вирусов».

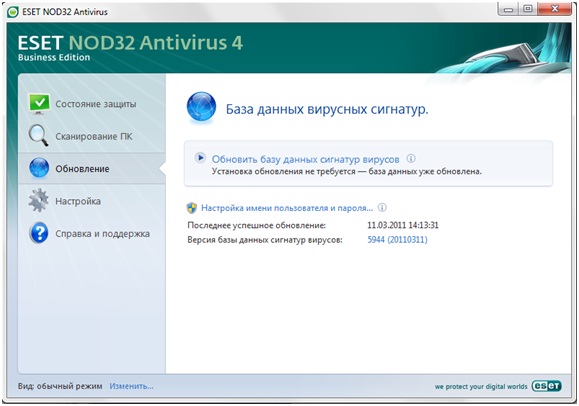


Рисунок 5.5 – Обновление баз данных

Настройка **оффлайн обновления сигнатур угроз из локального сервера:**

1. Запускаем ESET NOD32;
2. Нажать клавишу «F5», далее перейти на вкладку «Обновление»;

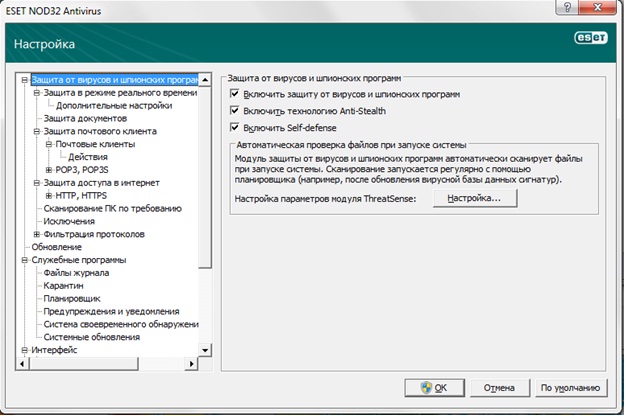


Рисунок 5.6 – Вкладка настройки

1. В строке «Сервер обновлений» нажать «Изменить»;

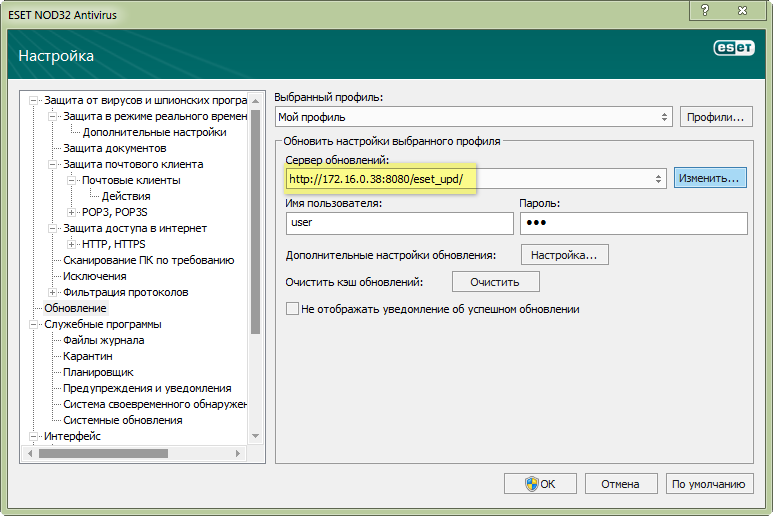


Рисунок 5.6 – Вкладка Обновления

1. Вводим необходимый адрес и нажимаем добавить;

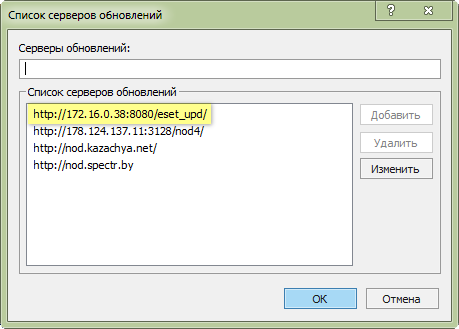


Рисунок 5.7 – Список серверов

1. Вернемся в предыдущее окно и введём имя пользователя и пароль;

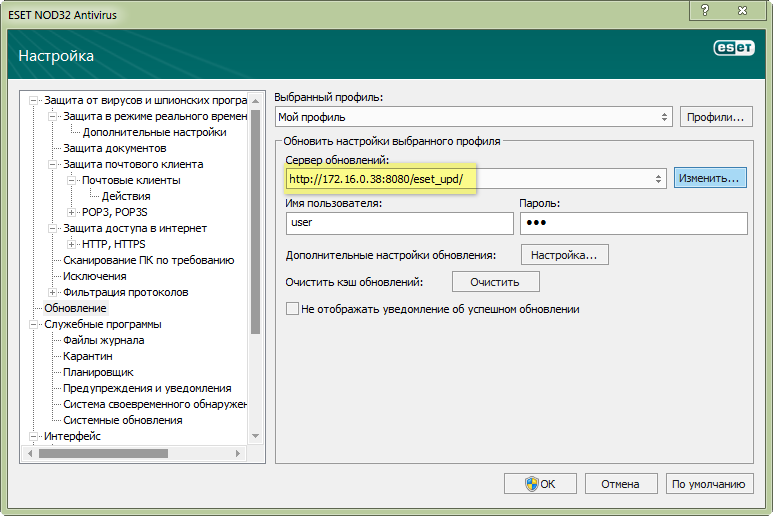


Рисунок 5.8 – Вкладка Обновления

1. В главном окне программы выбрать «Обновление», далее «Обновить версию базы данных сигнатур вирусов».

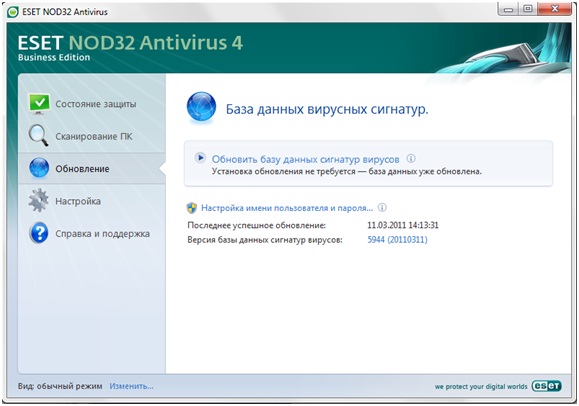


Рисунок 5.9 – Обновление баз данных

**Вывод:** Антивирус представляет собой мощную систему для обеспечения информационной безопасности аппаратного средства, ограничивая и нейтрализуя внешние опасные вмешательства. Все это осуществляется за счет постоянно обновляемой базы вирусных сигнатур.

**Практическое занятие №6**

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

Шифрование на сегодняшний день является одним из самых надежных способов предотвратить несанкционированный доступ к важным документам, базам данных, фотографиям и любым другим файлам.

1. Запуск программы TrueCrypt.

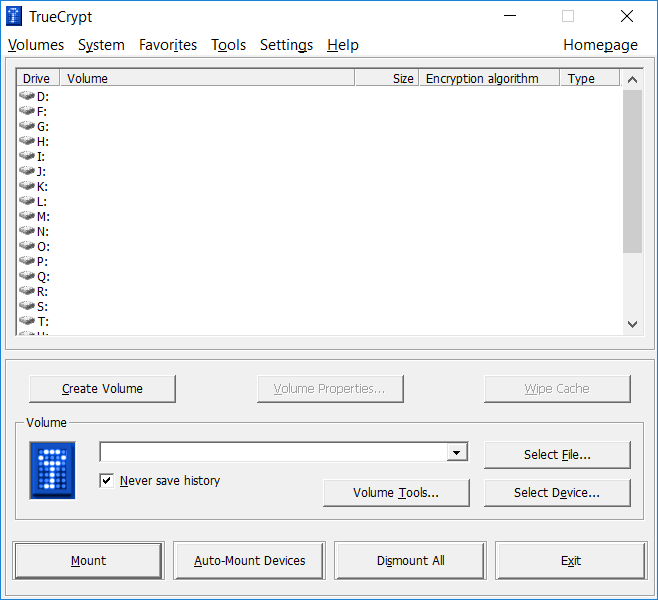


Рисунок 6.1 – Главное окно программы.

1. Окно для создания TrueCrypt- раздела.

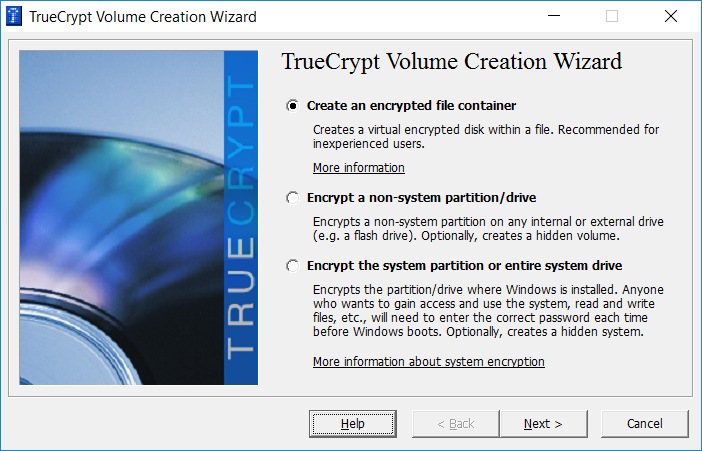


Рисунок 6.2 – Окно для создания TrueScript-раздела.

1. Выбор типа раздела.

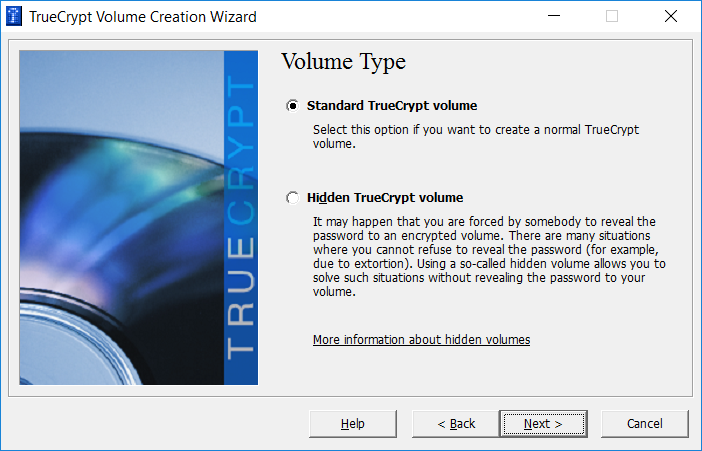


Рисунок 6.3 – Окно выбора типа раздела.

1. Указание места расположения раздела TrueCrypt

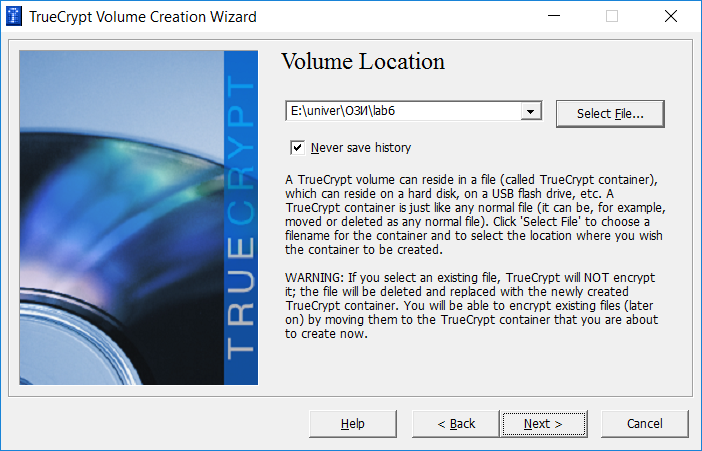


Рисунок 6.4 – Указание пути для создания раздела.

1. Выбор алгоритма для шифрования, а также хеш – алгоритма предназначенного для раздела.

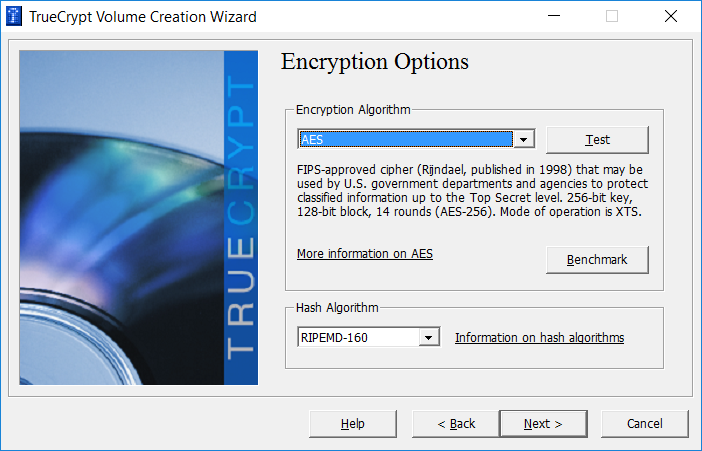


Рисунок 6.5 – Выбор алгоритмов

1. Указание размера контейнера TrueScript.

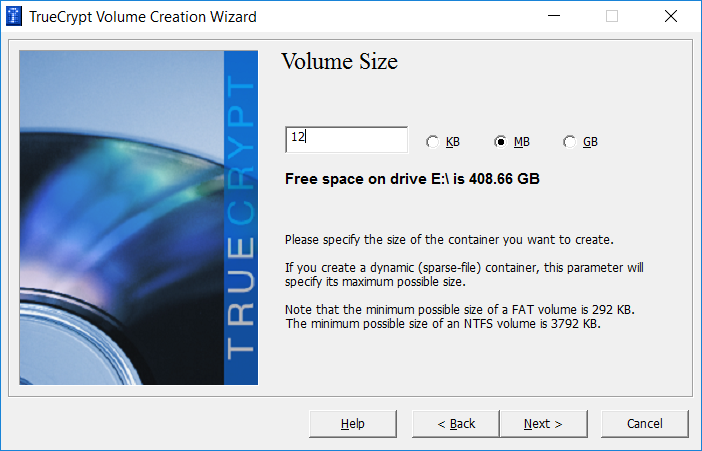


Рисунок 6.6 – Указание размера.

1. Указание пароля для созданного раздела.

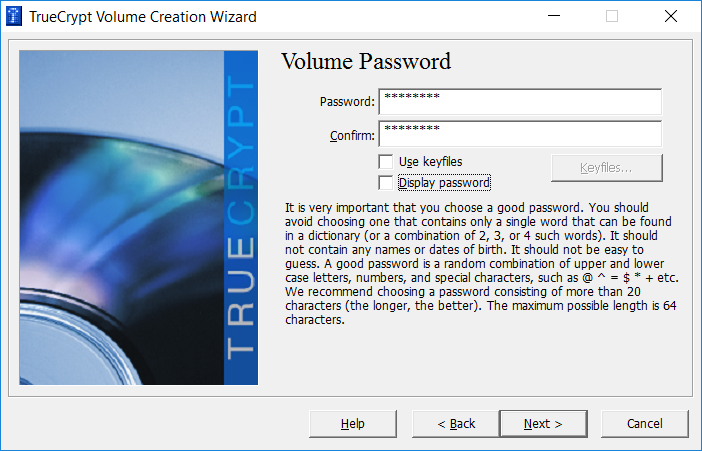


Рисунок 6.7 – Указание пароля

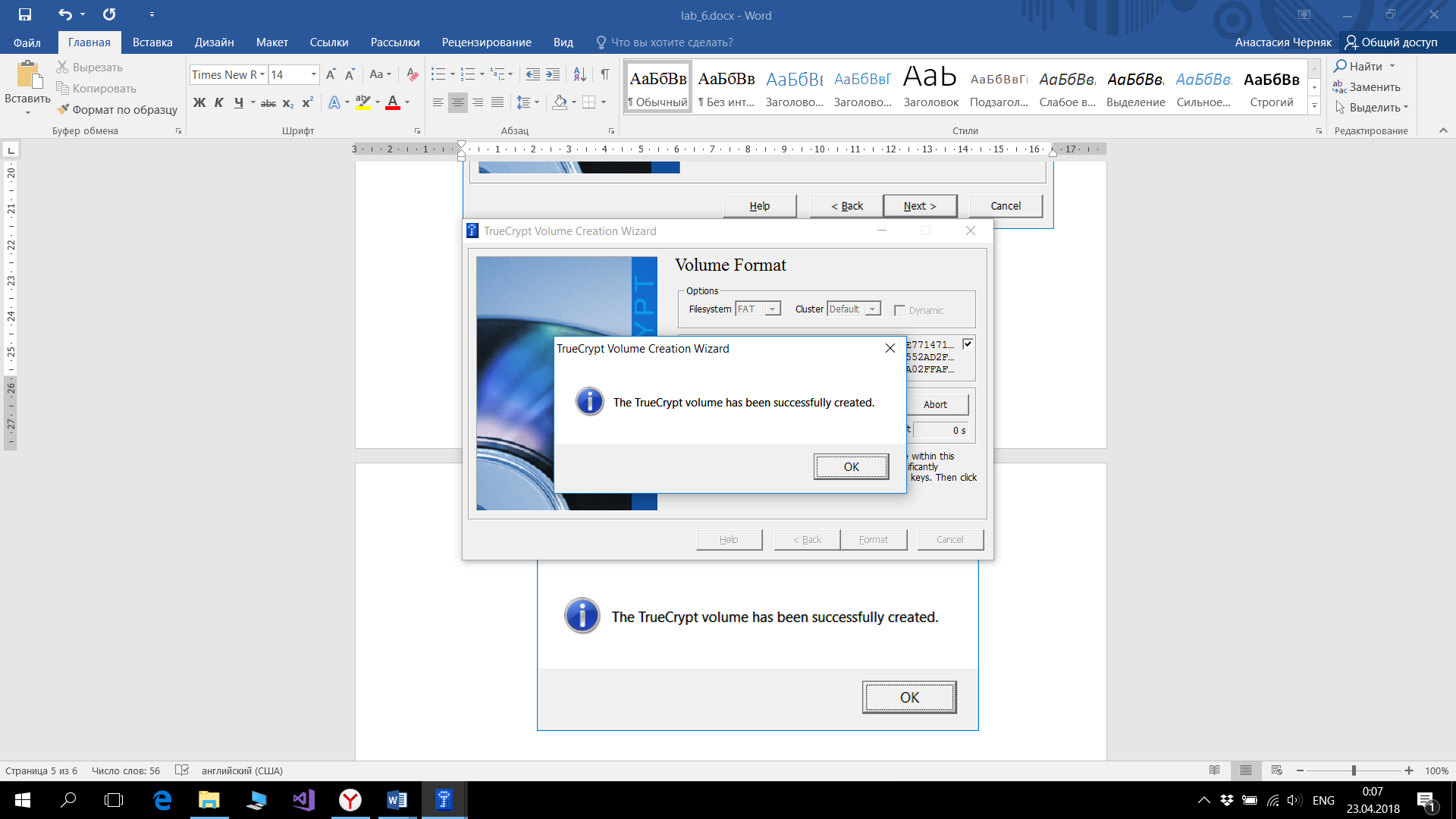


Рисунок 6.8 – Окно успешного создания.

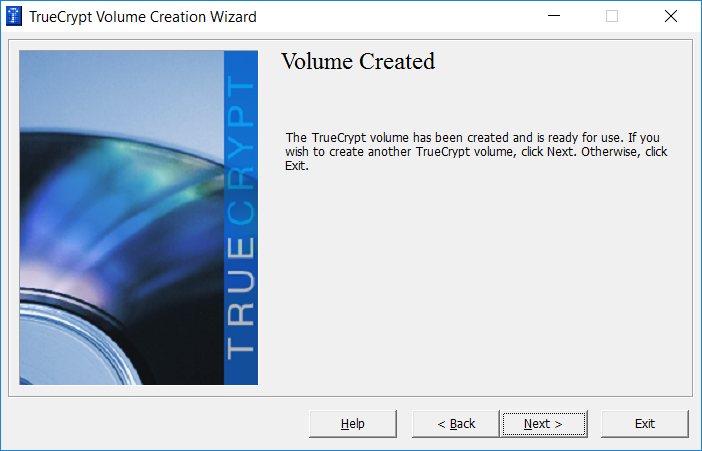


Рисунок 6.9 – Завершение создания.

1. Выбор диска, к которому будет cмонтирован контейнер.

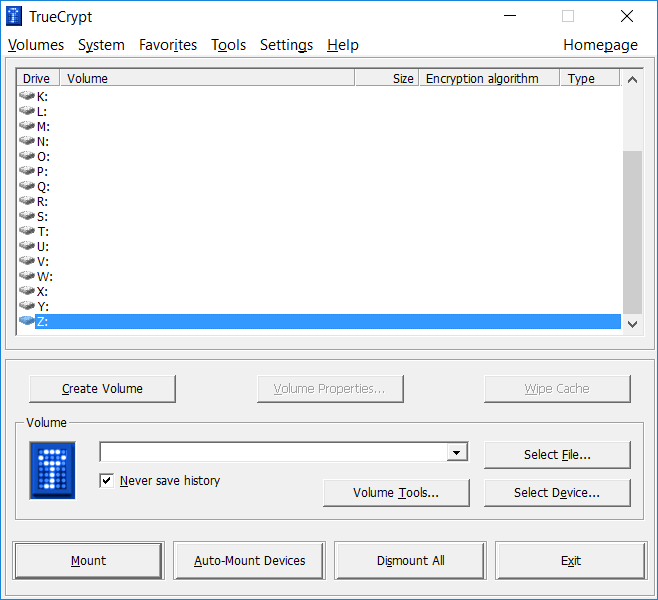


Рисунок 6.10 – Окно выбора диска.

1. Выбор файла, который был ранее создан.

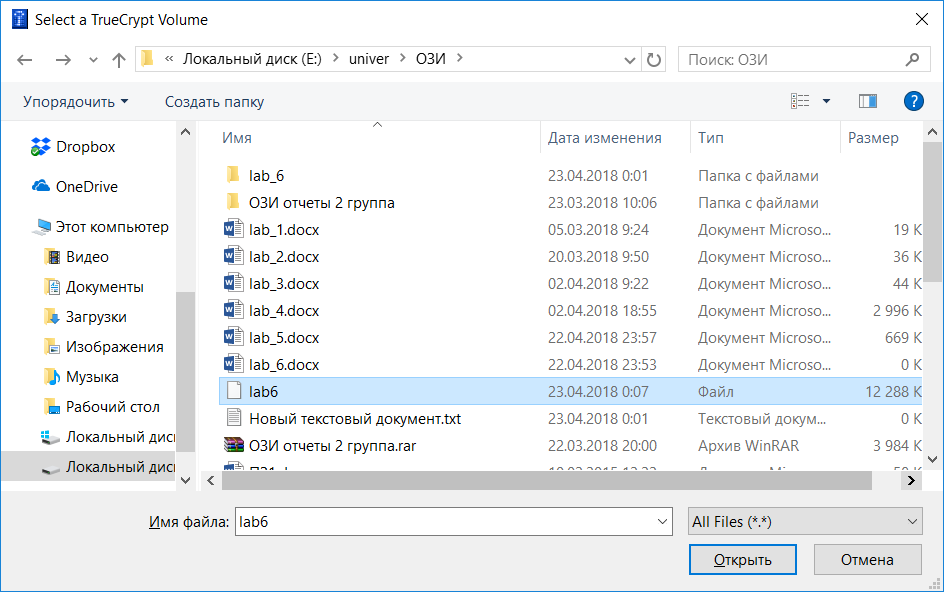


Рисунок 6.11 – Выбор файла.

1. Закрепление файла.

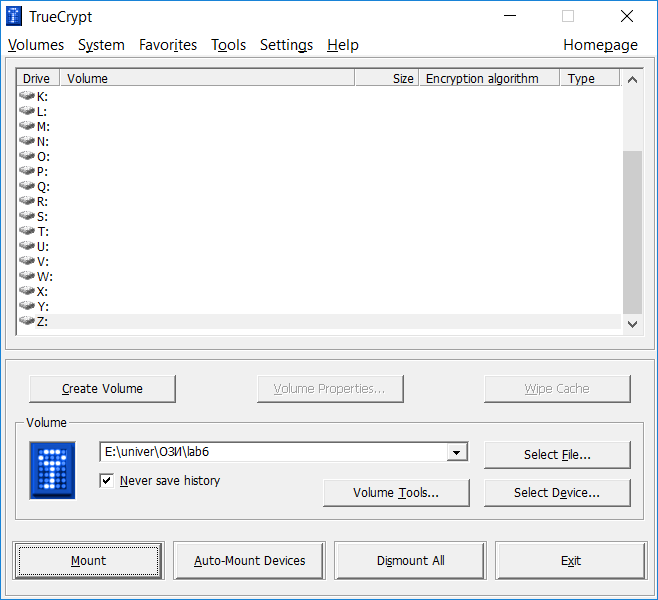


Рисунок 6.12 – Главное окно.

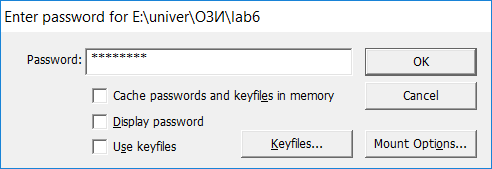


Рисунок 6.13 – Запрос пароля на прикрепление.

1. Проверка результатов проведенной работы.

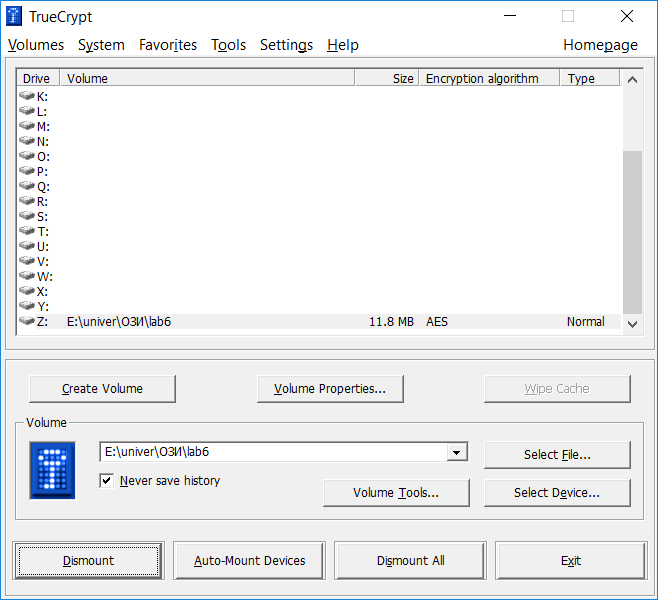


Рисунок 6.14 – Главное окно с просматриваемыми изменениями.

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

**Практическое занятие №7**

**Тема «Криптографическая защита информации»**

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

Помимо этого, современная криптография включает в себя асимметричные криптосистемы, системы электронной цифровой подпи си, 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. Есть шифры перестановки (transposition, permutation, P-блоки) и 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 группы моноалфавитных (код Цезаря) и полиалфавитных (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.



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

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

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

Схема обмена информацией такова:

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

Задание к выполнению:

Реализовать пример генерации секретного ключа методом Диффи-Хелмана. В качестве p и g взять два любых простых числа.

Секретный ключ 1-го человека должен быть: номер варианта + 8.

|  |  |
| --- | --- |
| Человек 1 | Человек 2 |
| Открытое простое число p=7 | Открытое простое число p=7 |
| Открытое простое число g=11 | Открытое простое число g=11 |
| Секретный ключ а=5+8=13 | Секретный ключ b=9 |
| Открытый ключ A=mod 7 =4 | Открытый ключ B=mod 7 =1 |
| Секретный ключ S= mod 7=1 | Секретный ключ S= mod 7=1 |
| S=1 | S=1 |

1. Зашифровать сообщение «хочузачетавтоматом» с использованием шифра Цезаря и полученного секретного ключа.

Пусть ключом k будет номер моего варианта, т.е. k=5.

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



Из этого следует, что в результате побуквенного шифрования фразы «хочузачетавтоматом» получаем «ъуьшмеьйчежчйсеьйс».

**Вывод:** я овладел основными криптографическими алгоритмами шифрования.

**Практическое занятие №8**

**Тема «Криптографическая защита информации»**

Цель: Овладеть 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.

**Практическая часть**

Реализовать пример шифрования сообщения в соответствии с вариантом:

|  |  |  |  |
| --- | --- | --- | --- |
| Номер варианта | Сообщение | P | Q |
| 8 | CBC | 29 | 73 |

1. Находим произведение p и q
2. Находим значение функции Эйлера для n
3. Выбирается произвольное целое e: 0 < e < n взаимно простое с значением функции Эйлера φ(n). В нашем примере возьмём e = 5. Пара чисел (e, n) объявляется открытым ключом шифра. В нашем примере (e, n) = (5, 2117)
4. Вычисляется целое число ***d*** (обратное число по модулю от е) из соотношения
5. Придаём ***k*** последовательно значения 1, 2, 3,.. до тех пор, пока не будет получено целое число ***d***

|  |  |  |  |
| --- | --- | --- | --- |
| k |  |  |  |
| 1 | 2016 | 5 | 403.4 |
| 2 |  |  | 806.6 |
| 3 |  |  | 1209.8 |
| 4 |  |  | 1613 |

Таблица 1. – Подбор значений k

Пара чисел (d, n) будет закрытым ключом шифра. В нашем примере (d, n) = (1613, 2117).

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

Числовые эквиваленты латинских букв указаны в таблице 1.

|  |  |  |
| --- | --- | --- |
| A – 1 | B – 2 | C – 3 |
| D – 4 | E – 5 | F – 6 |
| G – 7 | H – 8 | I – 9 |
| J – 10 | K – 11 | L – 12 |
| M – 13 | N – 14 | O – 15 |
| P – 16 | Q – 17 | R – 18 |
| S – 19 | T – 20 | U – 21 |
| V – 22 | W – 23 | X – 24 |
| Y – 25 | Z – 26 |  |

Таблица 2. – Числовые эквиваленты латинских букв

Расшифровка осуществляется по формуле:

**Вывод:** Я овладел навыками криптографической защиты информации.

**Практическое занятие №9**

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

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

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

1. **Произведения**

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

2**. Производные произведении**

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

3. **Компьютерные программы** (все виды программ)

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

Авторские нрава распространяются на:

* произведения, обнародованные (либо необнародованные, но находящиеся в какой-либо объективной форме) на территории РБ, независимо от гражданства авторов и их правопреемников;
* произведения авторов-граждан РБ (и их правопреемников), обнародованные (либо необнародованные, но находящиеся в какой-либо объективной форме) за пределами РБ;
* произведения авторов- 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.

**Личные неимущественные права:**

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

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

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

**Авторское право на составные произведения:**

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

**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.

**Субъекты авторского нрава и смежных нрав**

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.

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, 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.

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

**Авторский договор**

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

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

Постановочный договор заключается тогда, когда основным способом использования произведения является его публичное исполнение.

Сценарный договор – это договор, который регламентирует отношения, связанные с использованием текста, по которому снимается кинофильм, телефильм, делается радио- или телепередача, проводится массово-зрелищное мероприятие и т.д. Сценарный договор близок к постановочному договору, из рамок которого он постепенно выделился в самостоятельный вид. Сценарный договор предполагает, что произведение (сценарий) может быть использовано в измененном виде.

Договор о депонировании рукописи регулирует условия и порядок обнародования и последующего использования произведения, которое помещается на хранение в специальный информационный орган.

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

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

Авторский договор должен предусматривать способы использования произведения (конкретные права, передаваемые по данному договору); срок, на который передается право, и территорию, на которую распространяется действие этого права на указанный срок; размер вознаграждения и (или) порядок определения размера вознаграждения за каждый способ использования произведения, порядок и сроки его выплаты, а также другие условия, которые стороны сочтут необходимыми.

**Практическое занятие №10**

**Тема «Составление и оформление заявок на объекты**

**промышленной собственности»**

Описание изобретения наряду с формулой изобретения и графическими материалами 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.

**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.

**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.

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

**Состав заявки на выдачу патента**:

1. Заявление.
2. Описание изобретения.
3. Формула изобретения.
4. Чертежи.
5. Реферат.
6. Доверенность (если необходима).
7. Документ, удостоверяющий уплату пошлин.

**Правовая охрана объектов промышленной собственности (ОПС)** осуществляется в рамках государственной, а также международных (надгосударственных) патентных систем. Уполномоченные организации выдают от имени государства или группы государств соответствующий охранный документ. Охранный документ (патент, свидетельство) – это выдаваемый патентным органом от имени государства документ, который удостоверяет авторство, приоритет на объект промышленной собственности и исключительное право на его использование.

**Практическое занятие №11**

**Тема «Патентные исследования»**

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

**Теоретическое введение**

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

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

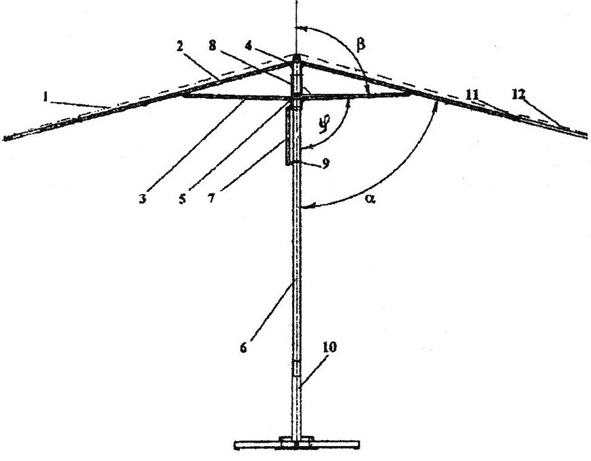
При определении уровня техники общедоступными считаются сведения, содержащиеся в источниках информации, с которыми любое лицо может ознакомиться сами либо о содержании которых ему может быть законным путем сообщено.

**Задание 1**

Изучить виды, содержание и порядок проведения патентных исследований.

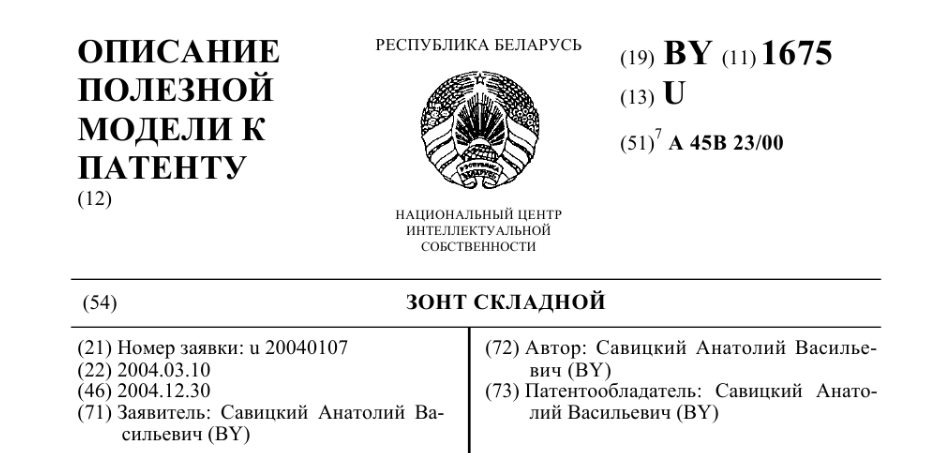
**Задание 2**

Рисунок 1 – Разработана конструкция зонта складного, отличающегося особенностями взаимного расположения конструктивных элементов.



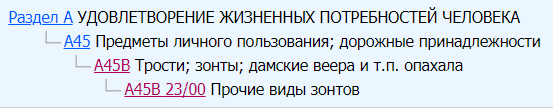
*Рис.1 Изображение зонта складного.*

Зонт складной, содержащий тент, каркас, состоящий из шарнирно связанных между собой несущих спиц и распорных спиц, которые, соответственно, посредством неподвижной и подвижной звездочек шарнирно соединены с опорным стержнем, на котором расположен движок механизма раскрытия и закрытия зонта, отличающийся тем, что верхний смежный угол между распорной спицей и опорным стержнем выполнен тупым, нижний смежный угол между распорной спицей и опорным стержнем выполнен острым, при этом движок механизма раскрытия и закрытия зонта выполнен в виде рукоятки, один конец которой связан с подвижной звездочкой, а другой конец посредством кольцевой серьги подвижно связан с опорным стержнем.



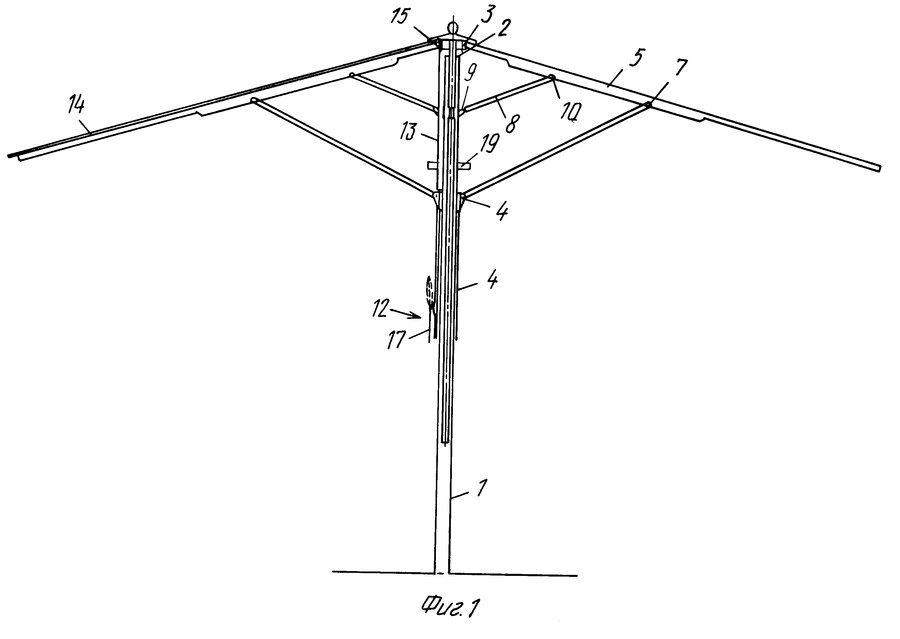
*Рис.2 Патент данной модели зонта*

Следовательно, поиск аналогово нужно производить в данной группе:



*Рис.3 Группа, к которой относится данный патент*

Проведенный патентный поиск по указанному классу, выявил следующие аналогичные по конструктивному выполнению патенты и полезные модели, приведенные на рисунках 4 –7 :

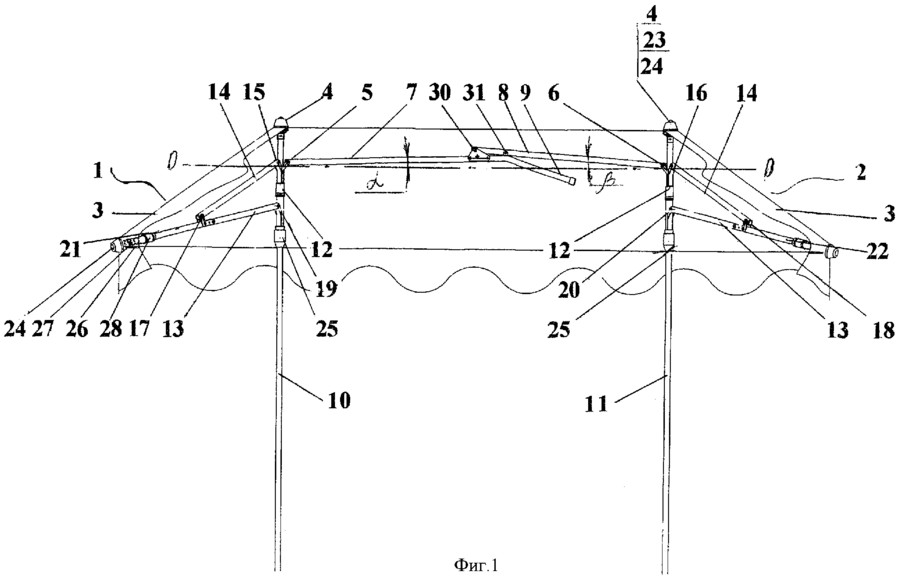


*Рис. 4 Зонт, в частности, стационарный зонт*

Зонт, в частности, стационарный зонт

Автор: Карл Клаус Бехер(DE)

Патент: 2126221

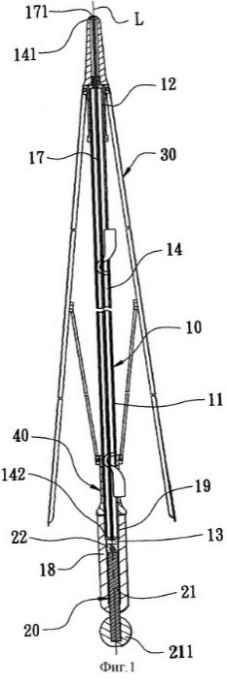


*Рис. 5 Складной навес*

Складной навес

Автор: Савицкий Анатолий Васильевич

Патент: 2347515

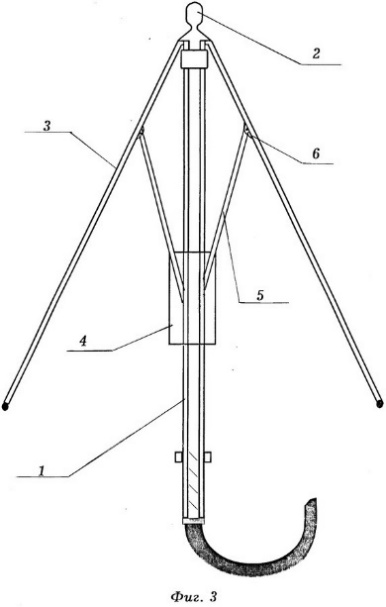


*Рис. 6 Выбрасывающий воду зонтик*

Выбрасывающий воду зонтик

Автор: Ванг Макс(TW)

Патент: 2255639



*Рис.7 Зонт детский*

Зонт детский.

Автор(ы): Котельников Владимир Александрович, Папиров Арнольд Михайлович, Зайцев Виктор Валерианович.

Патент: 2110201.

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Предмет поиска (объект исследования, его составные части) | Страна выдачи, вид и номер охранного документа. Классификационный индекс | Заявитель (патентообладатель), страна. Номер заявки, дата приоритета, конвенционный приоритет, дата публикации | Название изобретения (полезной модели, промышленного образца) | Сведения о действии охранного документа или причина его аннулирования (только для анализа патентной чистоты) |
| Складной зонт | Патент РФ № 2347515  МПК-8  A45B23/00 | Савицкий Анатолий Алексеевич.  Подача заявки: 2007-03-14  Публикация патента: 27-02-2009 | Складной навес | Действует |
| Патент РФ №  2110201  МПК-8  A45B23/00 | Котельников Владимир Александрович, Папиров Арнольд Михайлович, Зайцев Виктор Валерианович.  Подача заявки: 1997-11-28  Публикация патента:  1998-10-05 | Зонт детский | Действует |
| Патент РФ  № 2255639  МПК-8  A45B23/00 | ВАНГ Макс (TW).  Подача заявки: 2004-02-27  Публикация патента:  10-07-2005 | Выбрасывающий воду зонтик | Действует |
| Патент Китай  № 2126221  МПК-8  A45B23/00 | Карл Клаус Бехер (DE)  Подача заявки: 1997-03-20  Публикация патента:  20-02-1999 | Зонт, в частности, стационарный зонт | Действует |

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

**Вывод:** изучил виды, содержание и порядок проведения патентных исследований. Научился искать патенты и определять категорию, к которой относится патент, а также сравнивать патент с ранее существующими.

**Практическое занятие №12**

**Тема «Патентный поиск»**

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

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

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

<http://www1.fips.ru/wps/wcm/connect/content_ru/ru/inform_resources/inform_retrieval_system>

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

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

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

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

**Тема диплома:** Компьютерное программное средство для визуализации работы виртуального производственного комплекса на базе Android

**Результаты:**

**Национальный центр интеллектуальной собственности**

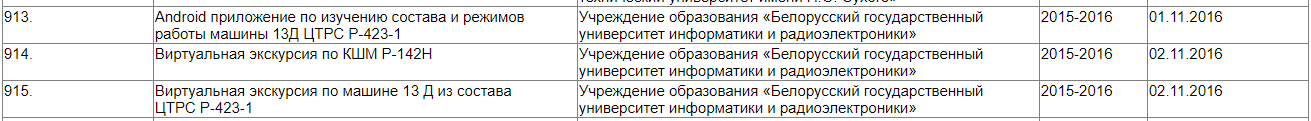


Рисунок 12.1 – Реестр зарегистрированных компьютерных программ 2016

**Российское агентство но патентам и товарным знакам (Роспатент)**

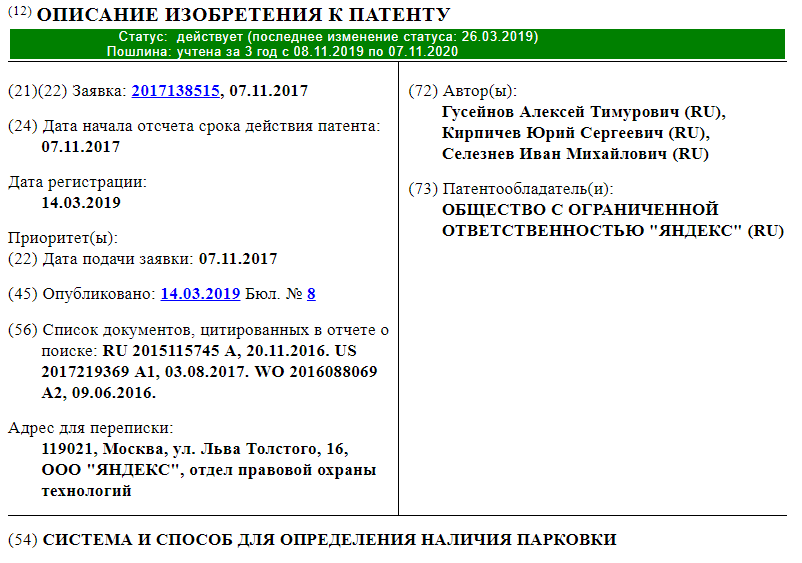


Рисунок 12.2 – Заявка: 2017138515

**Евразийские патенты**

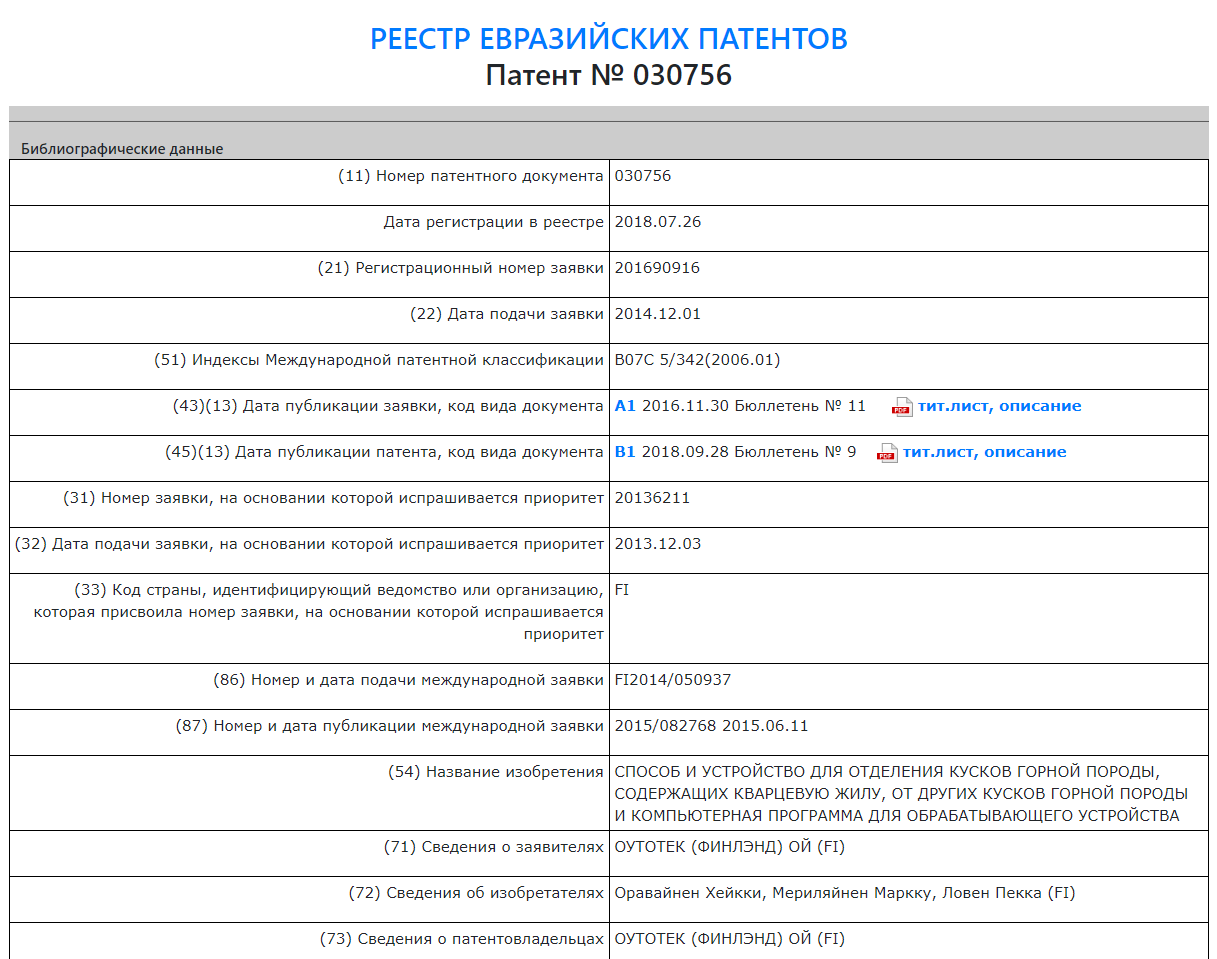


Рисунок 12.3 – Патент № 030756

**Европейский патентный офис**

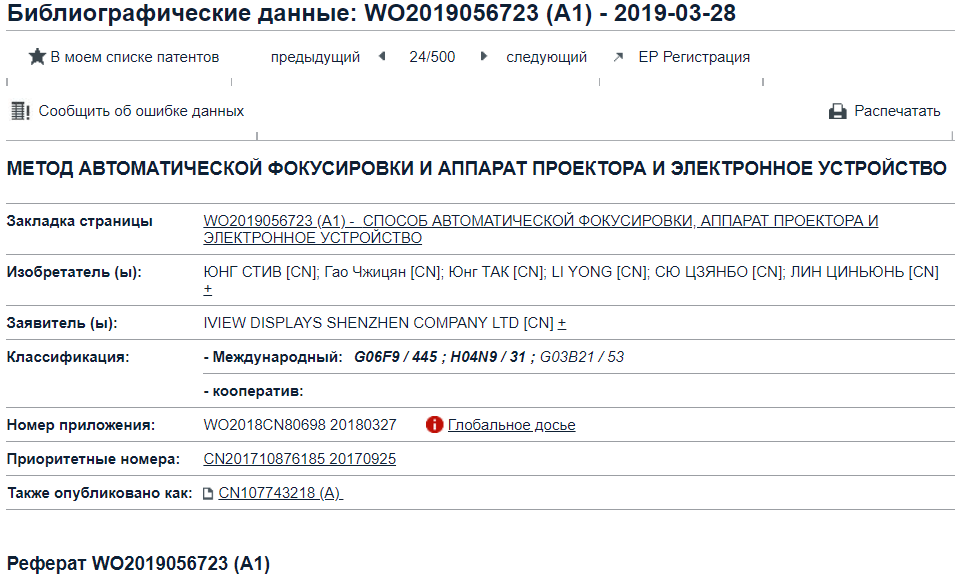


Рисунок 12.4 – Реферат WO2019056723 (A1)

**Практическое занятие №13**

**Тема «Регистрация компьютерных программ в Национальном центре интеллектуальной собственности»**

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

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

В результате проведения процедуры регистрации компьютерной программы:

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

**Подготовим комплект документов для регистрации компьютерной программы в НЦИС:**

|  |  |
| --- | --- |
| В Национальный центр  интеллектуальной собственности  220034, г. Минск, ул. Козлова, 20 | 05.04.2019  рег. № 228148869 |
|  |

**ЗАЯВКА**

**на оказание услуг по регистрации компьютерной программы**

|  |  |  |
| --- | --- | --- |
| 1. Заявитель | Матюх Арсений Артурович | |
| просит Национальный центр интеллектуальной собственности оказать услуги по регистрации компьютерной программы в соответствии с нижеприведенными данными | | |
| 1. Вид услуг | X | Стандартная регистрационная процедура (заявитель является автором) |
|  | Стандартная регистрационная процедура (заявитель не является автором) |
| X | Ускоренная регистрационная процедура  (заявитель является автором) |
|  | Ускоренная регистрационная процедура  (заявитель не является автором) |
| X | Оформление дополнительного экземпляра свидетельства |
| X | Оформление дополнительного экземпляра свидетельства на английском языке |
|  | Оформление изменений в отношении ранее зарегистрированной компьютерной программы |
| 1. Название компьютерной программы | Studac | |
| 1. Год создания компьютерной программы | 2020 | |
| 1. Авторы компьютерной программы | Матюх Арсений Артурович (28.10.1999) | |
| 1. Правообладатель компьютерной программы | Матюх Арсений Артурович | |
| 1. Основание принадлежности исключительного права на компьютерную программу | X | Создание компьютерной программы |
| X | Переход исключительного права в порядке служебного произведения |
|  | Приобретение исключительного права по договору |
|  | Правопреемство (в т.ч. наследование) в отношении исключительного права |
| 1. Данные для заключения договора на оказание услуг по регистрации компьютерной программы | Беларусь, г. Минск, ул. Бобруйская 25,  Н-р счета 1234 5678 9012 3456, срок 02/22,  Матюх Арсений Артурович, +375291615200,  cenia-v@mail.ru | |
| 1. Перечень прилагаемых материалов (с указанием носителя, кол-ва листов и т.д.) | экземпляр компьютерной программы, описание компьютерной программы, документы (заверенные копии), подтверждающие принадлежность исключительного права. | |
| Заявитель подтверждает свое понимание того, что регистрация компьютерной программы, о проведении которой просит Заявитель: 1) не является основанием или условием возникновения и осуществления авторского права на компьютерную программу, 2) осуществляется по инициативе Заявителя на основании предоставляемых им сведений (материалов), 3) в случае предоставления Заявителем для целей регистрации компьютерной программы недостоверных данных НЦИС или ассоциируемые с ним лица не могут рассматриваться ответственными за произведенную регистрацию компьютерной программы | | |
| 1. Дата Заявки и подпись Заявителя | 05.04.2019 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |

ПЕРЕЧЕНЬ СВЕДЕНИЙ (МАТЕРИАЛОВ),

|  |  |
| --- | --- |
| Вид сведений (материалов) | Примечания (форма представления, конкретные данные, которые должны содержаться в материалах и т.д.) |
| 1. Экземпляр компьютерной программы | Экземпляр программного обеспечения Studac для платформ Windows, Android IOS на электронном носителе |
| 2. Описание компьютерной  программы | Программное средство предназначено для ведения электронного расписания ВУЗов с возможностью динамического изменения в базе данных. Studac представляет собой программный комплекс для создание студенческого аккаунта с электронным расписанием и виртуальным электронным пропуском.  Перечень файлов: Studac.exe, Studac.apk, Studac.ipa. Язык программирования: C#.  Операционные системы: Windows 10, Android 5.0 и выше, IOS 10 и выше. |