Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Электронная тетрадь**

по Основам Защиты Информации

Студент: Бельский А.А.

ФИТ 2 курс 2 группа

Преподаватель: Берников В.О.

Минск 2020

**Практическое занятие №1**

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

**Цель работы:** изучить концепцию национальной безопасности Республики Беларусь.

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

**Основными национальными интересами в информационной сфере являются:**

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

**Основные источники угроз в ИТ-сфере являются:**

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

**В информационной сфере внутренними источниками угроз национальной безопасности являются:**

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

**В информационной сфере внешними источниками угроз национальной безопасности являются:**

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

**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»**

**Цель работы:** научиться решать задачи разработки средств защиты для обеспечения максимальной эффективности объекта в условиях несанкционированного доступа.

**Теоретическое введение**

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

– законодательные (правовые);

– организационные;

– технические;

– комплексные.

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 *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:

|  |  |
| --- | --- |
|  | (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 (2.1) – (2.2) 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, т.е. если:

|  |  |
| --- | --- |
|  | (2.12) |

то:

|  |  |
| --- | --- |
|  | (2.13) |

В этом случае (2.11) и (2.12) принимают вид:

|  |  |
| --- | --- |
|  | (2.14) |

Или:

|  |  |
| --- | --- |
|  | (2.15) |

где Cдоп — допустимые расходы на защиту.

**Задание на выполнение**

**Исходные данные.** Положительный эффект функционирования объекта: . Положительный эффект функционирования объекта с учетом воздействия несанкционированного доступа: . Коэффициент снижения негативного воздействия несанкционированного доступа на эффективность функционирования объекта: . Стоимость средств защиты: .

**Решение.** Определим уменьшение положительного эффекта функционирования объекта, вызванное воздействием несанкционированного доступа используя формулу (2.1):



Пусть эта величина согласно формуле (2.3) также представляет собой материальный ущерб, вызванный уменьшением эффективности функционирования объекта.



Определим относительную эффективность функционирования объекта по формуле (2.2):



Определим уменьшение положительного эффекта функционирования объекта согласно формуле (2.4), вызванное воздействием несанкционированного доступа, при наличии средств защиты.



Определим положительный эффект функционирования объекта с учетом воздействия несанкционированного доступа при наличии средств защиты по формуле (2.9):



Определим относительную эффективность функционирования объекта при наличии средств защиты по формуле (2.6):



Определим суммарный ущерб объекту при наличии средств защиты по формуле (2.8):



Для обеспечения защиты объектов информационной безопасности должны быть соответствующие правовые акты, устанавливающие порядок защиты и ответственность за его нарушение.

**Практическое занятие №3**

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

**Цель работы:** разработать проект политики информационной безопасности бизнес-компании.

По мере того, как процесс информатизации большинства областей деятельности Республики Беларусь, правительства, социальной сферы, бизнеса и т.д. развивается быстрыми темпами встаёт вопрос о комплексном подходе к защите информации. Политики информационной безопасности направлены на решение этой серьёзной проблемы. Под политиками информационной безопасности понимают формальное изложение правил поведения лиц, получающих доступ к конфиденциальным данным в корпоративной информационной системе. Корректно разработанные и остающиеся актуальными они отражают мнение руководства по вопросу информационной безопасности, также связывают воедино все методы защиты информации, позволяют разработать единые стандарты в области защиты информации и регламентируют работу сотрудников. Политики информационной безопасности являются основой для дальнейшей разработки документов по обеспечению безопасности стандартов, процедур, регламентов должностных инструкций.

Актуальность и необходимость внедрения политик информационной безопасности для компаний объясняется необходимостью создания механизма управления и планирования информационной безопасности. Также политики информационной безопасности позволяют совершенствовать следующие направления деятельности компании:

* поддержка непрерывности бизнеса;
* повышение уровня доверия к компании;
* привлечение инвесторов;
* минимизация рисков бизнеса с помощью защиты своих интересов в информационной сфере;
* повышение качества деятельности по обеспечению информационной безопасности;
* снижение издержек.

Естественно, что совершенствование направлений деятельности организации зависит от грамотности составления политики безопасности.

Политики информационной безопасности определяют стратегию и тактику построения системы защиты информации. Стратегическая часть связана со стратегией развития бизнеса компании и развитием её стратегии. Тактическая часть в свою очередь подробно описывает правила безопасности. В соответствии с определением политики информационной безопасности и рекомендациями международных стандартов в области планирования и управления политиками информационной безопасности, политики должны содержать:

* определение предмета задач и целей;
* условия применения и их ограничения;
* отражение позиции руководства в отношении выполнения политики информационной безопасности и создания комплексной системы информационной безопасности;
* определение прав и обязанностей сотрудников;
* определение границ ответственности сотрудников за выполнение политики информационной безопасности;
* порядок действий в случае нарушения политики безопасности.

Как правило основная ошибка заключается в отсутствии в компании формализованных, зафиксированных и утвержденных процессов обеспечения информационной безопасности. Эти процессы должны определять единую техническую политику с точки зрения обеспечения информационной безопасности и планы развития компании.

Основные положения информационной безопасности и позиция руководства компании прописываются в концепции информационной безопасности. Концепция информационной безопасности реализуется в частных политиках информационной безопасности, процедурах, руководствах и стандартах, обеспечивающих детальную интерпретацию положения концепции информационной безопасности для сотрудников, партнёров и клиентов компании. Эта структура руководящих документов и называется политикой информационной безопасности (рисунок 1).

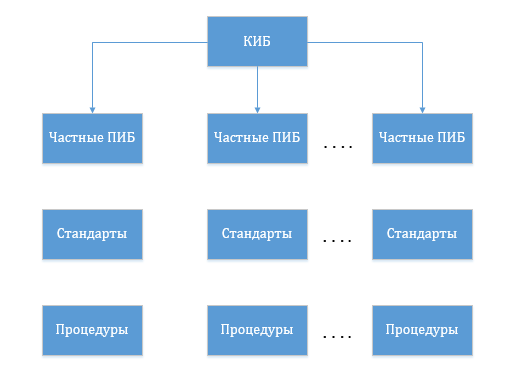


Рис. 3.1 – Структура руководящих документов ПИБ

Частные политики информационной безопасности определяют почему компания защищает свою информацию. Стандарты обозначают, что компания намерена предпринимать меры для реализации и управления безопасностью информации. Процедуры описывают как компания будет выполнять требования, описанные в высокоуровневых документах, частной политике и руководствах.

При разработке каждой новой политики информационной безопасности составляются свои руководства, стандарты и процедуры. У нескольких разработанных частных политик могут быть одинаковые пересекающие друг друга стандарты и процедуры.

Таким образом политика информационной безопасности является неотъемлемой частью систем установления режима информационной безопасности и контроля за ним систем информационной безопасности и систем управления информационной безопасности соответственно.

Для выполнения лабораторной работы будет выбрана структура компании ООО «Яринвестстрой» (рисунок 2).

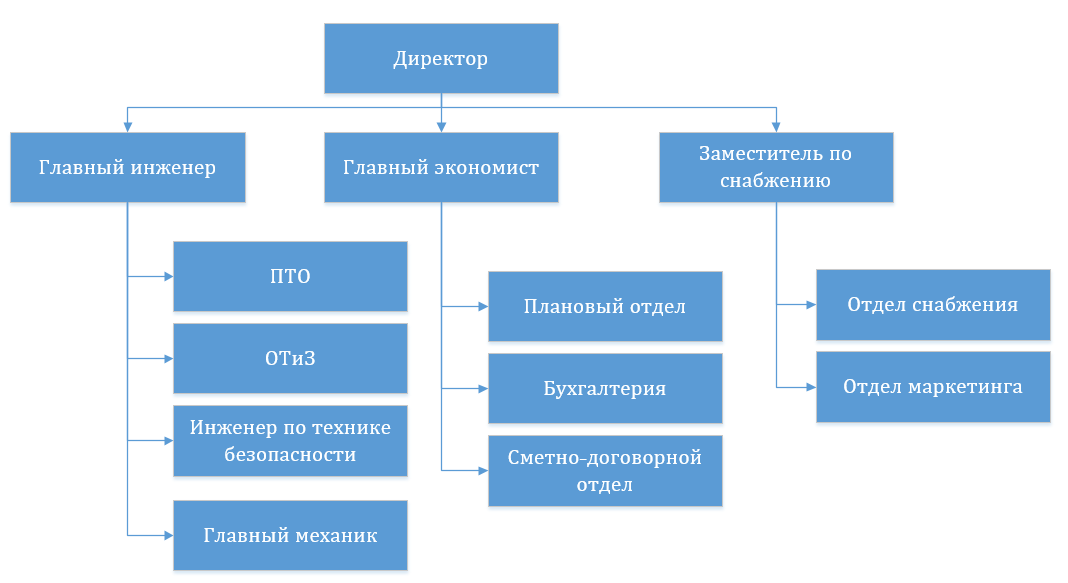


Рис. 3.2 – Структура ООО «Яринвестстрой»

Организационная структура компании состоит из следующих отделов:

* плановый отдел;
* производственно-технический отдел;
* отдел труда и заработной платы;
* сметно-договорной отдел;
* отдел снабжения;
* отдел маркетинга;
* бухгалтерия.

Главный инженер – занимается производственной и технической деятельностью, отвечает за организацию труда и его безопасность.

Производственно-технический отдел – организует и контролирует ведение исполнительной документации, организует и проводит техни­ческую учебу инженерно-технических работников, а также професси­ональную подготовку рабочих.

Главный механик – участвует в определении потребности в строи­тельных машинах и механизмах для строящихся объектов и в разработке планов механизации работ.

Организация труда и заработной платы – занимается задачами оказания помощи в подготовке плановых заданий бригадам, подготовка нормативной базы по организации труда, ведение отчетности по затратам труда.

Инженер по технике – безопасности обучает работников; безопасным методам производства работ, проводит инструктаж, контролирует соблюдение требований безопасности.

Главный экономист – отвечает за плановую работу и экономический анализ производственной и коммерческой деятельности.

Плановый отдел – разрабатывает годовые и оперативно-производственные планы работы строительно-монтажного управления и производственных подразделений.

Бухгалтерия – отдел, отвечающий за составления отчётности о приходе и расходе финансовых средств.

Сметно-договорной отдел – получает от заказчиков проектно-сметную документацию на планируемые к строительству объекты, организует ее изучение.

Заместитель начальника по снабжению – организует работу по обеспечению строительства объектов материальными ресурсами, для чего ведет маркетинговую работу и заключает договора на поставку материальных ресурсов через отдел снабжения и группу маркетинга.

Отдел снабжения – определяет потребность в строительных материалах, изделиях и конструкциях инструменте, инвентаре, спецодежде.

Эффективность управления деятельностью зависит оттого, насколько грамотно сформирована организационная структура управления и насколько она соответствует цели деятельности организации.

В настоящее время под организационной структурой понимается упорядоченная совокупность устойчиво взаимосвязанных элементов, обеспечивающих функционирование и развитие организации как единого целого. Структура управления определяется также как форма разделения и кооперации управленческой деятельности. Можно сказать, что структура управления есть не что иное, как оптимальное распределение работы, прав и ответственности, порядка и форм взаимодействия между членами коллектива организации.

Составляющими организационных структур являются:

* элементы организационных структур управления – службы или органы аппарата управления, а также отдельные работники этих служб (органов);
* организационные отношения – отношения (связи) между подразделениями организации, уровнями ее управления, персоналом, посредством которых реализуются функции управления;
* уровни управления – совокупность прав, обязанностей и ответственности, характерная для должностных лиц, занимающих определенную ступень в иерархической структуре организации.

Все множество потенциальных угроз безопасности информации делится на три класса по природе их возникновения:

* антропогенные;
* техногенные;
* естественные (природные).

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

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

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

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

На сегодняшний день для большинства предприятий и банковских систем самыми актуальными являются 3 угрозы:

* угроза доступности;
* угроза целостности;
* угроза конфиденциальности.

Угроза доступности (отказа служб) возникает всякий раз, когда в результате преднамеренных действий, предпринимаемых другим пользователем или злоумышленником, блокируется доступ к некоторому ресурсу вычислительной системы. Реально блокирование может быть постоянным – запрашиваемый ресурс никогда не будет получен, или оно может вызывать только задержку запрашиваемого ресурса, достаточно долгую для того, чтобы он стал бесполезным. В этих случаях говорят, что ресурс исчерпан.

Доступность информации – свойство системы (среды, средств и технологии обработки), в которой циркулирует информация, характеризующееся способностью обеспечивать своевременный беспрепятственный доступ субъектов к интересующей их информации и готовность соответствующих автоматизированных служб к обслуживанию поступающих от субъектов запросов всегда, когда возникает в этом необходимость.

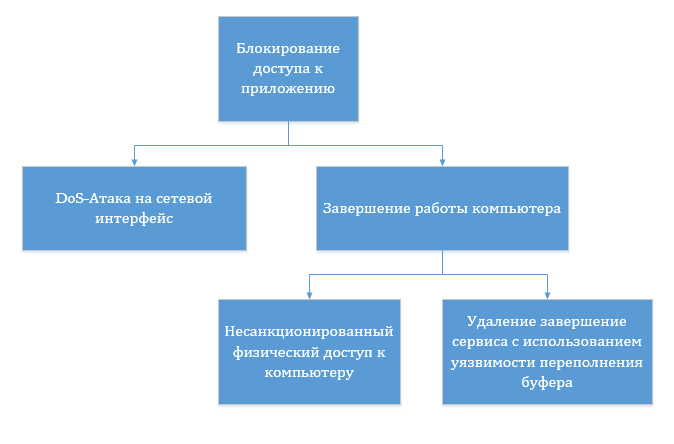


Рис. 3.3 – Дерево угрозы блокирования доступа к сетевому приложению

Самыми частыми и самыми опасными (с точки зрения размера ущерба) являются непреднамеренные ошибки штатных пользователей, операторов, системных администраторов и других лиц, обслуживающих ИС.  
Иногда такие ошибки и являются собственно угрозами (неправильно введенные данные или ошибка в программе, вызвавшая крах системы), иногда они создают уязвимые места, которыми могут воспользоваться злоумышленники. По некоторым данным, до 65% потерь – следствие непреднамеренных ошибок. Пожары и наводнения не приносят столько бед, сколько [безграмотность](https://pandia.ru/text/category/bezgramotnostmz/) и небрежность в работе. Самый радикальный способ борьбы с непреднамеренными ошибками – максимальная автоматизация и строгий контроль.

Угрозы доступности могут выглядеть грубо – как повреждение или даже разрушение оборудования (в том числе носителей данных) и может вызываться естественными причинами (чаще всего – грозами). Опасны протечки [водопровода](https://pandia.ru/text/category/vodoprovod/) и [отопительной системы](https://pandia.ru/text/category/otopitelmznie_sistemi/), в сильную жару ломаются кондиционеры, установленные в серверных залах, набитых дорогостоящим оборудованием. Общеизвестно, что периодически необходимо производить резервное копирование данных. Однако даже если это предложение выполняется, резервные носители обычно хранят небрежно, не обеспечивая их защиту от вредного воздействия окружающей среды.

Пример удаленного потребления ресурсов – атака, получившая наименование **«**SYN-наводнение**»**. Она представляет собой попытку переполнить таблицу «полуоткрытых» TCP-соединений сервера (установление соединений начинается, но не заканчивается), что приводит к затруднению установления новых соединений пользователей, то есть сервер блокируется.

Угроза нарушения целостности включает в себя любое умышленное изменение информации, хранящейся в вычислительной системе или передаваемой из одной системы в другую, в том числе и несанкционированное изменение информации при случайных ошибках программного или аппаратного обеспечения. Санкционированными изменениями являются те, которые сделаны уполномоченными лицами с обоснованной целью (например, периодическая запланированная коррекция некоторой базы данных).

Целостность информации – существование информации в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).

Угроза нарушения конфиденциальности заключается в том, что информация становится известной тому, кто не располагает полномочиями доступа к ней. Иногда, в связи с угрозой нарушения конфиденциальности, используется термин «утечка».

Существует различие между статической и динамической целостностью. С целью нарушения статической целостности злоумышленник может: ввести неверные данные; изменить данные. Иногда изменяются содержательные данные, иногда – служебная информация. Угрозами динамической целостности являются нарушение атомарности транзакций, переупорядочение, кража, дублирование данных или внесение дополнительных сообщений (сетевых пакетов и т. п.). Соответствующие действия в сетевой среде называются активным прослушиванием.

Угрозой целостности является не только фальсификация или изменение данных, но и отказ от совершенных действий. Если нет средств обеспечить «неотказуемость», компьютерные данные не могут рассматриваться в качестве доказательства. Потенциально уязвимы с точки зрения нарушения целостности не только данные, но и программы. Внедрение вредоносного ПО – пример подобного нарушения.

Актуальной и весьма опасной угрозой является внедрение руткитов (набор файлов, устанавливаемых в системе с целью изменения ее стандартной функциональности вредоносным и скрытным образом), ботов (программа, автоматически выполняющая некоторую миссию; группа компьютеров, на которой функционируют однотипные боты, называется бот-сетью), потайных ходов (вредоносная программа, слушающая команды на определенных TCP-или UDP-портах) и шпионского программного обеспечения (вредоносное ПО, нацеленное на компрометацию конфиденциальных данных пользователя. Например, «троянцы» Back Orifice и Netbus позволяют получить контроль над пользовательскими системами с различными вариантами MS-Windows.

Конфиденциальность информации – субъективно определяемая (приписываемая) характеристика (свойство) информации, указывающая на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемая способностью системы (среды) сохранять указанную информацию в тайне от субъектов, не имеющих полномочий доступа к ней.

Конфиденциальную информацию можно разделить на предметную и служебную. Служебная информация (например, пароли пользователей) не относится к определенной предметной области, в информационной системе она играет техническую роль, но ее раскрытие особенно опасно, поскольку оно чревато получением несанкционированного доступа ко всей информации, в том числе предметной. Опасной нетехнической угрозой конфиденциальности являются методы морально-психологического воздействия, такие как «маскарад» – выполнение действий под видом лица, обладающего полномочиями для доступа к данным. К неприятным угрозам, от которых трудно защищаться, можно отнести злоупотребление полномочиями. На многих типах систем привилегированный пользователь (например, системный администратор) способен прочитать любой (незашифрованный) файл, получить доступ к почте любого пользователя.

В настоящее время наиболее распространены так называемые «фишинговые» атаки. Фишинг (fishing – рыбная ловля) – вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей - логинам и паролям. Это достигается путём проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, от имени банков, сервисов (Rambler, Mail.ru) или внутри социальных сетей (Facebook, Вконтакте, Одноклассники). Целью фишеров сегодня являются [клиенты банков](https://pandia.ru/text/category/klienti_banka/) и электронных [платёжных систем](https://pandia.ru/text/category/platyozhnie_sistemi/). Так, например, в США, маскируясь под Службу внутренних доходов, фишеры собрали значительные данные о налогоплательщиках в 2009 году.

Источники угроз по отношению к инфраструктуре ООО «Яринвестстрой» могут быть как внешними, так и внутренними.

Источниками внутренних угроз являются:

* сотрудники организации;
* программное обеспечение;
* аппаратные средства.

К информационным угрозам относятся:

* несанкционированный доступ к информационным ресурсам;
* незаконное копирование данных в информационных системах;
* противозаконный сбор и использование информации;
* использование информационного оружия.

К программным угрозам относятся:

* использование ошибок и «дыр» в ПО;
* компьютерные вирусы и вредоносные программы;

К физическим угрозам относятся:

* уничтожение или разрушение средств обработки информации и связи;

Для предотвращения угроз требуется разработать меры защиты.

Практически в каждой компании установлена система контроля доступа. Сотрудникам выдаются специальные электронные пропуска, представляющие собой пластиковые карты или брелоки, которые содержат персональные коды доступа. Считыватели, устанавливаемые у входа в контролируемое помещение, распознают код идентификаторов. Информация поступает в систему контроля доступа, которая на основании анализа данных о владельце идентификатора, принимает решение о допуске или запрете прохода сотрудника на охраняемую территорию. В случае разрешения доступа, система приводит в действие исполнительные устройства, такие как электромеханические замки, турникеты, автоматические шлагбаумы или приводы ворот. В противном случае двери блокируются, включается сигнализация и оповещается охрана.

Построение надежной защиты включает оценку циркулирующей в компьютерной системе информации с целью уточнения степени ее конфиденциальности, анализа потенциальных угроз ее безопасности и установление необходимого режима ее защиты.

Отдельный раздел законопроекта "О коммерческой тайне", посвященный организации защиты коммерческой информации, определяет необходимый комплекс мероприятий по ее защите:

* установление особого режима конфиденциальности;
* ограничение доступа к конфиденциальной информации;
* использование организационных мер и технических средств защиты информации;
* осуществление контроля за соблюдением установленного режима конфиденциальности.

Установление особого режима конфиденциальности направлено на создание условий для обеспечения физической защиты носителей конфиденциальной информации. Как правило, особый режим конфиденциальности подразумевает:

* организацию охраны помещений, в которых содержатся носители конфиденциальной информации;
* установление режима работы в помещениях, в которых содержатся носители конфиденциальной информации;
* установление пропускного режима в помещения, содержащие носители конфиденциальной информации;
* закрепление технических средств обработки конфиденциальной информации за сотрудниками, определение персональной ответственности за их сохранность;
* установление порядка пользования носителями конфиденциальной информации (учет, хранение, передача другим должностным лицам, уничтожение, отчетность);
* организацию ремонта технических средств обработки конфиденциальной информации;

Требования устанавливаемого на предприятии особого режима конфиденциальности оформляются в виде организационно-распорядительных документов и доводятся для ознакомления до сотрудников предприятия.   
Ограничение доступа к конфиденциальной информации способствует созданию наиболее эффективных условий сохранности конфиденциальной информации. Необходимо четко определять круг сотрудников, допускаемых к конфиденциальной информации, к каким конкретно сведениям им разрешен доступ и полномочия сотрудников по доступу к конфиденциальной информации. Как показывает практика работы, для разработки необходимого комплекса мероприятий по защите информации желательно привлечение квалифицированных экспертов в области защиты информации.  
Традиционно для организации доступа к конфиденциальной информации использовались организационные меры, основанные на строгом соблюдении сотрудниками процедур допуска к информации, определяемых соответствующими инструкциями, приказами и другими нормативными документами. Однако с развитием компьютерных систем эти меры перестали обеспечивать необходимую безопасность информации. Появились и в настоящее время широко применяются специализированные программные и программно-аппаратные средства защиты информации, которые позволяют максимально автоматизировать процедуры доступа к информации и обеспечить при этом требуемую степень ее защиты. Подробнее о существующих средствах защиты информации мы остановимся ниже. Осуществление контроля за соблюдением установленного режима конфиденциальности предусматривает проверку соответствия организации защиты информации установленным требованиям, а также оценку эффективности применяемых мер защиты информации. Как правило, контроль осуществляется в виде плановых и внеплановых проверок силами своих сотрудников или с привлечением других организаций, которые специализируются в этой области. По результатам проверок специалистами по защите информации проводится необходимый анализ с составлением отчета, который включает:

* вывод о соответствии проводимых на предприятии мероприятий установленным требованиям;
* оценка реальной эффективности применяемых на предприятии мер защиты информации и предложения по их совершенствованию.

Обеспечение и реализация перечисленных выше мероприятий потребует создания на предприятии соответствующих органов защиты информации. Эффективность защиты информации на предприятии во многом будет определяться тем, насколько правильно выбрана структура органа защиты информации и квалифицированы его сотрудники. Как правило, органы защиты информации представляют собой самостоятельные подразделения, однако на практике часто практикуется и назначение одного из штатных специалистов предприятия ответственным за обеспечение защиты информации. Однако такая форма оправдана в тех случаях, когда объем необходимых мероприятий по защите информации небольшой и создание отдельного подразделения экономически не выгодно.  Созданием органов защиты информации на предприятии завершается построение системы защиты информации, под которой понимается совокупность органов защиты информации или отдельных исполнителей, используемые ими средства защиты информации, а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами по защите информации.

Как уже отмечалось выше, эффективность защиты информации в автоматизированных системах достигается применением средств защиты информации (СЗИ). Под средством защиты информации понимается техническое, программное средство или материал, предназначенные или используемые для защиты информации. В настоящее время на рынке представлено большое разнообразие средств защиты информации, которые условно можно разделить на несколько групп:

* средства, обеспечивающие разграничение доступа к информации в автоматизированных системах;
* средства, обеспечивающие защиту информации при передаче ее по каналам связи;
* средства, обеспечивающие защиту от утечки информации по различным физическим полям, возникающим при работе технических средств автоматизированных систем;
* средства, обеспечивающие защиту от воздействия программ-вирусов;
* материалы, обеспечивающие безопасность хранения, транспортировки носителей информации и защиту их от копирования.

Основное назначение средств защиты первой группы - разграничение доступа к локальным и сетевым информационным ресурсам автоматизированных систем. СЗИ этой группы обеспечивают:

* идентификацию и аутентификацию пользователей автоматизированных систем;
* разграничение доступа зарегистрированных пользователей к информационным ресурсам;
* регистрацию действий пользователей;
* защиту загрузки операционной системы с гибких магнитных дисков и CD-ROM;
* контроль целостности СЗИ и информационных ресурсов.

В качестве идентификаторов пользователей применяются, как правило, условные обозначения в виде набора символов. Для аутентификации пользователей применяются пароли.

Разграничение доступа зарегистрированных пользователей к информационным ресурсам осуществляется СЗИ в соответствии с установленными для пользователей полномочиями. Как правило, СЗИ обеспечивают разграничение доступа к гибким и жестким дискам, логическим дискам, директориям, файлам, портам и устройствам. Полномочия пользователей устанавливаются с помощью специальных настроек СЗИ. По отношению к информационным ресурсам средствами защиты могут устанавливаться такие полномочия, как разрешение чтения, записи, создания, запуска исполняемых файлов и другие. Системы защиты информации предусматривают ведение специального журнала, в котором регистрируются определенные события, связанные с действиями пользователей, например, запись (модификация) файла, запуск программы, вывод на печать и другие, а также попытки несанкционированного доступа к защищаемым ресурсам и их результат. Особо стоит отметить наличие в СЗИ защиты загрузки операционной системы с гибких магнитных дисков и CD-ROM, которая обеспечивает защиту самих средств защиты от "взлома" с использованием специальных технологий. В различных СЗИ существуют программные и аппаратно-программные реализации этой защиты, однако практика показывает, что программная реализация не обеспечивает необходимой стойкости.  
Контроль целостности средств защиты и защищаемых файлов заключается в подсчете и сравнении контрольных сумм файлов. При этом используются различной сложности алгоритмы подсчета контрольных сумм. Несмотря на функциональную общность средств защиты информации данной группы, СЗИ различных производителей различаются:

* условиями функционирования (операционная среда, аппаратная платформа, автономные компьютеры и вычислительные сети);
* сложностью настройки и управления параметрами СЗИ;
* используемыми типами идентификаторов;
* перечнем событий, подлежащих регистрации;
* стоимостью средств защиты.

С развитием сетевых технологий появился новый тип СЗИ - межсетевые экраны (firewalls), которые обеспечивают решение таких задач, как защита подключений к внешним сетям, разграничение доступа между сегментами корпоративной сети, защита корпоративных потоков данных, передаваемых по открытым сетям.

Широкое развитие корпоративных сетей, интеграция их с информационными системами общего пользования помимо явных преимуществ порождает новые угрозы безопасности информации. Причины возникновения новых угроз характеризуются:

* сложностью и разнородностью используемого программного и аппаратного обеспечения корпоративных сетей;
* большим числом узлов сети, участвующих в электронном обмене информацией, их территориальной распределенностью и отсутствием возможности контроля всех настроек;
* доступностью информации корпоративных систем внешним пользователям (клиентам, партнерам и пр.) из-за ее расположения на физически соединенных носителях.

Применение описанных выше средств защиты информации, а также встроенных в операционные системы механизмов защиты информации не позволяет в полной мере ликвидировать эти угрозы. Наличие постоянных или временных физических соединений является важнейшим фактором, который влияет на повышение уязвимостей корпоративных систем из-за брешей в используемых защитных и программных средствах и утечки информации вследствие ошибочных или неграмотных действий персонала. Обеспечение требуемой защиты информационных ресурсов предприятий в этих условиях достигается применением дополнительных инструментальных средств. К их числу относятся:

* средства анализа защищенности операционных систем и сетевых сервисов;
* средства обнаружения опасных информационных воздействий (атак) в сетях.

Средства анализа защищенности операционных систем позволяют осуществлять ревизию механизмов разграничения доступа, идентификации и аутентификации, средств мониторинга, аудита и других компонентов операционных систем с точки зрения соответствия их настроек и конфигурации установленным в организации. Кроме этого, средствами данного класса проводится контроль целостности и неизменности программных средств и системных установок и проверка наличия уязвимостей системных и прикладных служб. Как правило, такие проверки проводятся с использованием базы данных уязвимостей операционных систем и сервисных служб, которые могут обновляться по мере выявления новых уязвимостей.   
К числу средств анализа данного класса относится программное средство администратора ОС Solaris ASET (Automated Security Tool), которое входит в состав ОС Solaris, пакет программ COPS (Computer Oracle and Password System) для администраторов Unix-систем, и система System Scanner (SS) фирмы Internet Security System Inc. для анализа и управления защищенность операционных систем Unix и Windows NT/ 95/98.  
Использование в сетях Internet/Intranet протоколов TCP/IP, которые характеризуются наличием в них неустранимых уязвимостей, привело к появлению в последнее время новых разновидностей информационных воздействий на сетевые сервисы и представляющих реальную угрозу защищенности информации. Средства анализа защищенности сетевых сервисов применяются для оценки защищенности компьютерных сетей по отношению к внутренним и внешним атакам. По результатам анализа защищенности сетевых сервисов средствами генерируются отчеты, включающие в себя список обнаруженных уязвимостей, описание возможных угроз и рекомендации по их устранению. Поиск уязвимостей основывается на использовании базы данных, которая содержит широко известные уязвимости сетевых сервисных программ и может обновляться путем добавления новых уязвимостей.  
К числу средств анализа данного класса относится программа SATAN (автор В.Венема), Netprobe фирмы Qualix Group и Internet Scanner фирмы Internet Security System Inc. Наибольшая эффективность защиты информации достигается при комплексном использовании средств анализа защищенности и средств обнаружения опасных информационных воздействий (атак) в сетях. Средства обнаружения атак в сетях предназначены для осуществления контроля всего сетевого трафика, который проходит через защищаемый сегмент сети, и оперативного реагирование в случаях нападения на узлы корпоративной сети. Большинство средств данной группы при обнаружении атаки в сети оповещают администратора системы, регистрируют факт нападения в журнале системы и завершают соединение с атакующим узлом. Дополнительно, отдельные средства обнаружения атак позволяют автоматически реконфигурировать межсетевые экраны и маршрутизаторы в случае нападения на узлы корпоративной сети.

Обобщая все вышесказанное и учитывая возможные виды угрозы/атаки на торговую сеть, можем выделить следующие рекомендации, либо советы, следуя которым возможно снизить риски опасного воздействия и их последствий:

* вооруженная охрана магазинов торговой сети и офисов компании;
* четкая и строгая иерархия должностей и полномочий в компании. Каждый должен заниматься строго своим заданием;
* обязательная экстренная связь каждого магазина с милицией и пожарной службой (наличие кнопок экстренного вызова) и четкий инструктаж персонала на случай чрезвычайного происшествия;
* строгий подбор сотрудников с привлечением, при необходимости, милиции;
* защита главных серверов компании (если такие существуют) и важной корпоративной почты;
* использование новейших средств защиты (антивирусные продукты, фаерволлы) персональных компьютеров сотрудников и обязательное использование лишь лицензионных продуктов;
* разграничение доступа к финансовым отделам. Уборщица не должна знать номер банковского счета фирмы и тем более, его пароля;
* проведение регулярных бесед и инструктажей с сотрудниками;
* наличие как в магазинах, так и в офисах, наглядного отображения плана по работе во время чрезвычайных ситуаций.

Так же, эффективной мерой по защите является проведение тестовых экспериментов по атаке на фирму: наем специализированных людей, которые проведут атаку на сетевые ресурсы компании и выявят пробелы в защите. Данная операция безусловно является дорогостоящей, однако впоследствии, это сэкономит средства компании.

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

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

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

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

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

Прежде чем внедрять какие-либо решения по защите информации необходимо разработать политику безопасности, адекватную целям и задачам современной компании. В частности, политика безопасности должна описывать порядок предоставления и использования прав доступа пользователей, а также требования отчетности пользователей за свои действия в вопросах безопасности.

Система информационной безопасности (СИБ) окажется эффективной, если она будет надежно поддерживать выполнение правил политики безопасности, и наоборот.

Этапы построения политики безопасности – это внесение в описание объекта автоматизации структуры ценности и проведение анализа риска, и определение правил для любого процесса пользования данным видом доступа к ресурсам объекта автоматизации, имеющим данную степень ценности.

При этом политику безопасности желательно оформить в виде отдельного документа и утвердить руководством предприятия.

Опыт показывает, что для достижения удачных решений по защите информации кампаний необходимо сочетание правовых, организационных и технических мер. Это сочетание определяется конфиденциальностью защищаемой информации, характером опасности и наличием средств защиты. В общем случае технические меры безопасности составляют незначительную часть от общих мер защиты (правовых и организационных). Однако ни одну из них упускать нельзя. Каждая мера дополняет другую, и недостаток или отсутствие любого способа приведёт к нарушению защищённости.

Особое внимание при оценке эффективности системы защиты техническими средствами необходимо обратить на их надёжность и безотказность. При их эксплуатации имеют место поломки, сбои, отказы, вследствие чего они не обеспечивают выполнение задачи защиты. Отсюда задача обеспечения надлежащей надёжности технических средств обретает значительную важность, так как уровень, качество и безопасность защиты находятся в прямой зависимости от надёжности технических средств.

**Практическое занятие №4**

**Тема «Настройка Брандмауэра Windows»**

**Цель работы**: овладение навыками настройки и использования Брандмауэра Windows.

**Брандмауэр** (Межсетевой экран) – это аппаратный или программный комплекс, позволяющий проверять (фильтровать) входные и выходные потоки данных, проходящие через интернет или сеть. В случаи нарушения политики безопасности компьютера, брандмауэр блокирует эти данные (рисунок 4.1).

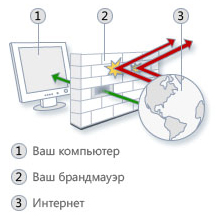


Рис. 4.1 – Принцип действия Брандмауэра

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

К числу таких служб и протоколов относятся:

* доступ к всемирной паутине WWW;
* программа электронной почты Send Mail;
* графическая оконная система X Windows.

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

Создание правила для программы на блокировку подключения состоит из следующих шагов:

Открываем «Мастер создания правила для входящего подключения» (рисунок 4.2).

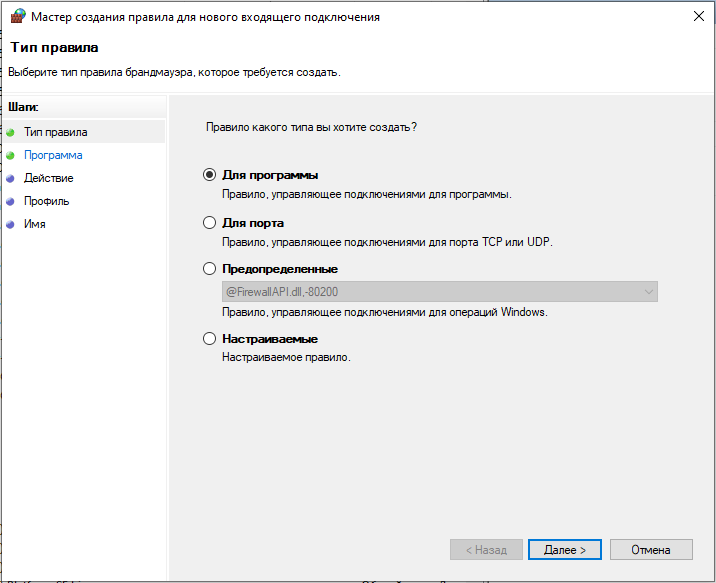


Рисунок 4.2 – Выбор типа правила

Указываем путь к программе(рисунок 4.3).

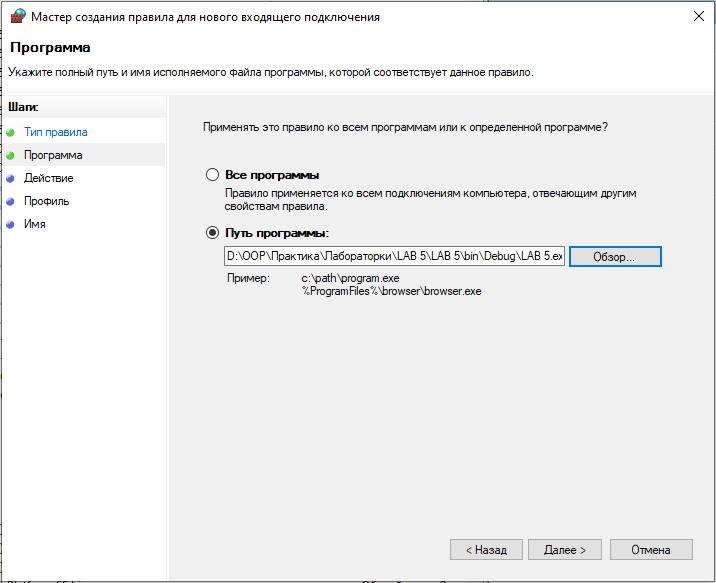


Рисунок 4.3 – Путь к программе

Далее выбираем блокировку подключения (рисунок 4.4).

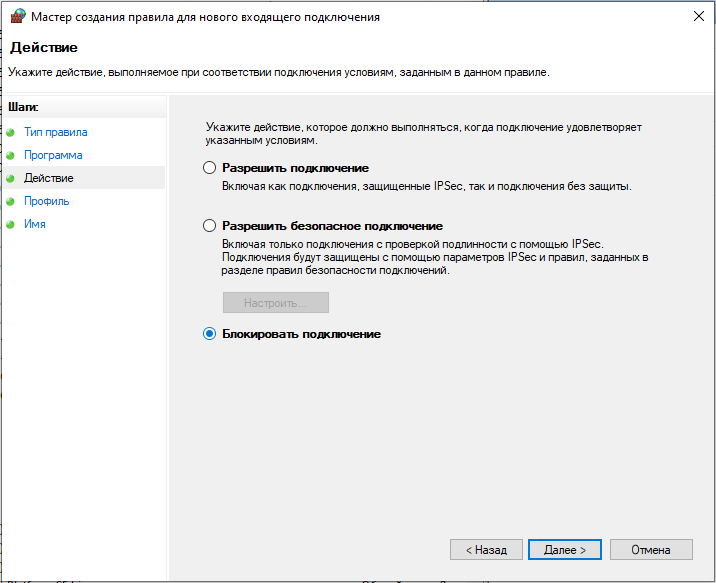


Рисунок 4.4 – Блокировка подключения

В Следующем окне указывается имя правила (рисунок 4.5).

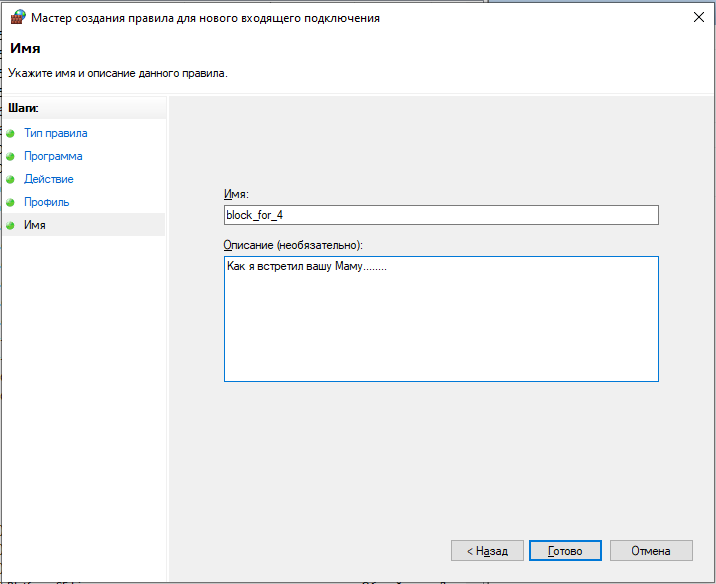


Рисунок 4.5 – Описание правила

Разрешить подключение (рисунок 4.6).

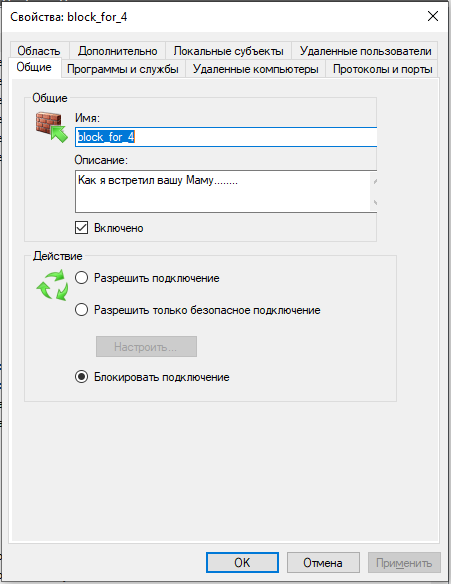


Рисунок 4.6 – Свойство правила

Встроенный брандмауэр Windows предоставляет возможность создавать мощные правила. Вы можете блокировать программам доступ к сети Интернет, ограничивать трафик на определенные порты и IP-адреса, а также многое другое, не устанавливая файрволл от стороннего производителя.

Тем же способом создаются и правила для исходящих подключений.

Открываем «Мастер создания правила для исходящего подключения» (рисунок 4.7).

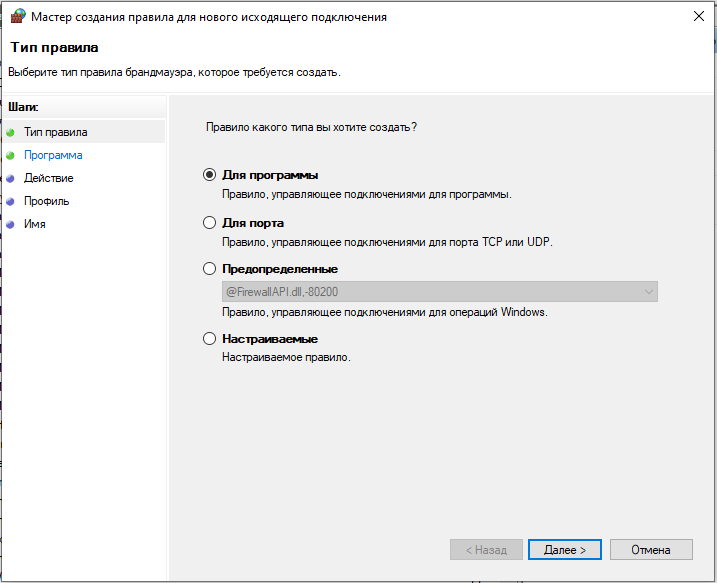


Рисунок 4.7 – выбор типа правила

Указываем путь к программе (рисунок 4.8).

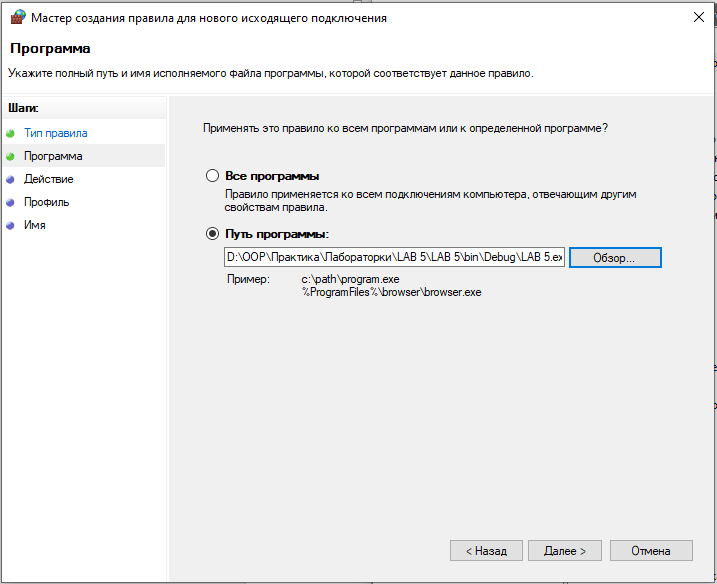


Рисунок 4.8 – Путь к программе

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

Далее выбираем блокировку подключения (рисунок 4.9).

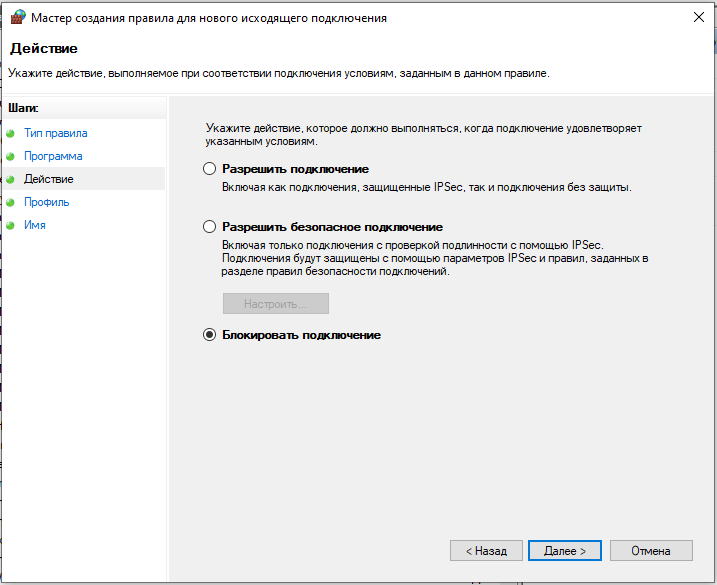


Рисунок 4.9 – Блокировка подключения

Потом выбираем окно свойств (рисунок 4.10).

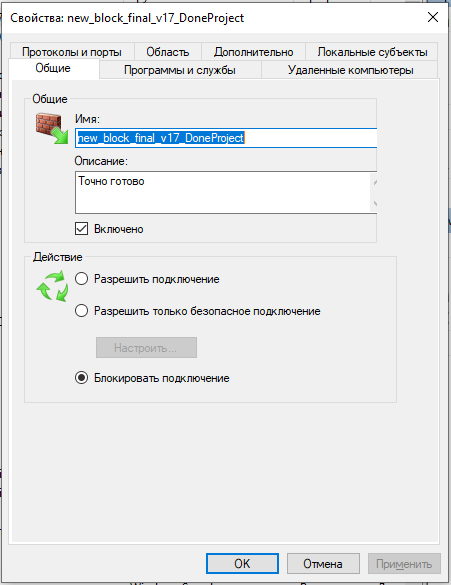


Рисунок 4.10 – Свойство правила

Аналогичные действия производим над вторым приложением. Демонстрация создания правил (рисунок 4.11).

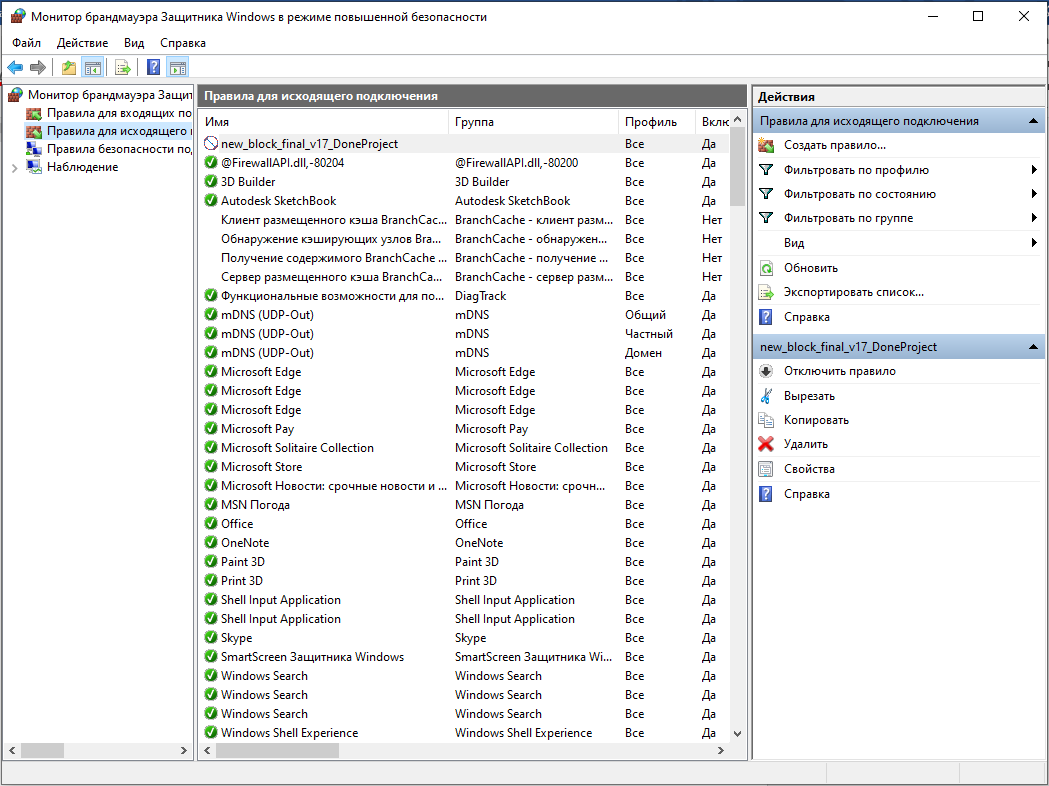


Рисунок 4.11 – Окно ввода имени

Для выполнения команд используем командную строку (рисунок 4.12).

Командная строка – специальная программа, позволяющая управлять операционной системой при помощи текстовых команд, вводимых в окне приложения. Её интерфейс полностью текстовый, в отличие от привычного вида операционной системы.

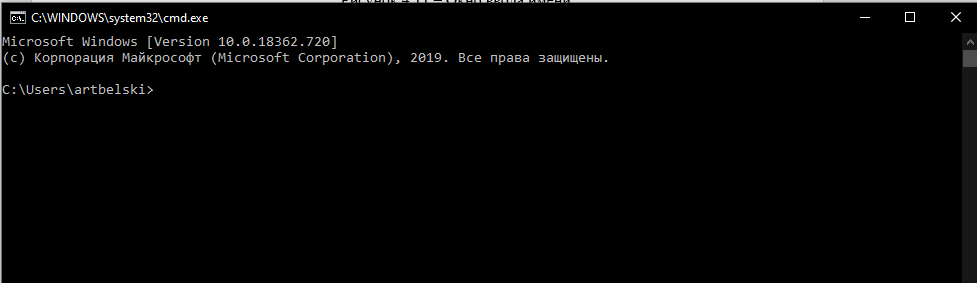


Рисунок 4.12 – Командная строка

Диспетчер проверки драйверов - verifier (рисунок 4.13).

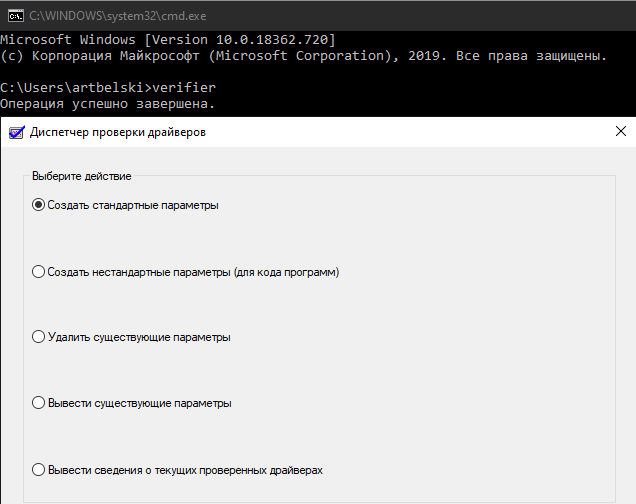


Рисунок 4.13 – Вызов диспетчера драйверов.

Редактор реестра (рисунок 4.14).

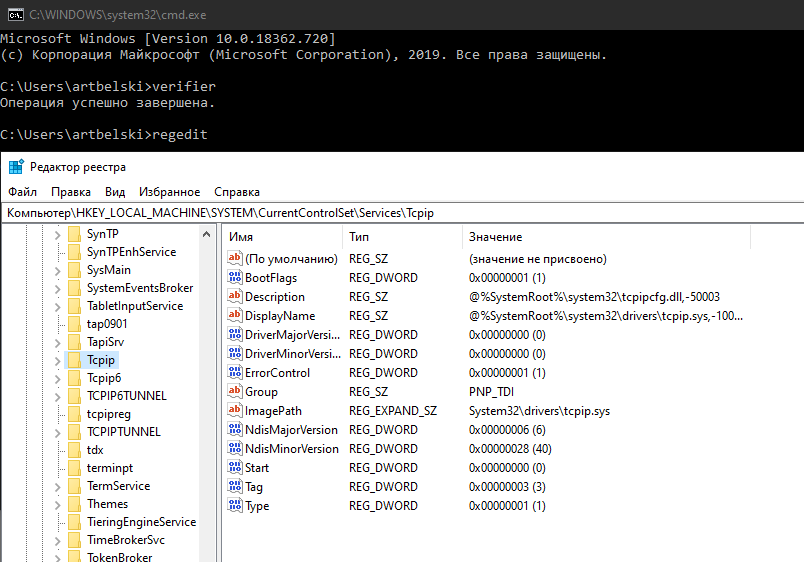


Рисунок 4.14 – Редактор реестра

**Вывод:** в результате выполнения работы ознакомился с брандмауэром Windows, с его возможностями добавлять правила для входящих и исходящих подключений. Также ознакомился с командами администратора.

**Практическое занятие №5**

**Тема «Настройка антивирусов»**

**Цель работы:** овладение навыками настройки и использования различных антивирусов.

Настроить режим фильтрации файрволла антивируса (один из описанных в теоретическом введении).

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

Существуют и другие режимы:

* автоматический;
* интерактивный;
* режим на основе политик;
* автоматический с исключениями;
* обучения.

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

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

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

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

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

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

Главное меню Касперского (рисунок 5.1).

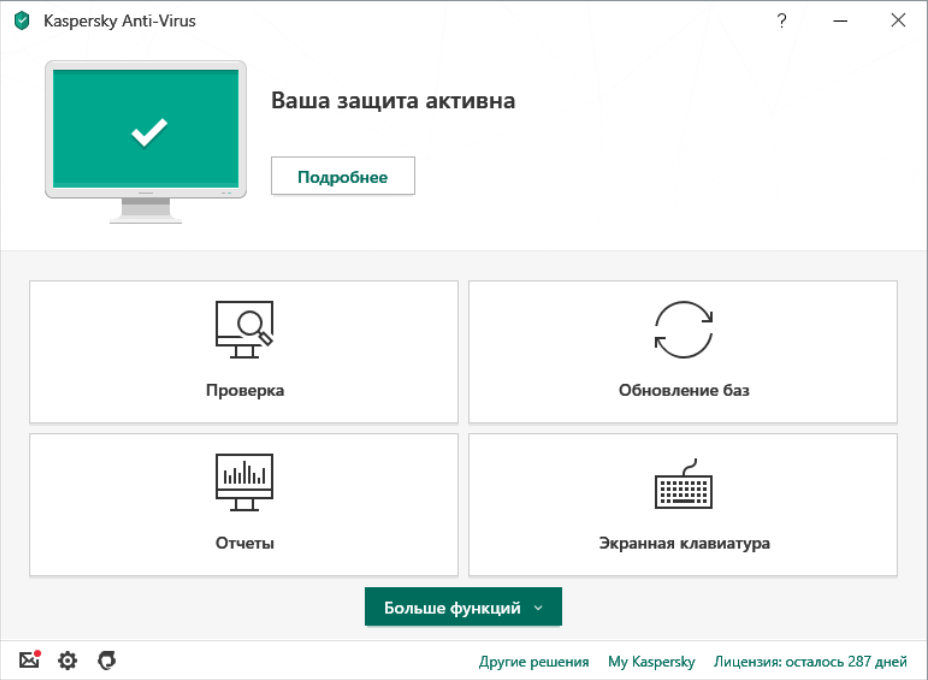


Рисунок 5.1 – Главное меню Касперского

Настройка сервера обновлений в антивирусе KASPERSKY производится по нажатию кнопки обновить, после открытия меню «Обновление баз» (рисунок 5.2).

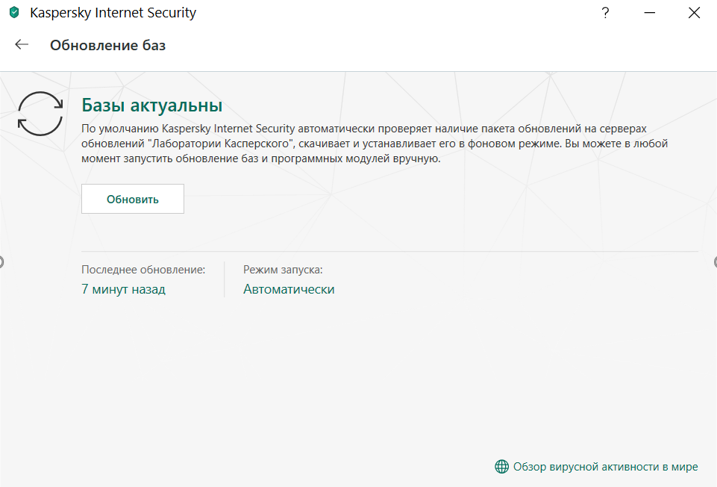


Рисунок 5.2 – Панель обновления

Чтобы заблокировать конкретной программе доступ к интернету требуется создать правило для программы в Сетевом экране (рисунок 5.3), для этого выполняются следующие действия:

* открыть Kaspersky Internet Security;
* в правом нижнем углу нажать на ссылку «Настройка»;
* выбрать сетевой экран.

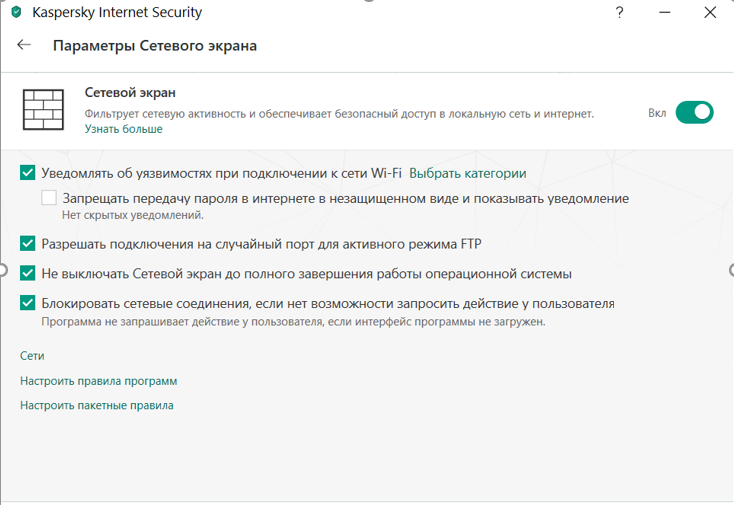


Рисунок 5.3 – Сетевой экран

В окне Параметры Сетевого экрана нажать на ссылку «Настроить правила программ», затем нажать на зелёную галочку и «Запретить» программе доступ в сеть (рисунок 5.4).

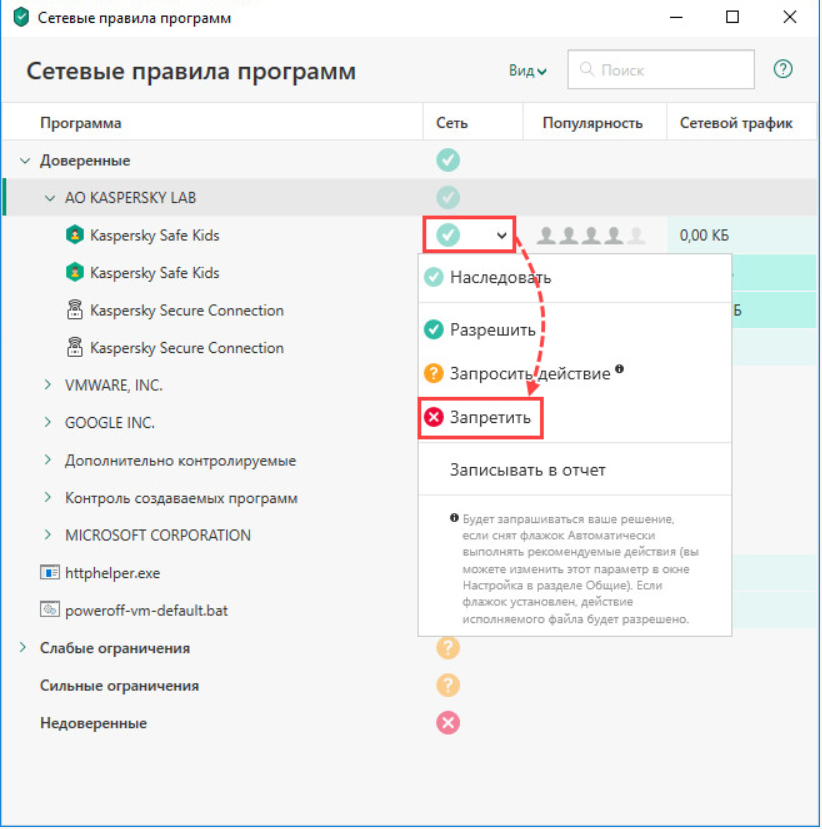


Рисунок 5.4 – Сетевые правила программ

Для добавления «Офлайн обновления сигнатур угроз» из локальной папки и «Офлайн обновление сигнатур угроз из локального сервера» требуется открыть пункт меню обновления (рисунок 5.1), далее перейти во вкладку режим запуска и затем выбрать пункт «Настроить источники обновлений» (рисунок 5.5), а в нем нажать кнопку добавить (рисунок 5.6) и прописать путь к требуемому файлу.

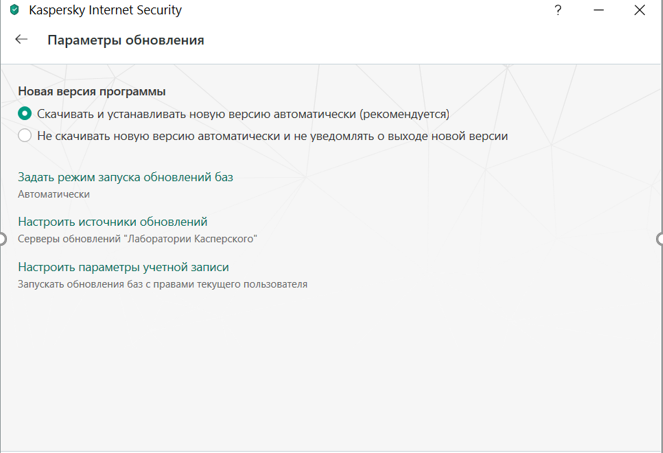


Рисунок 5.5 – Параметры обновления

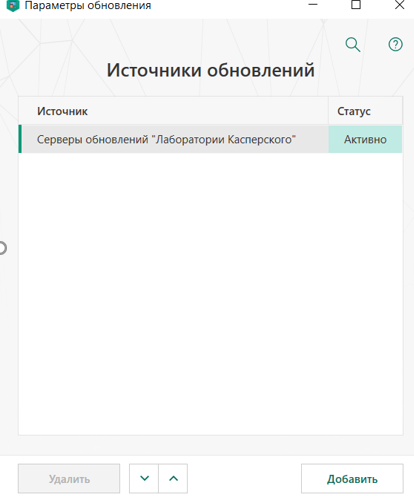


Рисунок 5.6 – Источники обновления

**Вывод:** антивирус способен в большинстве случаев удалить вредоносный программный объект не только из программного файла, но и из файла офисного документа, не нарушив его целостность. В некоторых случаях антивирус может удалить тело вредоносного объекта из зараженного файла, восстановив файл. Использование антивирусных программ не требует высокой квалификации и доступно практически любому пользователю компьютер.

**Практическое занятие №6**

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

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

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

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

Выполнение работы будет выполнено поэтапно.

Этап 1: установить и запустить программу.

Этап 2: открыть окно TrueCrypt (рисунок 6).

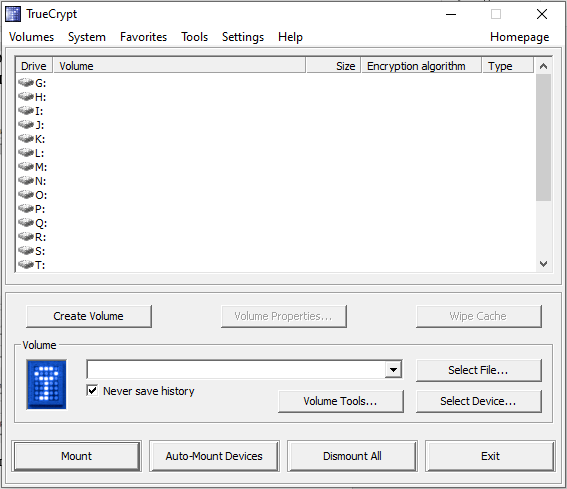


Рисунок 6 – Окно программы TrueCrypt

Далее нажать на кнопку «Create Volume» (рисунок 6.1).



Рисунок 6.1 – Мастер создания томов

На экране появится окно для создания TrueCrypt раздела. На этом этапе нужно выбрать место для создания раздела. Он может находится непосредственно в файле, пользователи называют его контейнером, в разделе диска либо внутри дискового устройства. Приступим к созданию раздела TrueCrypt в файле. Данное изображение имеет установку по умолчанию, поэтому жмём «Next» (рисунок 6.2).

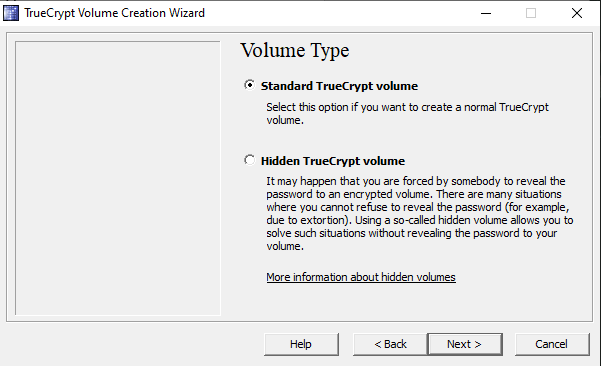


Рисунок 6.2 – Тип тома

Далее (рисунок 6.2) необходимо определится какой раздел вы создадите: скрытый или обычный. Руководство покажет создания обычного раздела. Опция уже выставлена. Поэтому нажимаем «Next».

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

Далее выбирает Select File. Открывается окошко для выбора файла (рисунок 6.3).

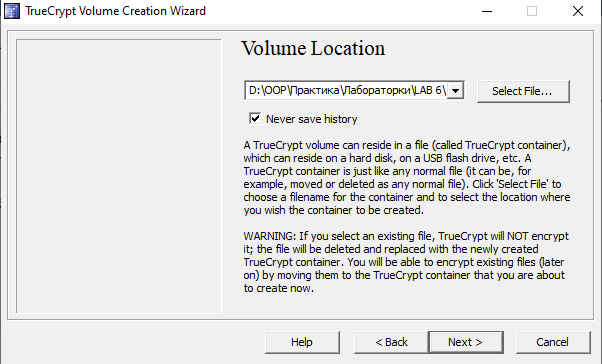


Рисунок 6.3 – Размещение тома

После выбора места жмем «Далее».

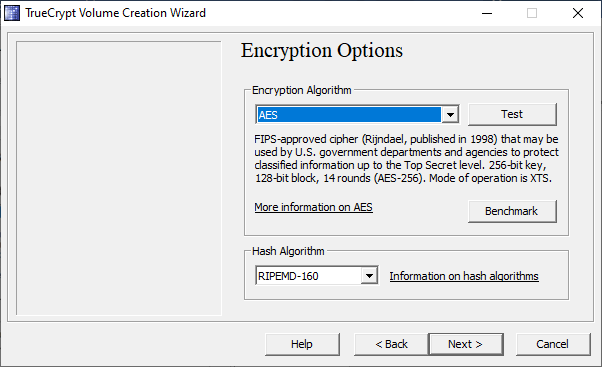


Рисунок 6.4 – Настройка шифрования

В данном разделе (рисунок 6.4) вам предлагается сделать выбор алгоритма для шифрования, а также хеш – алгоритма, предназначенного для раздела. Если вы не в состоянии что-то выбрать, оставляем всё как есть и жмем «Next».

Далее в окне (рисунок 6.5) мы указываем предполагаемый размер контейнера TrueCrypt в 1 мегабайт. Можно выбрать и другой размер, а затем нажимаем «Next».

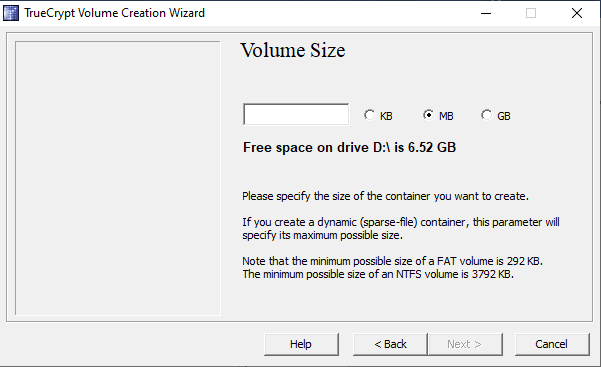


Рисунок 6.5 –Размер тома

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

После того как вы определитесь введите пароль в первое поле, а затем продублируйте его во второе и нажмите «Next». (Рисунок 6.6).



Рисунок 6.6 – Пароль тома

Чем дольше будет продолжаться процесс в открывшемся окне – тем лучше. Это повлияет на увеличение криптографических свойств ключей. Жмем Format и затем начинается процесс создания раздела. На диске D в указанной папке появится файл. Он будет выступать контейнером, в котором будет находится шифрованный раздел TrueCrypt. По окончанию вы увидите окно, показанное ниже.

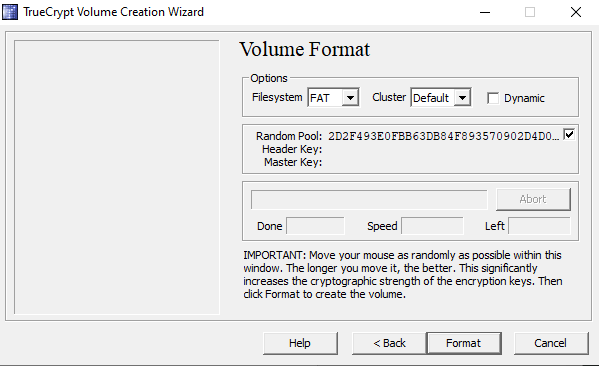


Рисунок 6.7 – Формирование тома

Жмем «ОК» для **его закрепления (рисунок 6.8).**

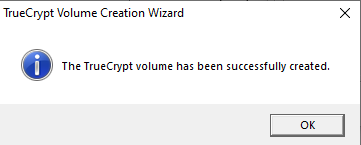
****

Рисунок 6.8 – Кнопка подтверждения

Вы создали раздел TrueCrypt. В окошке TrueCrypt Volume Creation Wizard жмем «Exit». (Рисунок 6.9). После этого окно пропадает. Возвращаемся к главному окну программы TrueCrypt, если оно исчезло повторяем 1 этап и приступаем к монтировке.

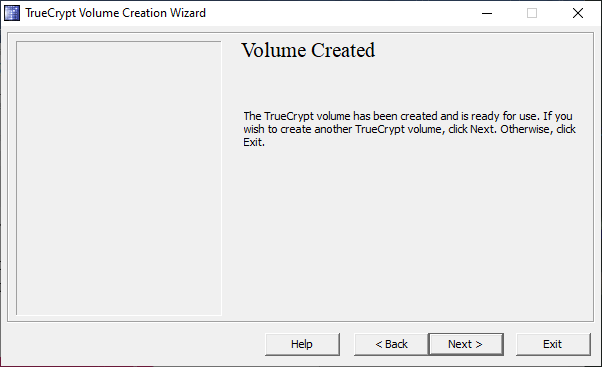


Рисунок 6.9 – Созданный том

Выбираем одну из букв, представленных в списке, это будет буква диска, к которому вы переименуйте ваш контейнер (рисунок 6.10).

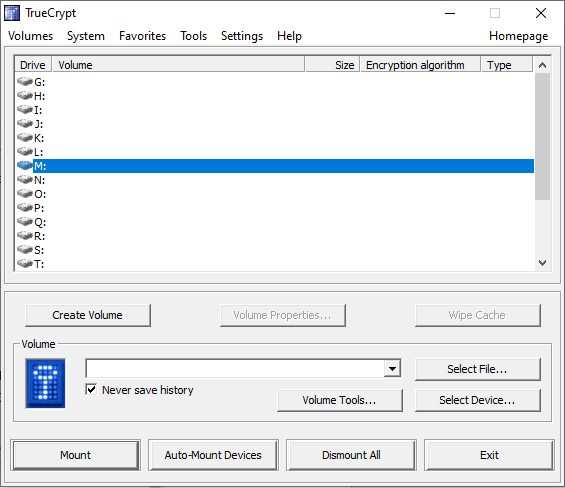


Рисунок 6.10 – Выбор буквы тома

Жмем Select File. При этом должна открыться стандартная версия окна, в которой необходимо выбрать файл (рисунок 6.10).

В данном окне находим файл, который вы создали с 6 по 11 этап и выбираем его. Жмем «Open», после этого окно должно исчезнуть (рисунок 6.11).

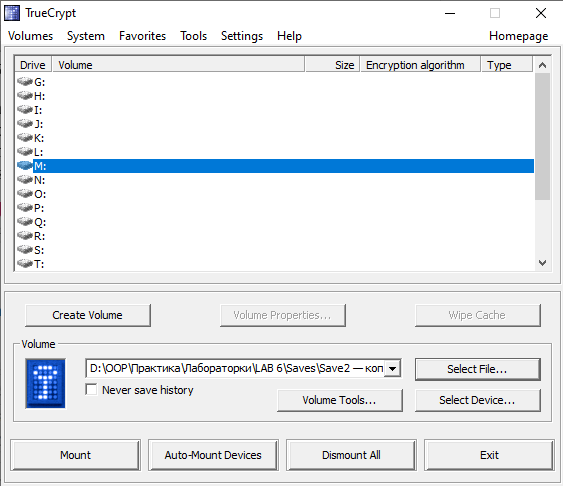


Рисунок 6.11 – Выбор файла

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

Вводим пароль, который вы установили на 10 этапе в поле, выделенное красным. Жмем «ОК».

Далее TrueCrypt приступает к монтировке раздела. В случае неправильного введения пароля TrueCrypt запросит повторный ввод, если пароль введен верно монтировка раздела пройдет успешно (рисунок 6.12)

Финальный этап:

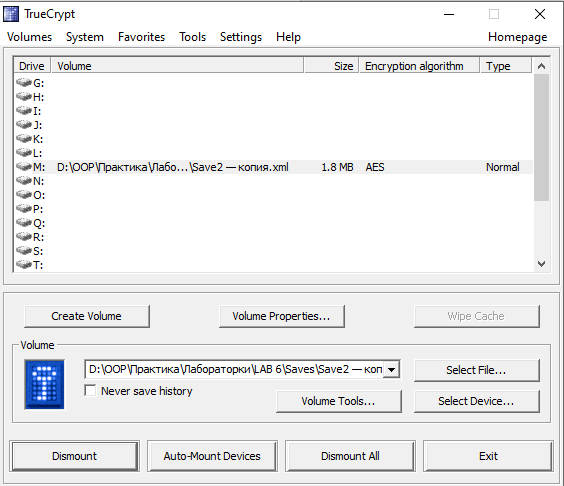


Рисунок 6.12 – Завершение операции

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

Если вы решите открыть файл, который размещен в TrueCrypt, то расшифровка будет производится автоматически через ОЗУ во время воспроизведения.

Важно: обратите внимание, что при каждом открытие документа у вас будут требовать пароль.

Открыть уже смонтированный раздел можно два раза нажав на него мышкой как указанно на картинке ниже. Открыть его так же можно, как и все прочие диски, через вкладку «Мой компьютер» (рисунок 6.13).

Вы имеете возможность осуществить копирование как с раздела TrueCrypt, так и на него. Все файлы автоматически расшифровываются или наоборот – зашифровываются.

Обратите внимание, что ни одна расшифрованная информация не подлежит сохранению, а лишь временно сохраняется в ОЗУ. Даже во время открытия файла данные по-прежнему зашифрованные. Во время выключения или перезагрузки вашего компьютера, даже несанкционированного, раздел размонтируется и в доступе к файлам будет отказано. Для возобновления доступа необходимо произвести примонтировку описанную с 13 по 18 этап.

Для закрытия раздела и отказа в доступе к данным вам следует выполнить следующие действия:

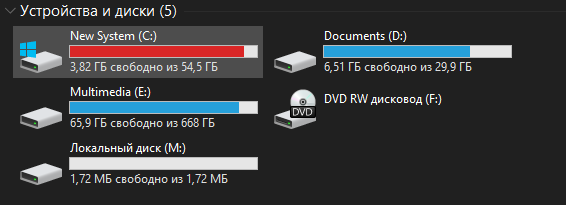


Рисунок 6.13 – Отображение созданного раздела

Из списка разделов, представленных в главном окне, необходимо выбрать один раздел и нажать «Dismount».  Для открытия доступа к разделам необходимо повторить с 13 по 18 этап.

**Вывод:** в результате выполнения работы ознакомился 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.

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.

Классификация алгоритмов шифрования:

* Симметричные (с секретным, единым ключом, одно ключевые, single key).
* потоковые:
* с одноразовым или бесконечным ключом (infinite-key cipher);
* с конечным ключом;
* на основе генератора псевдослучайных чисел;
* блочные;
* шифры перестановки (permutation, P-блоки).

Шифры замены (substitution, S-блоки):

* моно алфавитные;
* полиалфавитные.

Асимметричные (с открытым ключом, public-key):

* Диффи-Хеллман DH (Diffie, Hellman);
* Райвест-Шамир-Адлeман RSA (Rivest, Shamir, Adleman);
* Эль-Гамаль (ElGamal).

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). Он 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 (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.

Это можно показать следующей формулой: .

По получении А партнер P2 генерирует случайное число у и посылает P2 вычисленное значение: .

Партнер P1, получив В, вычисляет: .

Партнер P2 в свою очередь вычисляет: .

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.

Реализовать пример генерации секретного ключа с использованием метода Диффи-Хелмана:

В качестве p и g взять два любых простых числа.

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

открытое простое число ;

открытое простое число ;

секретный ключ 1: ;

открытый ключ 1: ;

секретный ключ 2: ;

открытый ключ 2: ;

секретный ключ:;

секретный ключ: ;

;

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

Шифр Цезаря один из наиболее древнейших известных шифров. Схема шифрования очень проста – используется сдвиг буквы алфавита (рисунок 7.1) на фиксированное число позиций.



Рисунок 7.1 – Алфавит

Ключ 2: «чрщхйвщзфвдфровфро».

**Вывод**: в результате выполнения работы овладел основными криптографическими алгоритмами шифрования.

**Практическое занятие №8**

**Тема «Криптографическая защита информации»**

**Цель работы:** получение основных сведений из курса теории чисел

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

* ассоциативность: ;
* коммутативность: ;
* существует нейтральный элемент – 0 и 1 соответственно:

, ;

* закон дистрибутивности: ;
* для каждого целого существует единственное противоположное, то есть такое целое , что .

Теорема 1 (О делении с остатком). Для любых целых чисел a и b, , существует единственные целые числа q и , такие, что .

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

Следствие*.* Пусть – натуральное число, . Для всякого целого числа *a* и максимального целого с условием существуют единственные целые такие, что .

Такое равенство записывают сокращённо или (если *b* известно по контексту) и называют записью числа *a* в *b* – ичной позиционной системе счисления или системе счисления по основанию *b*. Нам кажется естественной привычная десятичная позиционная система записи целых чисел . В различных ситуациях более удобными оказываются другие основания. К примеру, во всех компьютерах на микроуровне вычисления проводятся в двоичной системе счисления. Для перехода к ней с десятичной применяют промежуточную – 16-ричную систему счисления.

Лемма 1*.* Если в равенстве все слагаемые – целые числа и все, кроме может быть одного, делятся на целое , то и это исключенное слагаемое делится на .

Определение 1***.***Если целые числа делятся на целое , то *d* называют их общимделителем.

В дальнейшем речь идет только о положительных целых делителях.

Определение 2. Максимальный из общих делителей целых чисел называется их наибольшим общим делителем и обозначается через НОД ().

Теорема 2. Если , то НОД (a, b) = НОД (b, c).

Теорема 3 позволила Евклиду (примерно 2300 лет тому назад) обосновать следующий факт.

Теорема 3*.* Наибольший общий делитель целых чисел *a* и *b*  равен последнему отличному от нуля остатку цепочки равенств:

*;*

*;*

*…………………*

то есть = НОД .

Теорема 3 формулирует алгоритм Евклида нахождения наибольшего общего делителя целых чисел. Его вариантом является следующий – второй способ вычисления наибольшего общего делителя по алгоритму Евклида – вычисляем последовательно разности до получения последней ненулевой разности, которая и совпадает с НОД (a, b).

Теорема 4. Если d = НОД (a, b), то существуют такие целые u и v, что выполняется следующее соотношение (Безу): d = au+ bv.

Определение 3. Натуральное число называется простым, если оно делится только на 1 и на себя.

Теорема 5*.* Всякое натуральное числолибо является простым числом, либо имеет простой делитель

Заметим, что из соотношения натуральных чисел, больших единицы, следует, что, либо *p,* либо *q* принадлежит отрезку . Легко видеть, что наименьший натуральный делитель натурального числа является простым числом. Исторически первый метод проверки натурального числа на простоту заключается в делении его на простые числа, не превосходящие , носит название «решета Эратосфена». К настоящему времени разработан достаточно большой цикл алгоритмов проверки числа на простоту.

Теорема 6(Евклид)*.* Простых чисел бесконечно много.

Значение простых чисел в том, что они по теореме 2.5 являются составными кирпичиками всех натуральных чисел.

Определение 4. Целые числа *a* и *b* называютсявзаимнопростыми*,* еслиНОД .

Теорема 7 (Критерий взаимной простоты целых чисел). Целые числа *a* и *b* взаимно просты тогда и только тогда, когда существуют такие целые u и v, что выполняется равенство .

Следствие. НОДтогда и только тогда, когдаНОД иНОД .

Важным в теории чисел и ее приложениях является следующее свойство взаимно простых целых чисел.

Лемма 2. Пусть произведение целых чисел *ab* делится на целое число *с* и НОД . Тогда *b* делится на *с*.

Теорема 8*(*Основная теорема арифметики*)*. Всякое целое число однозначно раскладывается в произведение простых множителей:

*.*

Если в этом равенстве собрать одинаковые множители, то получим каноническое разложение целого числа: .

Теорема 9. Пусть  *-* натуральное число*,* . Для любых целых чисел *a* и *b* следующие условия равносильны:

* *a* и *b* имеют одинаковые остатки от деления на
* *a – b* делится *на m,* тоесть *a – b = mq* для подходящего целого *q;*
* *a = b + mq* для некоторого целого *q.*

Определение 5. Целые числа, а и b называются сравнимыми по модулю m, если они удовлетворяют одному из условий теоремы 2.9. Этот факт обозначают формулой или и называют данную формулу сравнением.

Условие варианта 7: *а* = 7049964661, *b* = 168687989.

Задание 1.Найти канонические разложения чисел

;

Следовательно, числа *a* и *b* раскладываются следующим образом:

7049964661=79∙79∙79∙79∙181;

168687989=79∙79∙151∙179.

Задание 2.Найти НОД (a*,* b) пользуясь, а) алгоритмом Евклида, б) разложением чисел на простые множители.

Решение. Применим алгоритм Евклида.

Найдём НОД (*a, b*), воспользовавшись разложением на простые множители чисел *a* и *b*, полученным в решении предыдущего задания: 7049964661=79∙79∙79∙79∙181, 168687989=79∙79∙151∙179.

Следовательно, наибольшим общим делителем будет произведение одинаковых множителей, входящих, как в одно, так и в другое разложения чисел: НОД (a, b) = 79∙79 =

Найдём НОД (a, b) методом остатков от делений:

7049964661 % 168687989 = 133757112;

168687989 % 133757112 = 34930877;

133757112 % 34930877 = 28964481;

34930877 % 28964481 = 5966396;

28964481 % 5966396 = 5098897;

5966396 % 5098897 = 867499;

5098897 % 867499 = 761402;

867499 % 761402 = 106097;

761402 % 106097 = 18723;

106097 % 18723 = 12482;

18723 % 12482 = 6241;

12482 % 6241 = 0.

Следовательно, НОД (a; b) = 6241.

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

Реализуем расширенный алгоритм Евклида в функции языка С#.

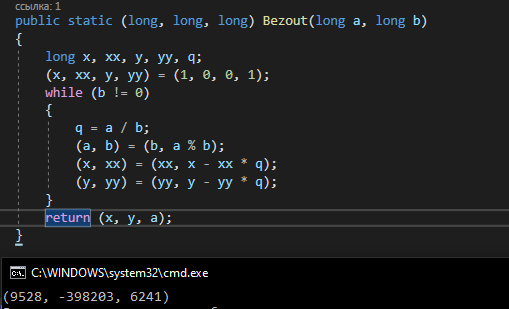


Рисунок 8.1 – Листинг алгоритма Евклида для вычисления коэффициентов Безу

;

.

Задание4. Найти остаток от деления на 17.

Вычислим остаток от деления на 17 среди первых 20 степеней числа 1997.

1. ;
2. ;
3. ;
4. ;
5. ;
6. ;
7. ;
8. ;
9. ;
10. ;
11. ;
12. ;
13. ;
14. ;
15. ;
16. ;
17. ;
18. ;
19. ;
20. .

Замечаем, что числа повторяются с циклом 8. Так как , то

**Вывод**: в результате выполнения работы получил основные сведения из курса теории чисел.

### **Практическое занятие №9**

**Тема Криптографическая защита информации**

**Цель работы:** овладение навыками работы с известными криптографическими алгоритмами.

Несмотря на достаточно большое число различных систем с открытыми ключами, одной из наиболее популярных остается криптосистема RSA. Авторы воспользовались тем фактом, что нахождение больших простых чисел в вычислительном отношении осуществляется легко, а разложение на множители произведения двух таких чисел – сложно.

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:;

Что означает, что их разность 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 следующее соотношение: ;

Если a и b имеют одинаковые остатки при делении на m.

Приведем некоторые очевидные свойства сравнений через следующую формулу: ;

Тогда, исходя из формулы  и : ;

Легко также проверить, что операция сравнения по модулю m является эквивалентностью (выполняются свойства рефлективности, 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 .

Для любого х, простого относительно p, и  для любого х.

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

Теорема 2. Если n будет равна произведению p и q, и они отличные друг от друга простые числа, то.

Теорема 3. Если n будет равна произведению p и q, и они отличные друг от друга простые числа, и х – простое относительно p и q, то .

Следствия:

Если n будет равна произведению p и q, и они отличные друг от друга простые числа, е – простое число относительно Ф(n), то отображение является взаимно однозначным на алгебраическом кольце вычетов Z(n).

Если е – простое число относительно Ф(n), то существует целое число d, такое, что .

Пусть n будет равна произведению p и q, и они отличные друг от друга 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 .

Итак, в реальных системах RSA реализуется следующим образом:

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

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

Номер варианта: 3. Сообщение: CDA. P:11. Q:101.

Найдём произведение P и Q.

Найдём значение функции Эйлера для n:

Выбираем произвольное целое e: взаимно простое с значением функции Эйлера . То есть . Пара чисел объявляется открытым ключом шифра. То есть .

Вычисляем целое число d (обратное число по модулю от е) из соотношения:.

Придаём k последовательно значения 1, 2, 3, … до тех пор, пока не будет получено целое число d. Это можно вычислить по следующей формуле:

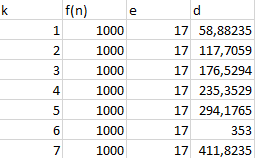


Рисунок 9.1 – Подбор значения k

Пара чисел будет закрытым ключом шифра. В нашем примере

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

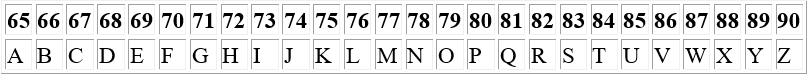


Рисунок 9.2 – Числовые эквиваленты латинских букв

;

;

;

.

Расшифровка осуществляется по формуле:

;

;

;

;

**Вывод:** в результате выполнения работы я ознакомился с криптографическим алгоритмом RSA.

### **Практическое занятие №10**

**Авторское право и смежные права**

**Цель работы:** изучить основные положения авторского права и смежных прав.

Объекты, на которые распространяется авторское право.

Объекты авторского права и смежных прав (литературные, художественные, научные произведения, компьютерные программы, базы данных, музыкальные произведения, исполнительская деятельность артистов, аудио- и видеозаписи, радио- и телевизионные передачи и др.). Авторское право распространяется как на обнародованные, так и на необнародованные произведения, существующие в какой-либо объективной форме.

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, 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.

Производные произведении:

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

Компьютерные программы (все виды программ):

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

Авторские права распространяются на:

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

Авторское право на произведение не связано с правом собственности на материальный объект, в котором произведение выражено.

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.

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.

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 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.

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

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

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

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

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

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.

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

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.

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

Авторский договор – это соглашение, в силу которого одна сторона (автор) передает или обязуется передать другой стороне (пользователю) свои права на использование произведения, а пользователь обязуется уплатить автору установленное вознаграждение за использование или предоставление такого права.

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. Издательский договор наиболее полно урегулирован действующим законодательством и исследован юридической наукой. Нередко выводы, которые первоначально делаются на базе применения норм об издательском договоре, а также сложившейся практики разрешения споров, впоследствии распространяются и на другие авторские договоры.

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. Издательский договор наиболее полно урегулирован действующим законодательством и исследован юридической наукой. Нередко выводы, которые первоначально делаются на базе применения норм об издательском договоре, а также сложившейся практики разрешения споров, впоследствии распространяются и на другие авторские договоры.

Постановочный договор заключается тогда, когда основным способом использования произведения является его публичное исполнение. Его предметом могут быть драматические произведения, музыка или либретто оперы, балета, оперетты, музыка к драматическому спектаклю и т.п., которые используются театрально-зрелищными организациями (театрами, филармониями, цирками, концертными организациями и т.д.) путем постановки на сцене. В настоящее время постановочный договор должен заключаться пользователями в отношении как необнародованных, так и обнародованных произведений.

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. Их основное различие заключается в том, что литературный сценарий в отличие, например, от драматического произведения используется не в своем неизменном виде, а служит основой для создания более приближенного к нуждам кинематографа, телевидения или радио режиссерского сценария, по которому, собственно, и ставится фильм или делается передача. В этом смысле 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. Обычно путем депонирования используются научные произведения, представляющие интерес лишь для ограниченного круга специалистов, но запросам которых им предоставляются копии депонированных произведений или их отдельных частей.

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. Он заключается лишь с внештатными художниками предприятий, произведения которых принимаются к использованию. Авторы получают вознаграждение как за сам факт создания произведения, принятого к использованию, так и за последующее тиражирование в зависимости от объема использования.

Содержание авторского договора:

* авторский договор на передачу исключительных прав, разрешающий использование произведения определенным способом и в установленных пределах только лицу, которому эти права передаются;
* авторский договор на передачу неисключительных прав, разрешающий использование произведения и другим лицам, в том числе самому обладателю исключительных прав, заключившему авторский договор.

Авторский договор заключается в письменной форме и, по желанию сторон, может быть заверен нотариально. Договор может быть изменен, прекращен или расторгнут также только письменно. В каждом отдельном случае издатель и автор выбирают и согласуют оригинальный текст авторского договора. Следует отметить, что авторский договор не обязательно представляет собой единый документ. Он может включать и различного рода дополнительные соглашения. Авторское право предусматривает возможность заключения еще одного вида договора - авторского договора заказа. По договору заказа автор обязуется создать произведение в соответствии с условиями договора и передать его заказчику. Особенность авторского договора заказа состоит в том, что заказчик обязан в счет обусловленного договором вознаграждения выплатить автору аванс. Размер, порядок и сроки выплаты аванса устанавливаются в договоре по соглашению сторон.

В соответствии с законом, авторский договор должен предусматривать следующие обязательные положения:

* способы использования произведения (конкретные права, передаваемые по данному договору);
* срок и территорию, на которые передается право;
* размер вознаграждения и (или) порядок определения размера вознаграждения за каждый способ использования произведения, порядок и сроки его выплаты.

**Вывод**: в результате лабораторной работы я ознакомился с основными положениями авторского права и смежных прав.

### **Практическое занятие №11**

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

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

На данном практическом занятии рассматриваются следующие вопросы:

* Основные составляющие описания изобретения?
* Правила оформления описания изобретения?
* Какие основные пункты должна содержать заявка на изобретение?
* Основные документы, необходимые для подачи заявки на изобретения?
* Отличия заявок на охранные документы различных объектов промышленной собственности?
* На какие ОПС выдаются патенты?
* На какие ОПС выдаются свидетельства?

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

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.

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.

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.

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.

Заявка на изобретение подается в трех экземплярах и должна содержать:

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

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

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.

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.
* доверенность, при подаче заявки через патентного поверенного;
* заверенная копия первой заявки, в случае подачи заявки в соответствии с Парижской конвенцией по охране промышленной собственности (конвенционная заявка).

При экспертизе заявки на полезную модель проверка соответствия заявленной полезной модели условиям патентоспособности не осуществляется.

До даты получения заявителем решения о выдаче патента на полезную модель, а в случае принятия решения об отказе в выдаче патента - до момента истечения срока его обжалования, возможно преобразование заявки на полезную модель в заявку на изобретение.

Охранный документ (патент, свидетельство) – это выдаваемый патентным органом от имени государства документ, который удостоверяет авторство, приоритет на объект промышленной собственности и исключительное право на его использование. Приоритет - первенство, чаше всего, определяемое датой подачи заявки на ОПС. Конвенционный приоритет обозначает, что заявка, поданная в одной стране-участнице конвенции, обладает во всех других странах приоритетом в течение года, исчисляемого с момента подачи заявки в первой стране. Одной из наиболее распространенных коммерчески значимых форм правовой охраны является патент, который обеспечивает патентообладателю исключительное (монопольное) право на использование объекта промышленной собственности и запрещает всем третьим лицам их использование в коммерческих целях без разрешения патентообладателя. Являясь одновременно правовым, техническим и информационным документом, патент выступает не только в качестве формы правовой охраны от несанкционированного использования, но и своеобразным экономическим стимулом для инвестиций в научные исследования и промышленность.

ОПС патенты выдаются на: устройства, изделия, способы, вещества, биотехнические продукты, применение устройства, способа, вещества, биотехнического продукта по определенному положению:

* устройство (например, машина, прибор, инструмент, деталь и др.);
* способ (например, способ изготовления изделий, нанесения покрытий, способ лечения и др.);
* вещество (сплав, смесь, раствор, химическое соединение и др.);   
  биотехнологический продукт;
* применение устройства, способа, вещества, биотехнологического продукта по определенному назначению.

ОПС свидетельства выдаются на: открытия, научные теории, математические методы, изобретения, противоречащие принципам гуманности и морали.

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

**Вывод**: в результате выполнения работы ознакомился с правилами составления и оформления заявок на объекты промышленной собственности.

### **Практическое занятие №12**

**Тема «Патентные исследования»**

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

**Задние для выполнения**

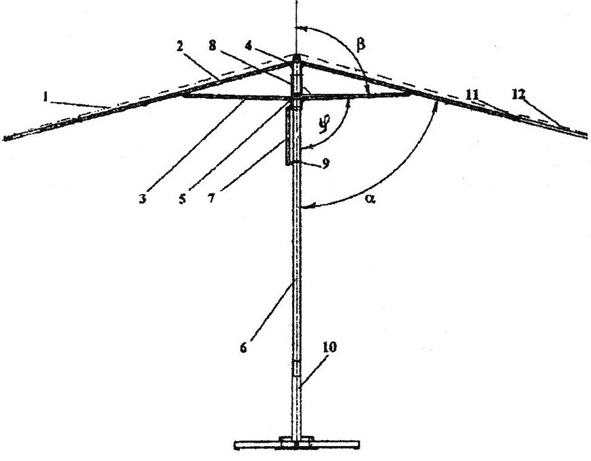


Рисунок 12.1 – Конструкция зонта складного

Полезная модель относится к наземным сооружениям, преимущественно к конструкции средних и больших складных зонтов с опорным стержнем и может быть использована предприятиями торговли и туризма для уличных кафе, мест отдыха для защиты от солнечных лучей и непогоды.

В основу полезной модели поставлена задача улучшения служебных качеств зонта путем повышения надежности работы самофиксации зонта в положении его раскрытия и улучшения комфортабельности его обслуживания за счет простого перевода зонта в режим раскрытие-закрытие без использования специальных механизмов.

Наиболее близкой по технической сущности к заявленной полезной модели является принятая в качестве прототипа конструкция складного зонта, содержащего тент с клапаном и каркас, состоящий из шарнирно связанных между собой распорных спиц и несущих радиальных спиц, с упругими элементами на концах и средством для крепления к ним тента, и посредством двух звездочек, связанных со стволом опорного стержня, на котором расположен механизм раскрытия и закрытия зонта.

**Таблица 12.1 – Источники информации**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Источник информации, по которым будет проводиться поиск** | | | | | | | | | | | |
| Предмет поиска (объект исследования, его составные части) | Страна поиска | Патентные | | НТИ | | Конъюнктурные | | Другие | | Ретроспективность | Наименование информационной базы (фонда) |
| Наименование | Классификационные  рубрики: МПК (МКИ)\*  МКПО\*\* МКТУ\*\*\* другие | Наименование | Рубрики УДК\*\*\*\* и другие | Наименование | Код товара ГС СМТК БТН | Наименование | Классификационные индексы |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| Зонт складной | Республика Беларусь | Зонт складной | МПК А45В 23/00  МКПО 03-03 | Складные зонты | УДК 685.555 | Зонты и солнцезащитные зонтики | 899.41 6601.10-.99 |  |  | 20 лет | База патентов Беларуси |

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

\*\* - МКПО - Международная классификация промышленных образцов

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

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

**Таблица 12.2 – Сведения о патенте**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 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) |
| 1 | 2 | 3 | 4 | 5 |
| Зонт складной | BY 1675 U A 45B 23/00 | Заявитель: Савицкий Анатолий Васильевич (BY)  Номер заявки: 20040107  Дата приоритета:  10.03.2004  Дата публикации:  30.12.2004 | Зонт складной | Действует |

Проведенный патентный поиск по указанному классу, выявил следующие аналогичные по конструктивному выполнению патенту и полезные модели, приведенные на рисунках 12.2-12.5:

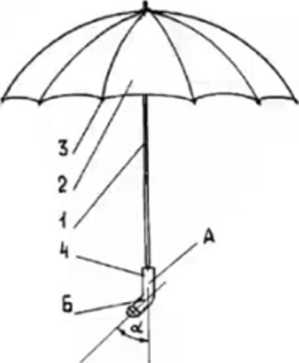


Рисунок 12.2 - Зонт

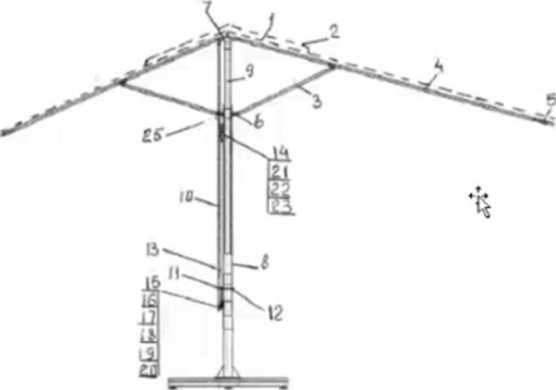


Рисунок 12.3 – Большой зонт



Рисунок 12.4 – Складной зонт

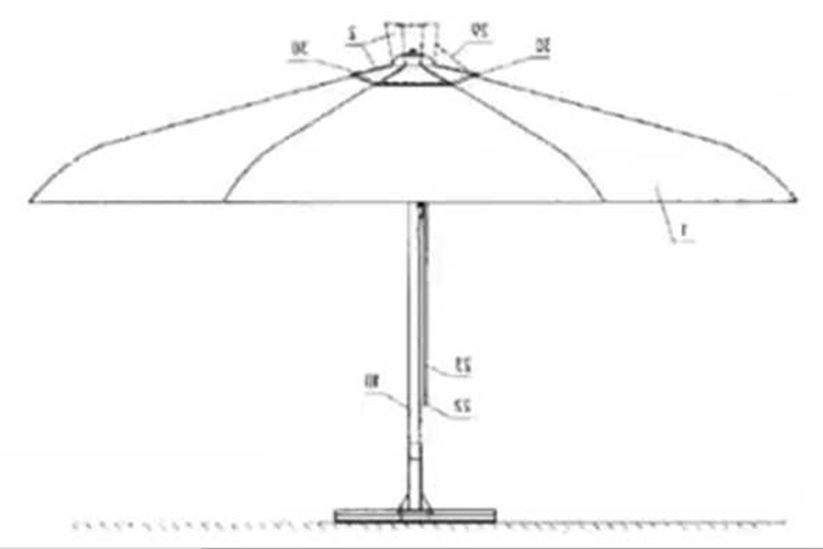


Рисунок 12.5 – Большой зонт

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

**Таблица 12.3 – Сведения о патентах-аналогах**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 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) |
| 1 | 2 | 3 | 4 | 5 |
| Зонт складной | U 3148 | Щепочкина Юлия  Алексеевна  Публикация: 30.12.2006 | Зонт | Действует |
| U 2959 | Савицкий Анатолий Васильевич  Подача заявки: 07.02.2006  Публикация: 30.08.2006 | Зонт большой | Действует |
| U 1675 | Савицкий Анатолий Васильевич  Подача заявки: 10.03.2004  Публикация: 30.12.2004 | Зонт складной | Действует |
| U 1259 | Савицкий Анатолий Васильевич  Подача заявки: 27.06.2003  Публикация: 30.03.2004 | Большой зонт | Действует |

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

### **Практическое занятие №13**

**«Патентный поиск»**

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

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

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

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

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

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

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

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

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

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

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

**Задание для выполнения: Модуль проверки данных банковских CRM систем**

Система управления взаимоотношениями с клиентами – [прикладное программное обеспечение](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%B8%D0%BA%D0%BB%D0%B0%D0%B4%D0%BD%D0%BE%D0%B5_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%BD%D0%BE%D0%B5_%D0%BE%D0%B1%D0%B5%D1%81%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%B8%D0%B5) для организаций, предназначенное для [автоматизации](https://ru.wikipedia.org/wiki/%D0%90%D0%B2%D1%82%D0%BE%D0%BC%D0%B0%D1%82%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F) стратегий взаимодействия с [заказчиками](https://ru.wikipedia.org/wiki/%D0%97%D0%B0%D0%BA%D0%B0%D0%B7%D1%87%D0%B8%D0%BA) ([клиентами](https://ru.wikipedia.org/wiki/%D0%97%D0%B0%D0%BA%D0%B0%D0%B7%D1%87%D0%B8%D0%BA)), в частности для повышения уровня продаж, оптимизации [маркетинга](https://ru.wikipedia.org/wiki/%D0%9C%D0%B0%D1%80%D0%BA%D0%B5%D1%82%D0%B8%D0%BD%D0%B3) и улучшения обслуживания клиентов путём сохранения информации о клиентах и истории взаимоотношений с ними, установления и улучшения [бизнес-процессов](https://ru.wikipedia.org/wiki/%D0%91%D0%B8%D0%B7%D0%BD%D0%B5%D1%81-%D0%BF%D1%80%D0%BE%D1%86%D0%B5%D1%81%D1%81) и последующего анализа результатов.

CRM — модель взаимодействия, основанная на теории, что центром всей философии бизнеса является клиент, а главными направлениями деятельности компании являются меры по обеспечению эффективного маркетинга, [продаж](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D1%8F%D0%BC%D1%8B%D0%B5_%D0%BF%D1%80%D0%BE%D0%B4%D0%B0%D0%B6%D0%B8) и обслуживания клиентов. Поддержка этих бизнес-целей включает сбор, хранение и анализ информации о потребителях, поставщиках, партнёрах, а также о внутренних процессах компании. Функции для поддержки этих бизнес-целей включают продажи, маркетинг, [поддержку](https://ru.wikipedia.org/wiki/%D0%A2%D0%B5%D1%85%D0%BD%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B0%D1%8F_%D0%BF%D0%BE%D0%B4%D0%B4%D0%B5%D1%80%D0%B6%D0%BA%D0%B0) потребителей.

|  |  |
| --- | --- |
| **Классы МПК:** | G06F 19/00, G06F 17/60, G07F 19/00 Система проведения безналичного расчета |
| **Автор(ы):** | Валерий Альбертович Жмышенко |
| **Патентообладатель(и):** | ООО «Зигота» |
| **Приоритеты:** | подача заявки: 2020-06-18  публикация патента: 10.04.2021 |

Система аутентификации пользователя банковского счета при дистанционном банковском обслуживании, включающая электронное коммуникационное устройство, например, смартфон или планшет, и сканер считывания персональных биометрических характеристик пользователя, отличающаяся тем, что используют сканер считывания отпечатка папиллярного рисунка пальца.

Система по п. 1, отличающаяся тем, что сканер считывания отпечатка папиллярного рисунка пальца выполнен в виде модуля электронного коммуникационного устройства. (Рисунок 13.1)

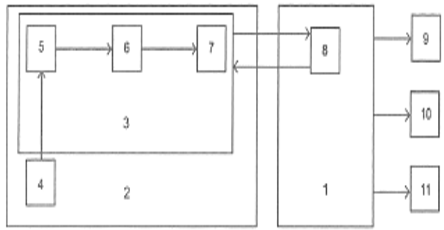


Рисунок 13.1 – Система аутентификации пользователя банковского счета при дистанционном банковском обслуживании

|  |  |
| --- | --- |
| **Классы МПК:** | G06F 19/00, G06F 17/60, G07F 19/00 Система проведения безналичного расчета |
| **Автор(ы):** | Виталий Цаль Альбертович |
| **Патентообладатель(и):** | Тюменцев Павел Дмитриевич |
| **Приоритеты:** | подача заявки: 20022-11-29  публикация патента: 30-06-20023 |

Система для проведения безналичного расчета, включающая взаимодействующие посредством сети связи, по меньшей мере, одно персональное мобильное средство связи покупателя, средство для генерирования запроса на обслуживание, центр идентификации первичного кода абонента мобильной сети связи, осуществляющий проверку аутентичности запроса, процессинговый центр банка и процессинговый центр продавца, осуществляющие обработку запроса, отличающаясятем, что дополнительно содержит имитатор личного кода покупателя и идентификатор личного кода покупателя, средство генерирования запроса на обслуживание выполнено в виде устройства ввода информации, связанного с персональным мобильным средством связи покупателя, персональное мобильное средство связи покупателя снабжено средством визуализации личного кода покупателя, а процессинговый центр продавца снабжен соответствующим средством считывания и идентификации личного кода покупателя и выполнен с возможностью обработки запроса на обслуживание покупателя по результатам идентификации первичного кода абонента мобильной сети связи и личного кода покупателя. Система по п. 1, отличающаясятем, что имитатор личного кода покупателя выполнен в виде имитатора штрих-кода, предпочтительно кода EAN-13. Система по любому из пп. 1, 2, отличающаясятем, что имитатор личного кода покупателя размещен в процессинговом центре банка.

Система по любому из пп. 1, 2, отличающаясятем, что имитатор личного кода покупателя размещен в персональном мобильном средстве связи покупателя.

Система по любому из пп. 1, 2, отличающаясятем, что имитатор личного кода покупателя размещен в процессинговом центре банка и в персональном мобильном средстве связи покупателя. Система по любому из пп. 1-5, отличающаясятем, что идентификатор личного кода покупателя размещен в процессинговом центре банка. Система по любому из пп. 1-6, отличающаясятем, что средство визуализации личного кода покупателя выполнено в виде дисплея персонального мобильного средства связи покупателя, выполненного с возможностью воспроизведения текстово-графической информации, предпочтительно штрих-кода.

Система по любому из пп. 1-7, отличающаясятем, что средство считывания и идентификации личного кода покупателя выполнено в виде сканера, выполненного с возможностью считывания и идентификации текстово-графической информации, предпочтительно штрих-кода.

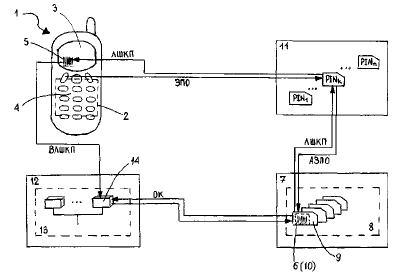


Рисунок 13.2 – Система проведения безналичного расчета

|  |  |
| --- | --- |
| **Классы МПК:** | G07D/00, G06F 17/60Способ проведения финансовых операций и система для его осуществления |
| **Автор(ы):** | [Лена Головач Леонидович](http://bypatents.com/patents/bursh-vladimir-leonidovich), [Колешко Владимир Михайлович](http://bypatents.com/patents/koleshko-vladimir-mihajjlovich), [Карякин Юрий Дмитриевич](http://bypatents.com/patents/karyakin-yurijj-dmitrievich) |
| **Патентообладатель(и):** | [Бурш Владимир Леонидович](http://bypatents.com/patents/bursh-vladimir-leonidovich), [Колешко Владимир Михайлович](http://bypatents.com/patents/koleshko-vladimir-mihajjlovich), [Карякин Юрий Дмитриевич](http://bypatents.com/patents/karyakin-yurijj-dmitrievich) |
| **Приоритеты:** | подача заявки: 1998-07-24  публикация патента: 30-12-2002 |

Способ проведения финансовых операций, заключающийся в вводе финансовой информации в компьютерную финансовую систему, обработке финансовой информации, ее индексировании, формировании базы данных, формировании транзакций и передаче их в компьютеры финансовых учреждений, отличающийсятем, что одновременно с вводом финансовой информации из нее выделяют часть информации, состав которой определен налоговым органом и преимущественно включает учетный номер налогоплательщика, даты начала и окончания действия сделки, суммы платежей или их эквиваленты, коды финансовых учреждений, номера расчетных счетов, эту часть информации кодируют и подают в компьютерную систему налогового органа, где ее регистрируют, а регистрационный номер используют при формировании транзакций, при этом осуществляют защиту зарегистрированной информации, которую используют налоговым органом для контроля подлинности финансовых документов, причем защиту зарегистрированной информации осуществляют путем формирования ее в виде документа на носителе, на поверхность которого наносят защитную машиночитаемую метку, при этом считывают тонкую структуру поверхности носителя, эту информацию обрабатывают, кодируют и совместно с кодированной информацией, состав которой определен налоговым органом, используют для формирования защитной машиночитаемой метки, причем для контроля подлинности финансового документа считывают защитную машиночитаемую метку с поверхности носителя, сравнивают полученную информацию с эталонным сигналом и по результату сравнения судят о подлинности финансового документа.

Способ по п. 1, отличающийсятем, что зарегистрированную кодированную информацию шифруют любым известным способом шифрования для передачи этой части информации субъектам хозяйствования.

Способ по п. 1 или 2, отличающийсятем, что при контроле подлинности финансовых документов первоначально считывают и обрабатывают информацию о структуре поверхности носителя, на основе чего формируют эталонный сигнал, с которым сравнивают только ту часть информации, заключенную в защитной машиночитаемой метке, которая относится к структуре поверхности носителя.

Система для проведения финансовых операций, включающая терминалы с устройствами ввода и отображения информации и передачи ее в компьютерную финансовую систему, которая содержит системы с устройствами приема информации от множества терминалов, связанные с первым входом процессорного устройства для обработки информации, второй вход-выход которого соединен с запоминающим устройством для хранения информации и программ ее обработки, устройством отображения информации и средством связи с компьютерами финансовых учреждений, отличающаяся тем, что компьютерная финансовая система дополнительно включает устройство считывания тонкой структуры поверхности документа на носителе, выход которого подключен к третьему входу процессорного устройства, и принтер высокого разрешения, выход которого соединен с четвертым входом процессорного устройства, при этом компьютерная финансовая система оснащена комплектом программ для считывания тонкой структуры поверхности носителя, обработки считанной информации и формирования защитной машиночитаемой метки, содержащей информацию о тонкой структуре поверхности носителя и кодированную информацию, состав которой определен налоговым органом и преимущественно включает учетный номер налогоплательщика, даты начала и окончания действия сделки, суммы платежей или их эквиваленты, коды финансовых учреждений, номера расчетных счетов, при этом к пятому входу процессорного устройства через дополнительное оборудование связи подключена компьютерная система налогового органа.

Система по п. 4, отличающаясятем, что включает средства хранения зарегистрированной защищенной информации, связанные с компьютерной финансовой системой и компьютерной системой налогового органа.

Система по п. 4 или 5, отличающаясятем, что она оснащена программными и/или аппаратными средствами шифрования, которые одновременно подключены к компьютерной финансовой системе и компьютерной системе налогового органа.

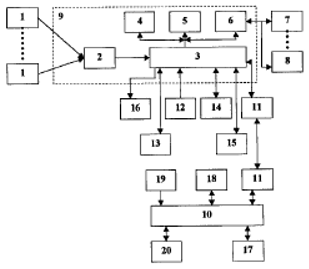


Рисунок 13.3 – Способ проведения финансовых операций и система для его осуществления

**Вывод:** получил навыки патентного поиска по заданной тематике.