УЗБЕКСКОЕ АГЕНТСТВО СВЯЗИ И ИНФОРМАТИЗАЦИИ
ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

К защите.

Зав. Кафедрой

_____

_____2010г.

Выпускная
квалификационная работа бакалавра
на тему:

Разработка технологии, алгоритмов и программных средств, обеспечения безопасности данных, хранимых на оптических носителях.

Выпускник: _____ **Аббасов А.У.**
(подпись) (фамилия)

Руководитель: _____ _____.
(подпись) (фамилия)

БЖД: _____ _____
(подпись) (фамилия)

Рецензент: _____ _____
(подпись) (фамилия)

ТАШКЕНТ-2010

ТАШКЕНТСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Факультет: ИИТ кафедра: Информационные технологии

Направление (специальность): Информатика и информационные технологии

УТВЕРЖДАЮ

Зав кафедрой _____

_____ _____ 2010 г.

ЗАДАНИЕ

на выпускную квалификационную работу

Аббасова Акмаля Улугбековича

1. Тема работы: **Разработка технологии, алгоритмов и программных средств, обеспечения безопасности данных, хранимых на оптических носителях.**

2. Утверждена приказом по университету от 12.01.2010 года № 26-07

3. Срок сдачи законченной работы _____

4. Исходные данные к работе Литературные данные, материалы предвыпускной практики, входящие данные .

5. Содержание расчётно – пояснительной записи (перечень подлежащих разработке вопросов) Аннотация, Введение, Проблемы информационной безопасности. Задачи защиты информации и анализ современных угроз безопасности, Глава II. Технологии защиты информации. Проектирование системы защиты данных, хранимых на оптических носителях, Глава III. Разработка программных средств системы защиты данных, хранимых на оптических носителях, Глава 4 Обеспечение безопасности жизнедеятельности, Заключение, Использованные литературы, Приложение

6. Перечень графического материала Презентационные материалы

7. Дата выдачи задания

Руководитель _____ Задание принял _____

(подпись) (подпись)

8. Консультанты по отдельным разделам выпускной работы

Раздел	Ф.И.О руководителя	Подпись дата	
		Задание выдал	Задание получил
Основная часть			
БЖД			

9. График выполнения работы

№	Наименование раздела работы	Срок выполнения	Отметка руководителя о выполнении
1	Введение		
2	Глава I. Проблемы информационной безопасности. Задачи защиты информации и анализ современных угроз безопасности.		
3	Глава II. Технологии защиты информации. Проектирование системы защиты данных, хранимых на оптических носителях.		
4	Глава III. Разработка программных средств системы защиты данных, хранимых на оптических носителях.		
5	Глава IV. Обеспечение безопасности жизнедеятельности		
6	Заключение		

Выпускник _____ -_____- _____ 2010г.

(подпись)

Руководитель _____ -_____- _____ 2010г.

(подпись)

А Н Н О Т А Ц И Я

В данной выпускной квалификационной работе рассматриваются задачи повышения безопасности информации хранимой на оптическом носителе.

На основе проведенных исследований разработано программное средство для обеспечения безопасности информации хранимой на оптическом носителе.

MAZMUNNOMA

Ushbu bakalavrlik malakaviy ishida optik xotiralarda saqlanadigan ma’lumot xavfsizligini oshirish masalasi ko’rib chiqilgan.

Olib borilgan tadqiqotlar asosida, optik xotirada saqlanuvchi ma’lumotni xavfsizligini ta’minlovchi dasturiy vosita ishlab chiqildi.

A B S R T A C T

In this graduation qualifying work, problems of protection user data, storaged in optical device are considered.

Based on the studies developed software which provide protection of user data stored in optical device.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Республика Узбекистан наряду с развивающимися странами мира вступает на путь информатизации всех областей жизнедеятельности человека. В Республике ведутся масштабные работы по информатизации органов государственного управления, министерств, ведомств, концернов, ассоциаций, организаций, предприятий, школ и высших учебных заведений. Информационные технологии находят широкое применение в кредитно-финансовых структурах, различных сферах экономики, науки, образования и управления. Создаются локальные, корпоративные информационно-компьютерные сети, формируются электронные информационные ресурсы, развивается индустрия информационных услуг с применением сетей связи и телекоммуникаций.

Уже сегодня многие министерства, ведомства и организации имеют возможность выхода в международные и зарубежные информационные сети, в сеть Internet. Подключение юридических и физических лиц республики к сети Internet предоставляет им возможность доступа к богатым мировым информационным ресурсам, а также представлять в мировое сообщество собственную информацию коммерческого, экономического, научно-технического, технологического и другого характера.

Надо признать, что уровень информатизации в нашей стране пока отстает, например, от Западно-Европейских стран, но уже и до нас доходят отголоски «информационной войны», мы сталкиваемся с проблемой, о которой лет 10 назад знали единицы – это проблема информационной безопасности. В данной работе выполнен краткий обзор проблемы информационной безопасности и одному из многих направлений уделено особое внимание – это обеспечение безопасности информации хранимой на оптическом носителе.

Важную роль в увеличении количества рабочих мест играет развитие и расширение сферы услуг и сервиса. Наиболее высокими темпами развивались услуги связи, информатизации, финансовые, банковские, транспортные услуги, по ремонту автомобилей и бытовой техники. Особо следует отметить динамичное развитие услуг в сфере информационно-коммуникационных технологий, которые за последние четыре года в среднем увеличиваются ежегодно на 50 процентов. В результате доля сферы услуг в ВВП возросла в 2008 году до 45,3 процента против 42,5 процента в 2007 году [1].

Самая актуальная проблема сегодняшнего дня — это разразившийся в 2008 году мировой финансовый кризис, его воздействие и негативные последствия, поиск путей выхода из складывающейся ситуации.

Получив начало с провалов и несостоятельности ипотечного кредитования в США, кризис нашел свое масштабное отражение в кризисе ликвидности важнейших банков и финансовых структур, катастрофическом падении индексов и рыночной стоимости крупнейших компаний на ведущих фондовых рынках мира. Все это, в свою очередь, явилось причиной серьезного спада производства, резкого снижения темпов роста экономики во многих странах, со всеми вытекающими отсюда негативными последствиями.

Многие ведущие аналитические и экспертные центры, анализируя и обобщая материалы, связанные с состоянием и возможными последствиями глобального финансового кризиса, приходят к следующим выводам.

Первое — подтверждаются практически глобальные масштабы кризисных процессов, происходящих в финансово-банковской системе, неизбежность рецессии и экономического спада, свертывание объемов инвестиционной активности, снижение спроса и сокращение объемов международной торговли, а также серьезные социальные потери, которые могут коснуться многих стран в мире.

Второе — разразившийся глобальный финансовый кризис продемонстрировал серьезные пробелы и необходимость кардинального реформирования действующей мировой финансово-банковской системы, подтвердил отсутствие должного контроля за деятельностью банков, которые в основном обслуживали свои корпоративные интересы, увлекаясь различными спекулятивными операциями на кредитном рынке и рынке ценных бумаг.

Третье — масштабы, глубина и последствия финансово-экономического кризиса в каждом отдельном государстве будут во многом зависеть, прежде всего, от прочности финансово-валютной системы, капитализации и ликвидности национальных кредитных институтов, их зависимости от иностранных и корпоративных банковских структур, а также размеров золото-валютных резервов и способности оплачивать зарубежные кредиты, в конечном итоге — от уровня устойчивости, диверсификации и конкурентоспособности экономики страны.

Четвертое — скорейший выход из мирового финансового кризиса и смягчение его последствий во многом зависит от эффективности и согласованности принимаемых мер в рамках отдельных государств и мирового сообщества в целом.

Состоявшийся в ноябре в Вашингтоне Саммит 20 крупнейших государств, объединяющих около 85 процентов мирового совокупного продукта, подтвердил все возрастающие масштабы глобального финансового кризиса.

Обсуждения на Саммите показали, что сегодня речь не идет о предупреждении, а только о поисках путей выхода из мирового финансового кризиса, то есть рубеж невозврата к прежним позициям практически пройден[1].

Цели и задачи исследования. Повысить безопасность информации хранимой на оптических носителях, посредством разработки технологии, алгоритмов и инструментальных средств.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Проанализировать современные угрозы информации и информационным системам.
2. Рассмотреть методы и средства защиты информации.
3. Изучить материалы по созданию безопасной информационной системы, учитывая требования предъявляемые к безопасным информационным системам.
4. Разработать технологию и алгоритмы защиты информации хранимой на оптическом носителе.
5. Разработать программное средство защиты информации хранимой на оптическом носителе.

В первой главе работы рассматривается общая проблема информационной безопасности. Проводится анализ наиболее известных угроз безопасности информации, и осуществляется их классификация. Также рассматривается требования предъявляемые к защите информации.

Во второй главе рассматриваются принципы построения систем защиты информации. Дается описание средствам защиты информации от несанкционированного доступа. Также речь идет о технологии криптографической защиты информации. Данная глава заканчивается проектированием системы защиты данных, хранимых на оптических носителях.

В третьей главе приводится структура программного средства. Разрабатывается модуль файловой системы, модуль работы с оптическими носителями, модуль сокрытия данных и пользовательский интерфейс.

1. ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. ЗАДАЧИ ЗАЩИТЫ ИНФОРМАЦИИ И АНАЛИЗ СОВРЕМЕННЫХ УГРОЗ БЕЗОПАСНОСТИ

1.1. ОСНОВНЫЕ ПОНЯТИЯ ЗАЩИТЫ ИНФОРМАЦИИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

Современные методы обработки, передачи и накопления информации способствовали появлению угроз, связанных с возможностью потери, искажения и раскрытия личных, адресованных или принадлежащих конечным пользователям данных. Поэтому, на сегодняшний день, обеспечение информационной безопасности компьютерных систем является одним из ведущих направления развития ИТ.

Информационная безопасность - такое состояние рассматриваемой системы, при котором она, с одной стороны, способна противостоять дестабилизирующему воздействию внешних и внутренних информационных угроз, а с другой - ее функционирование не создает информационных угроз для элементов самой системы и внешней среды[2].

Приведенное определение представляется достаточно полным и вполне корректным. Однако, для того, чтобы служить более конкретным ориентиром в направлении поиска путей решения проблем информационной безопасности, оно нуждается в уточнении и детализации его основополагающих понятий. При этом отправной точкой может служить тот факт, что информация как непременный компонент любой организованной системы, с одной стороны, легко уязвима (т. е. весьма доступна для дестабилизирующего воздействия большого числа разноплановых угроз), а с другой сама может быть источником большого числа разноплановых угроз как для элементов самой системы, так и для внешней среды. Отсюда естественным образом вытекает, что обеспечение информационной безопасности в общей постановке проблемы может быть достигнуто лишь при взаимоувязанном решении трех составляющих проблем:

- **первая** - защита находящейся в системе информации от дестабилизирующего воздействия внешних и внутренних угроз информации;
- **вторая** - защита элементов системы от дестабилизирующего воздействия внешних и внутренних информационных угроз;
- **третья** - защита внешней среды от информационных угроз со стороны рассматриваемой системы.

В соответствии с изложенным общая схема обеспечения информационной безопасности может быть представлена так, как показано на рис. 1.1.

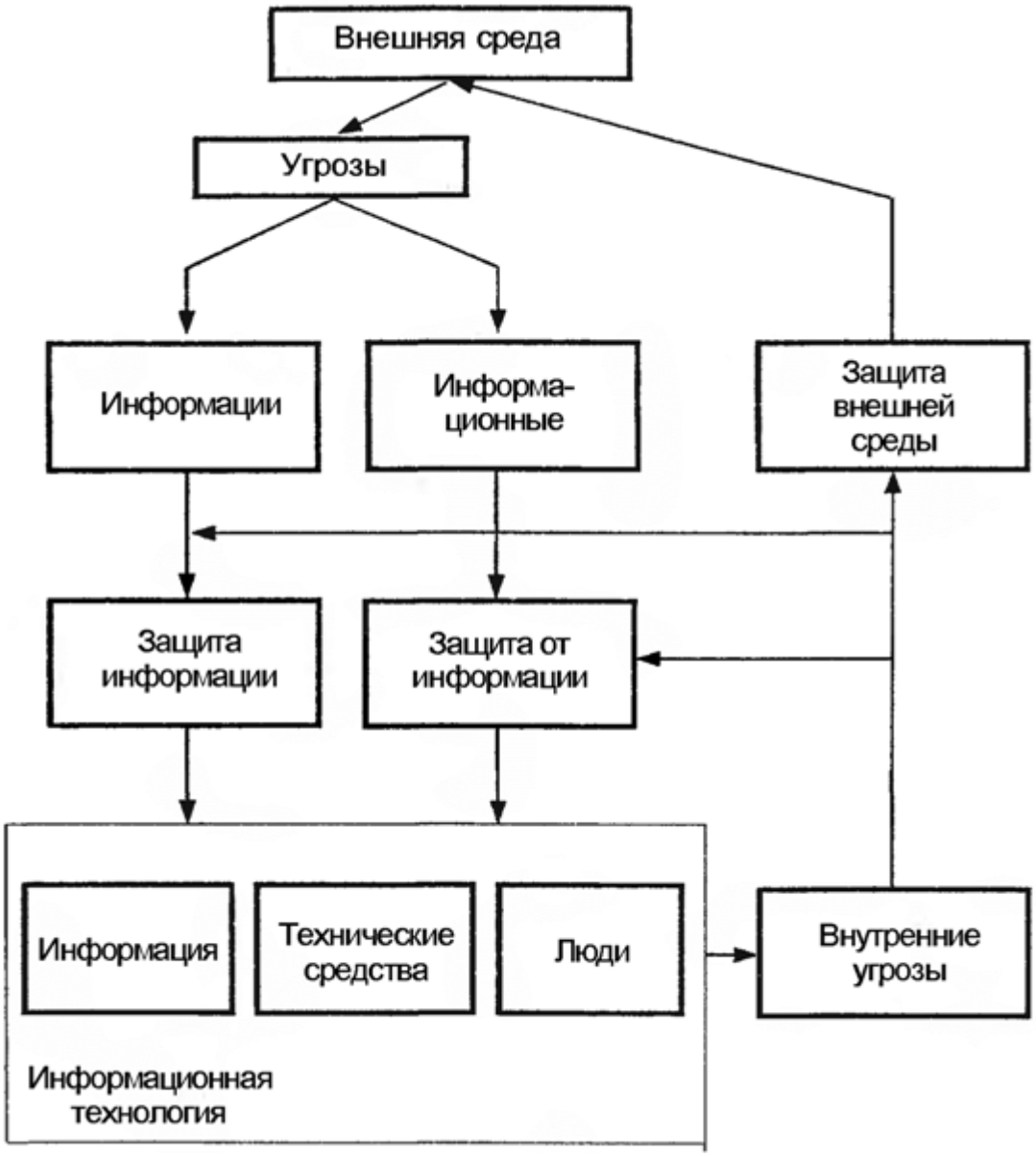

Рисунок. 1.1. Общая схема обеспечения информационной безопасности

Естественно, что проблемы информационной безопасности являются производными относительно более общих проблем информатизации. Поэтому содержание проблем информационной безопасности должно формироваться в строгом соответствии с содержанием проблем информатизации, а концептуальные подходы к их решению должны взаимоувязываться с концепциями информатизации.

К основным концептуальным вопросам информатизации, на базе которых должны решаться и проблемы информационной безопасности, очевидно, могут быть отнесены:

- сущность информатизации;
- конечные результаты информатизации;
- пути, средства и методы достижения основных результатов информатизации.

Не вдаваясь в философские аспекты информатизации, а взяв за основу ее прагматическое значение, можно с полным основанием утверждать, что сущность информатизации заключается в формировании такой информационной среды, в которой имелись бы все объективные предпосылки, необходимые для наиболее рационального информационного обеспечения всех сфер деятельности современного общества. Создание такой среды естественно предполагает всеобщую компьютеризацию, однако она представляет собой лишь компонент (хотя и один из важнейших) формирования общей инфраструктуры информационной среды.

В этих условиях производство, переработка и использование информации становятся важнейшей отраслью экономики, которая и получила общепризнанное название информационной индустрии. Таким образом, создание объективных предпосылок, необходимых для формирования информационной индустрии, и составляет основное содержание информатизации современного общества. При этом научно-методологическим базисом этого процесса служит такая отрасль науки, как информатика.

Перед информатикой фактически стоят две основные задачи: изучение информационных проблем общества и разработка путей, методов и средств наиболее рационального их решения. Изучение информационных проблем поставлено нами на первое место совсем не случайно. Этим однозначно определяется, что такое изучение является исходным базисом для реализации второй основной задачи информатики - разработки путей, методов и средств наиболее рационального решения этих проблем и прежде всего удовлетворения информационных потребностей общества в процессе его жизнедеятельности. Таким образом, пути, методы и средства информатизации должны разрабатываться исходя из информационных потребностей. Однако, в соответствии с законом об обратной связи, и информационные потребности общества должны максимально приспосабливаться к возможностям их удовлетворения. Это означает, что информационные процессы в различных сферах деятельности должны быть целенаправленно подготовлены к переводу их на индустриальные методы осуществления.

Структурированные таким образом информационные потребности общества и являются одной из основных предпосылок для разработки необходимого арсенала методов и средств информатизации. Основу этого арсенала должны составлять унифицированные методы и современные средства обработки информации. На их базе и должна разрабатываться концепция индустриализации переработки информации и необходимые для этого информационные технологии.

Объективные предпосылки индустриализации процесса информационного обеспечения различных сторон деятельности современного общества создаются совокупностью результатов, полученных в последнее время в рамках информатики. К ним, прежде всего относятся:

- системная классификация информации;
- унификация структуры информационного потока;
- унификация процедур (задач) обработки информации;

- систематизация методов обработки информации;
- унификация информационной технологии;
- формирование концепции управления процессами обработки
- информации по унифицированной технологии.

Последний из приведенных здесь результатов носит многоаспектный характер. Причем одной из основных его составляющих является проблема обеспечения информационной безопасности.

Современное состояние изучения и практической разработки проблемы информационной безопасности может быть оценено следующим образом. Первая ее составляющая, т. е. проблема защиты информации, уже продолжительное время (свыше 30 лет) находится в центре внимания специалистов, и к настоящему времени достигнуты следующие результаты:

- проблема получила практически всеобщее признание;
- заложены основы разработки теории защиты;
- налажено производство средств защиты;
- организована планомерная подготовка и повышение квалификации специалистов соответствующего профиля;
- создана государственная система защиты информации;
- накоплен значительный опыт практического решения задач защиты информации в системах различного масштаба и функционального назначения.

На основе перечисленных результатов справедливым будет утверждение, что проблема защиты информации имеет определенный базис для дальнейшего целенаправленного развития. При этом основные задачи дальнейшего развития могут быть сформулированы следующим образом.

Первая задача - регулярный сбор и обработка статистических данных о составе и результатах функционирования реальных систем защиты.

Полученные таким образом данные необходимы как для совершенствования методологии проектирования новых систем защиты и повышения эффективности их функционирования, так и для дальнейшего развития теории защиты, поскольку те основы, которые упоминались выше, носят по преимуществу вербальный характер. Развитая же теория должна содержать количественные методы анализа и синтеза систем защиты и управления ими в процессе функционирования.

Вторая задача - заключается в создании организационных структур, обеспечивающих решение первой задачи. Такие организационные структуры могут, например, формироваться в виде специализированных региональных центров защиты, на базе которых можно было бы развернуть эффективную систему сбора и обработки статистических данных, а также обеспечить оказание широкого спектра услуг своим абонентам.

Третья задача - это дальнейшее развитие научно-методологического базиса как основы интенсификации процессов защиты [6]. Составляющими частями данной задачи выступают:

во-первых, формирование более общей (по сравнению с классической) теории систем, ориентированной не только на технические, но и на социальные системы;

во-вторых, разработка на основе вербальной теории строгой теории защиты, базисом которой должны служить общая теория систем и статистические данные о структуре и функционировании систем защиты информации, получаемые при решении первой сформулированной задачи;

в-третьих, разработка комплекса рабочих моделей, необходимых и достаточных для решения всех задач защиты информации.

Так в самом общем виде могут быть представлены состояние и основные направления развития защиты информации как первой составляющей общей проблемы информационной безопасности.

1.2. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И.

Информационная безопасность подчеркивает важность информации в современном обществе - понимание того, что информация - это ценный ресурс, нечто большее, чем отдельные элементы данных.

Под угрозой (в общем смысле) обычно понимают потенциально возможное событие (воздействие, процесс или явление), которое может привести к нанесению ущерба чьим-либо интересам. В дальнейшем под угрозой безопасности автоматических систем (АС) обработки информации будем понимать возможность воздействия на АС, которое прямо или косвенно может нанести ущерб ее безопасности.

В настоящее время известен обширный перечень угроз информационной безопасности АС, содержащий сотни позиций.

Рассмотрение возможных угроз информационной безопасности проводится с целью определения полного набора требований к разрабатываемой системе зашиты.

Перечень угроз, оценки вероятностей их реализации, а также модель нарушителя служат основой для анализа риска реализации угроз и формулирования требований к системе защиты АС. Кроме выявления возможных угроз, целесообразно проведение анализа этих угроз на основе их классификации по ряду признаков. Каждый из признаков классификации отражает одно из обобщенных требований к системе защиты. Угрозы, соответствующие каждому признаку классификации, позволяют детализировать отражаемое этим признаком требование.

Необходимость классификации угроз информационной безопасности АС обусловлена тем, что хранимая и обрабатываемая информация в современных АС подвержена воздействию чрезвычайно большого числа факторов, в силу чего становится невозможным формализовать задачу описания полного множества угроз. Поэтому для защищаемой системы обычно определяют не полный перечень угроз, а перечень классов угроз.

В табл. 1.2 перечислены основные методы реализации угроз информационной безопасности.

Таблица 1.2. Методы реализации угроз.

Уровень доступа к информации в АС	Угроза раскрытия параметров системы	Угроза нарушения конфиденциальности	Угроза нарушения целостности	Угроза отказа служб (отказа доступа к информации)
Уровень носителей информации	Определение типа и параметров носителей информации	Хищение (копирование) носителей информации Перехват ПЭМИН	Уничтожение машинных носителей информации	Выведение из строя машинных носителей информации
Уровень средств взаимодействия с носителем	Получение информации о программно-аппаратной среде Получение детальной информации о функциях, выполняемых АС Получение данных о применяемых системах защиты	Несанкционированный доступ к ресурсам АС Совершение пользователем несанкционированных действий Несанкционированное копирование программного обеспечения Перехват данных, передаваемых по каналам связи	Внесение пользователем несанкционированных изменений в программы и данные Установка и использование нештатного программного обеспечения Заражение программными вирусами	Проявление ошибок проектирования и разработки программно-аппаратных компонент АС Обход механизмов защиты АС
Уровень представления информации	Определение способа представления информации	Визуальное наблюдение Раскрытие представления информации (дешифрование)	Внесение искажения в представление данных; уничтожение данных	Искажение соответствия синтаксических и семантических конструкций *языка*
Уровень содержания информации	Определение содержания данных на качественном уровне	Раскрытие содержания информации	Внедрение дезинформации	Запрет на использование информации

Для достижения требуемого уровня информационной безопасности АС необходимо обеспечить противодействие различным техническим угрозам и минимизировать возможное влияние «человеческого фактора».

1.3. ТРЕБОВАНИЯ К ЗАЩИТЕ ИНФОРМАЦИИ.

В самом общем виде и на чисто прагматическом уровне требования к защите могут быть определены как предотвращение угроз информации, по крайней мере тех из них, проявление которых может привести к существенно значимым последствиям. Но поскольку, как уже неоднократно нами отмечалось, защита информации есть случайный процесс (показатели уязвимости носят вероятностный характер), то и требования к защите должны выражаться терминами и понятиями теории вероятностей.

По аналогии с требованиями к надежности технических систем, обоснованными в классической теории систем, требования к защите могут быть сформулированы в виде условия:

(1.3)

где $\mathbf{P_3}$ - оценка реальной вероятности защищенности информации, а $\mathbf{P_3}$ - требуемый уровень защищенности.

С требованиями, выраженными в таком виде, можно оперировать с использованием методов классической теории систем. Однако на практике решение проблем защиты информации сопряжено с исследованиями и разработкой таких систем и процессов, в которых и конкретные методы, и общая идеология классической теории систем могут быть применены лишь с большими оговорками. Для повышения степени адекватности применяемых моделей реальным процессам необходим переход от концепции создания инструментальных средств получения необходимых решений на инженерной основе к концепции создания методологического базиса и инструментальных средств для динамического оптимального управления соответствующими

процессами (иными словами снова встает проблема перехода от экстенсивных к интенсивным способам решения проблем защиты информации).

Проблема определения требований к защите информации имеет комплексный характер и может рассматриваться как в организационном, так и в техническом аспектах. Причем в условиях автоматизированной обработки информации существует большое количество каналов несанкционированного ее получения, которые не могут быть перекрыты без применения специфических технических и программно-аппаратных средств. Это серьезно повышает удельный вес технических аспектов и приводит к необходимости определения требований к системам защиты, содержащим указанные средства.

Наиболее подходящим здесь оказывается подход, основанный на выделении некоторого количества типовых систем защиты, рекомендуемых для использования в тех или иных конкретных условиях и содержащих определенные механизмы защиты, т.е. подход, базирующийся на создании системы стандартов в области защиты информации.

Кроме того, имеются стандарты, касающиеся защиты информации от ее утечки через побочные электромагнитные излучения и наводки (ПЭМИН).

Рассмотрим возможные подходы к определению значений перечисленных показателей.

Важность информации. В соответствии с изложенным выше, важность информации должна оцениваться по двум группам критериев - по назначению информации и по условиям ее обработки.

В первой группе, очевидно, следует выделить две составляющие - важность задач для обеспечиваемой деятельности и степень важности информации для эффективного решения соответствующих задач.

Во второй группе также выделим две составляющих - уровень потерь в случае реализации угроз безопасности информации и уровень затрат на восстановление измененной информации.

Полнота информации. Полнота представляет собой показатель, характеризующий достаточность информации для решения соответствующих задач. Поэтому, чтобы иметь возможность определять данный показатель, необходимо для каждой задачи или группы задач заблаговременно составить перечень сведений, которые требуются для их решения.

Адекватность информации. Под адекватностью традиционно понимается степень соответствия оцениваемой информации действительному состоянию тех реалий, которые она отображает. В общем случае адекватность определяется двумя параметрами -объективностью генерирования информации и продолжительностью интервала времени между моментом генерирования и текущим моментом, т.е. моментом оценивания ее адекватности.

Объективность генерирования информации, очевидно, зависит от способа получения значений интересующих нас характеристик и качества его реализации.

Как и в случае оценки важности информации предположим, что при высоком качестве определения значения непосредственно и притом количественно измеряемой характеристики адекватность соответствующей информации будет близка к 1, а при низком качестве определения значения неизмеряемой характеристики, не имеющей даже отдаленного аналога, адекватность информации близка к нулю.

Релевантность информации. Релевантность характеризует соответствие информации потребностям решаемой задачи. Для количественного выражения данного показателя обычно используют так называемый коэффициент релевантности $\mathbf{K_p}$, определяющий отношение объема релевантной информации $\mathbf{N_p}$ к общему объему анализируемой информации $\mathbf{N_0}$:

$$K_p = N$$

(1.4)

Толерантность информации. Толерантность, как отмечалось выше, есть показатель, характеризующий удобство восприятия и использования информации в процессе решения задачи. Уже из самого определения видно, что понятие толерантности является очень широким, в значительной мере неопределенным и субъективным. Даже для цифровой информации значение толерантности может быть самым различным. Поэтому вряд ли можно надеяться на разработку строго формальной методики определения показателя толерантности. Из эвристических методов наиболее подходящими здесь представляются методы экспертно-лингвистических оценок. При этом в качестве значений лингвистической переменной могут быть использованы такие понятия, как: «весьма удобно, комфортно» (информация представлена в таком виде, что ее использование в процессе решения задачи происходит естественным образом, не требуя дополнительных усилий), «удобно» (использование информации если и требует дополнительных усилий, то лишь незначительных), «средне» (использование информации требует дополнительных усилий, вообще говоря, допустимых), «плохо» (использование информации сопряжено с большими трудностями), «очень плохо» (использование информации или вообще невозможно, или требует неоправданно больших усилий).

1.4. ПОСТАНОВКА ЗАДАЧИ И ЦЕЛИ ИССЛЕДОВАНИЯ.

Информация давно перестала быть просто необходимым для производства вспомогательным ресурсом или побочным проявлением всякого рода деятельности. Она приобрела ощутимый стоимостный вес, который четко определяется реальной прибылью, получаемой при ее использовании, или размерами ущерба, с разной степенью вероятности наносимого владельцу информации. Однако создание индустрии переработки информации порождает целый ряд сложных проблем. Одной из таких проблем является надежное обеспечение сохранности и установленного статуса информации,

циркулирующей и обрабатываемой в информационно-вычислительных системах и сетях.

Целью данной выпускной квалификационной работы является исследования проблем зашиты информации, изучения средств и методов зашиты информации и на основе полученных данных разработать технологию, алгоритмы и программное средство для обеспечения безопасности данных хранимых на оптических носителях.

Основные задачи:

- Повысить безопасность информации хранимой на оптических носителях, посредством разработки технологии, алгоритмов и инструментальных средств.

Выполняемые функции:

- Запись данных на оптический носитель с применением шифрования.
- Копирования данных с оптических носителей в жесткий диск с применением дешифрования.

Выводы.

В данной главе были рассмотрены понятии информационной безопасности и защиты информации. Обсуждались проблемы защиты информации и информационных систем, были рассмотрены современные угрозы безопасности информации и требования к защите информации и информационных систем.

2. ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ. ПРОЕКТИРОВАНИЕ СИСТЕМЫ ЗАЩИТЫ ДАННЫХ, ХРАНИМЫХ НА ОПТИЧЕСКИХ НОСИТЕЛЯХ.

2.1. ПРИНЦИПЫ ПОСТРОЕНИЕ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ.

Вопросы организации защиты информации должны решаться уже на предпроектной стадии разработки ИС.

Погрешности защиты могут быть в значительной мере устранены, если при проектировании учитывать следующие основные принципы построения системы защиты:

1. Простота механизма защиты. Этот принцип общеизвестен, но не всегда глубоко осознается. Механизмы защиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано со знанием специальных языков или с выполнением трудоемких действий при обычной работе законных пользователей.

2. Постоянство защиты. Надежный механизм, реализующий это требование, должен быть постоянно защищен от несанкционированных изменений. Ни одна компьютерная система не может рассматриваться как безопасная, если основные аппаратные и программные механизмы, призванные обеспечивать безопасность, сами являются объектами несанкционированной модификации или видоизменения.

3. Контроль должен быть всеобъемлющим. Этот принцип предполагает необходимость проверки полномочия любого обращения к любому объекту и является основой системы защиты.

4. Несекретность проектирования — механизм защиты должен функционировать достаточно эффективно даже в том случае, если его структура и содержание известны злоумышленнику. Не имеет смысла засекречивать детали реализации системы защиты, предназначенной для широкого использования. Эффективность защиты не должна зависеть от того,

насколько опытны потенциальные нарушители. Защита не должна обеспечиваться только секретностью структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно способствовать ее преодолению (даже автору).

5. Идентификация. Каждый объект ИС должен однозначно идентифицироваться. При попытке получения доступа к информации решение о санкционировании его следует принимать на основании данных претендента и наивысшей степени секретности информации, с которой он может работать. Такие данные об идентификации и полномочиях должны надежно сохраняться и обновляться компьютерной системой для каждого активного участника системы, выполняющего действия, затрагивающие ее безопасность. Пользователи должны иметь соответствующие полномочия, объекты (файлы) — соответствующий гриф, а система должна контролировать все попытки получения доступа.

6. Разделение полномочий — применение нескольких ключей защиты. Наличие нескольких ключей защиты удобно в тех случаях, когда право на доступ определяется выполнением ряда условий.

7. Минимальные полномочия. Для любой программы и любого пользователя должен быть определен минимальный круг полномочий, необходимых для работы.

8. Надежность. Система ЗИ должна иметь механизм, который позволил бы оценить обеспечение достаточной надежности функционирования СЗИ (соблюдение правил безопасности, секретности, идентификации и отчетности). Для этого необходимы выверенные и унифицированные аппаратные и программные средства контроля. Целью применения данных механизмов является выполнение определенных задач методом, обеспечивающим безопасность.

9. Максимальная обособленность механизма защиты означает, что защита должна быть отделена от функций управления данными.

10. Защита памяти. Пакет программ, реализующих защиту, должен размещаться в защищенном поле памяти, чтобы обеспечить системную локализацию попыток проникновения извне. Даже попытка проникновения со стороны программ операционной системы должна автоматически фиксироваться, документироваться и отвергаться, если вызов выполнен некорректно.

11. Удобство для пользователей: схема защиты должна быть в реализации простой, чтобы механизм защиты не создавал для пользователей дополнительных трудностей.

12. Контроль доступа к СВТ на основании авторизации пользователя по его физическому ключу и личному PIN-коду. Этот механизм дает защиту от атак неавторизованных пользователей на:

- доступ к ресурсам ПК;
- доступ к областям HD ПК;
- доступ к ресурсам и серверам сети;
- доступ к модулям выполнения авторизации пользователей.

13. Авторизация пользователя на основании физического ключа позволяет исключить непреднамеренную дискредитацию его прав доступа.

14. Отчетность. Необходимо защищать контрольные данные от модификации и несанкционированного уничтожения, чтобы обеспечить обнаружение и расследование выявленных фактов нарушения безопасности. Надежная система должна сохранять сведения о всех событиях, имеющих отношение к безопасности, в контрольных журналах. Кроме того, она должна гарантировать вам выбор интересующих событий при проведении аудита, чтобы минимизировать стоимость аудита и повысить эффективность анализа. Наличие программных средств аудита или создание отчетов еще не означает ни усиления безопасности, ни наличия гарантий обнаружения нарушений.

15. **Доступность к исполнению** только тех команд операционной системы, которые не могут повредить операционную среду и результат контроля предыдущей аутентификации.

16. **Наличие механизма защиты** информации, циркулирующей в локальной и распределенной сети. Данный механизм защищает от атак несанкционированных и недобросовестных пользователей:

- несанкционированное чтение информации;
- модификацию хранящейся и циркулирующей в сети информации;
- навязывание информации;
- отказ от авторства переданной информации.

17. **Системный подход** к защите информации предполагает необходимость учета всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для обеспечения безопасности ИС.

18. **Возможность наращивания**. Система защиты должна строиться с учетом не только всех известных каналов проникновения и НСД к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

19. **Комплексный подход** предполагает согласованное применение разнородных средств защиты информации.

20. **Адекватность** — обеспечение требуемого уровня защиты (определяется степенью секретности подлежащей обработке информации) при минимальных издержках на создание механизма защиты и обеспечение его функционирования. Важно правильно выбрать тот достаточный уровень защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми (задача анализа риска).

21. **Минимизация привилегий** в доступе, предоставляемых пользователям, т.е. каждому пользователю должны предоставляться только

действительно необходимые ему права по обращению к ресурсам системы и данным.

22. Полнота контроля — обязательный контроль всех обращений к защищаемым данным.

23. Наказуемость нарушений. Наиболее распространенная мера наказания — отказ в доступе к системе.

24. Экономичность механизма — обеспечение минимальности расходов на создание и эксплуатацию механизма.

25. Принцип системности сводится к тому, что для обеспечения надежной защиты информации в современных ИС должна быть обеспечена надежная и согласованная защита во всех структурных элементах, на всех технологических участках автоматизированной обработки информации и во все время функционирования ИС.

26. Специализированность, как принцип организации защиты, предполагает, что надежный механизм защиты может быть спроектирован и организован лишь профессиональными специалистами по защите информации. Кроме того, для обеспечения эффективного функционирования механизма защиты в состав ИС должны быть включены соответствующие специалисты.

27. Принцип неформальности означает, что методология проектирования механизма защиты и обеспечения его функционирования в основе своей — неформальна. В настоящее время не существует инженерной (в традиционном понимании этого термина) методики проектирования механизма защиты. Методики проектирования, разработанные к настоящему времени, содержат комплексы требований, правил, последовательность и содержание этапов, которые сформулированы на неформальном уровне, т.е. механическое их осуществление в общем случае невозможно.

28. Гибкость системы защиты Принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Для

обеспечения возможности варьирования уровнем защищенности, средства защиты должны обладать определенной гибкостью. Особенно важно это свойство в тех случаях, когда установку средств защиты необходимо осуществлять на работающую систему, не нарушая процесса ее нормального функционирования.

29. Принцип непрерывности защиты предполагает, что защита информации — это не разовое мероприятие и даже не определенная совокупность проведенных мероприятий и установленных средств защиты, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла ИС. Разработка системы защиты должна осуществляться параллельно с разработкой защищаемой системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные защищенные информационные системы.

2.2. СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ.

Направления обеспечения безопасности вообще рассматриваются как нормативно-правовые категории, определяющие комплексные меры защиты информации на государственном уровне, на уровне предприятия и организации, на уровне отдельной личности.

С учетом сложившейся практики обеспечения информационной безопасности выделяют следующие направления защиты информации:

- правовая защита — это специальные законы, другие нормативные акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе;
- организационная защита — это регламентация производственной деятельности и взаимоотношений исполнителей на

нормативно-правовой основе, исключающая или ослабляющая нанесение какого-либо ущерба исполнителям;

■ инженерно-техническая защита — это использование различных технических средств, препятствующих нанесению ущерба коммерческой деятельности.

Кроме этого, защитные действия, ориентированные на обеспечение информационной безопасности, могут быть охарактеризованы целым рядом параметров, отражающих, помимо направлений, ориентацию на объекты защиты, характер угроз, способы действий, их распространенность, охват и масштабность.

Так, по характеру угроз защитные действия ориентированы на защиту информации от разглашения, утечки и несанкционированного доступа. По способам действий их можно подразделить на предупреждение, выявление, обнаружение, пресечение и восстановление ущерба или иных убытков. По охвату защитные действия могут быть ориентированы на территорию, здание, помещение, аппаратуру или отдельные элементы аппаратуры.

Рис 2.1. Средства защиты информации.

.2.2.1. Правовая защита

Как известно, право — это совокупность общеобязательных правил и норм поведения, установленных или санкционированных государством в отношении определенных сфер жизни и деятельности государственных органов, предприятий (организаций) и населения (отдельной личности).

Правовая защита информации как ресурса признана на международном, государственном уровне и определяется межгосударственными договорами, конвенциями, декларациями и реализуется патентами, авторским правом и лицензиями на их защиту. На государственном уровне правовая защита регулируется государственными и ведомственными актами.

Современные условия требуют и определяют необходимость комплексного подхода к формированию законодательства по защите информации, его состава и содержания, соотнесения его со всей системой законов и правовых актов.

Требования информационной безопасности должны органически включаться во все уровни законодательства, в том числе и в конституционное законодательство, основные общие законы, законы по организации государственной системы управления, специальные законы, ведомственные правовые акты и другие. В литературе приводится такая структура правовых актов, ориентированных на правовую защиту информации. Первый блок — конституционное законодательство. Нормы, касающиеся вопросов информатизации и защиты информации, входят в него как составные элементы. Второй блок — общие законы, кодексы (о собственности, о недрах, о земле, о правах граждан, о гражданстве, о налогах, об антимонопольной деятельности), которые включают нормы по вопросам информатизации и информационной безопасности. Третий блок — законы об организации управления, касающиеся отдельных структур хозяйства, экономики, системы государственных органов и определяющие их статус. Они включают отдельные нормы по вопросам защиты информации. Наряду с общими вопросами информационного обеспечения и

защиты информации конкретного органа эти нормы до должны устанавливать е го обязанности по формированию, актуализации и безопасности информации, представляющей общегосударственный интерес. Четвертый блок — специальные законы, полностью относящиеся к конкретным сферам отношений.

2.2.2 Организационная защита

Организационная защита — это регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающей или существенно затрудняющей неправомерное овладение конфиденциальной информацией и проявление внутренних и внешних угроз. Организационная защита обеспечивает:

- организацию охраны, режима, работу с кадрами, с документами;
- использование технических средств безопасности и информационно-аналитическую деятельность по выявлению внутренних и внешних угроз пред-принимательской деятельности.

Организационные мероприятия играют существенную роль в создании надежного механизма защиты информации, так как возможности несанкционированного использования конфиденциальных сведений в значительной мере обусловливаются не техническими аспектами, а злоумышленными действиями, нерадивостью, небрежностью и халатностью пользователей или персонала защиты. Влияния этих аспектов практически невозможно избежать с помощью технических средств. Для этого необходима совокупность организационно-правовых и организационно-технических мероприятий, которые исключали бы (или, по крайней мере, сводили бы к минимуму) возможность возникновения опасности конфиденциальной информации.

2.2.3. Инженерно техническая защита

На вооружении промышленных шпионов, недобросовестных конкурентов и просто злоумышленников находятся самые разнообразные средства проникновения на объекты противоправных интересов и получения конфиденциальной информации. В этих условиях в интересах обеспечения информационной безопасности необходимы адекватные по ориентации, функциональному назначению и другим характеристикам технические средства защиты охраняемых секретов.

Инженерно-техническая защита (ИТЗ) по определению — это совокупность специальных органов, технических средств и мероприятий по их использованию в интересах защиты конфиденциальной информации. Многообразие целей, задач, объектов защиты и проводимых мероприятий предполагает рассмотрение некоторой системы классификации средств по виду, ориентации и другим характеристикам.

Многообразие классификационных характеристик позволяет рассматривать инженерно-технические средства по объектам воздействия, характеру мероприятий, способам реализации, масштабу охвата, классу средств злоумышленников, которым оказывается противодействие со стороны службы безопасности. По функциональному назначению средства инженерно-технической защиты делятся на следующие группы:

- физические средства, включающие различные средства и сооружения, препятствующие физическому проникновению (или доступу) злоумышленников на объекты защиты и к материальным носителям конфиденциальной информации и осуществляющие защиту персонала, материальных средств, финансов и информации от противоправных воздействий;

- аппаратные средства. Сюда входят приборы, устройства, приспособления и другие технические решения, используемые в интересах защиты

информации. В практике деятельности предприятия находит широкое применение самая различная аппаратура, начиная с телефонного аппарата до совершенных автоматизированных систем, обеспечивающих производственную деятельность. Основная задача аппаратных средств — обеспечение стойкой защиты информации от разглашения, утечки и несанкционированного доступа через технические средства обеспечения производственной деятельности;

- программные средства, охватывающие специальные программы, программные комплексы и системы защиты информации в информационных системах различного назначения и средствах обработки (сбора, накопления, хранения, обработки и передачи) данных;
- криптографические средства— это специальные математические и алгоритмические средства защиты информации, передаваемой по системам и сетям связи, хранимой и обрабатываемой на ЭВМ с использованием разнообразных методов шифрования.

Аппаратные средства и методы защиты распространены достаточно широко. Однако из-за того, что они не обладают достаточной гибкостью, часто теряют свои защитные свойства при раскрытии их принципов действия и в дальнейшем не могут быть используемы. Программные средства и методы защиты надежны и период их гарантированного использования без перепрограммирования значительно больше, чем аппаратных. Криптографические методы занимают важное место и выступают надежным средством обеспечения защиты информации на длительные периоды.

Очевидно что такое деление средств защиты информации достаточно условно, так как на практике очень часто они: и взаимодействуют и реализуются в комплексе в виде программно-аппаратных модулей с широким использованием алгоритмов закрытия информации.

2.2.3.1. Физические средства защиты

Физические средства защиты — это разнообразные устройства, приспособления, конструкции, аппараты, изделия, предназначенные для создания препятствий на пути движения злоумышленников. К физическим средствам относятся механические, электромеханические электронные, электронно-оптические, радио- и радиотехнические и другие устройства для воспрещение несанкционированного доступа (входа выхода) проноса (выноса) средств и материалов и других возможна видов преступных действий. Эти средств применяются для решения следующих задач:

1. охрана территории предприятия и наблюдение за ней;
2. охрана зданий» внутренних помещений и контроль за ними;
3. охрана оборудования, продукции, финансов и информации;
4. осуществление контролируемого доступа в здания и помещения.

Все физические средства защиты объектов можно разделить на три категории: средства предупреждения средства обнаружения и системы ликвидации угроз.

2.2.3.2. Аппаратные средства защиты

К аппаратным средствам защиты информации относятся самые различные по принципу действия, устройству и возможностям технические конструкции, обеспечивающие пресечение разглашения, защиту от утечки и противодействие несанкционированному доступу к источникам конфиденциальной информации. Аппаратные средства защиты информации применяются для решения следующих задач:

- проведение специальных исследований технических средств обеспечения производственной деятельности на наличие возможных каналов утечки информации;

- выявление каналов утечки информации на разных объектах и в помещениях;
- локализация каналов утечки информации;
- поиск и обнаружение средств промышленного шпионажа;
- противодействие несанкционированному доступу к источникам конфиденциальной информации и другим действиям.

По функциональному назначению аппаратные средства могут быть классифицированы на средства обнаружения, средства поиска и детальных измерений, средства активного и пассивного противодействия. При этом по своим техническим возможностям средства защиты информация могут быть общего назначения, рассчитанные на использование непрофессионалами с целью получения предварительных (общих) оценок, и профессиональные комплексы, позволяющие проводить тщательный поиск, обнаружение и прецизионные измерения все характеристик средств промышленного шпионажа.

2.2.3.3. Программные средства защиты

Системы защиты компьютера от чужого вторжения весьма разнообразны и классифицируются, как:

- средства собственной защиты, предусмотренные общим программным обеспечением;
- средства защиты в составе вычислительной системы;
- средства защиты с запросом информации;
- средства активной защиты;
- средства пассивной защиты и другие.

Можно выделить следующие направления использования программ для обеспечения безопасности конфиденциальной информации, в частности такие:

- защита информации от несанкционированного доступа;
- защита информации от копирования;
- защита программ от копирования;
- защита программ от вирусов;
- защита информации от вирусов;
- программная защита каналов связи.

По каждому из указанных направлений имеется достаточное количество качественных, разработанных профессиональными организациями и распространяемых на рынках программных продуктов (рис. 21). Программные средства защиты имеют следующие разновидности специальных программ:

- идентификации технических средств, файлов и аутентификации пользователей;
- регистрации и контроля работы технических средств и пользователей;
- обслуживания режимов обработки информации ог-раниченного пользования;
- защиты операционных средств ЭВМ и прикладных программ пользователей;
- уничтожения информации в защитные устройства после использования;
- сигнализирующих нарушения использования ресурсов;
- вспомогательных программ защиты различного назначения.

Идентификация технических средств и файлов, осуществляемая программно, делается на основе анализа регистрационных номеров различных компонентов и объектов информационной системы и сопоставления их со значениями адресов и паролей, хранящихся в защитном устройстве системы управления. Для обеспечения надежности защиты с помощью паролей работа

системы защиты организуется таким образом, чтобы вероятность раскрытия секретного пароля и установления соответствия тому или иному идентификатору файла или терминала была как можно меньше. Для этого надо периодически менять пароль, а число символов в нем установить достаточно большим.

2.3. ТЕХНОЛОГИЯ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ.

Криптография является методологической основой современных систем обеспечения безопасности информации в компьютерных системах и сетях. Исторически криптография (в переводе с греческого этот термин означает «тайнопись») зародилась как способ скрытой передачи сообщений. Криптография представляет собой совокупность методов преобразования данных, направленных на то, чтобы защитить эти данные, сделав их бесполезными для незаконных пользователей. Такие преобразования обеспечивают решение трех главных проблем защиты данных: обеспечение конфиденциальности, целостности и подлинности передаваемых или сохраняемых данных.

Для обеспечения безопасности данных необходимо поддерживать три основные функции:

- защиту конфиденциальности передаваемых или хранимых в памяти данных;
- подтверждение целостности и подлинности данных;
- аутентификацию абонентов при входе в систему и при установлении соединения;

Для реализации указанных функций используются криптографические технологии шифрования, цифровой подписи и аутентификации.

Конфиденциальность обеспечивается с помощью алгоритмов и методов симметричного и асимметричного шифрования, а так же путем взаимной

аутентификации абонентов на основе многоразовых и одноразовых паролей, цифровых сертификатов, смарт-карт и т. п.

Целостность и подлинность передаваемых данных обычно достигается с помощью различных вариантов технологии электронной подписи, основанных на односторонних функциях и асимметричных методах шифрования.

Аутентификация разрешает устанавливать соединения только между легальными пользователями и предотвращает доступ к средствам сети нежелательных лиц. Абонентам, доказавшим свою легальность (аутентичность), предоставляются разрешенные виды сетевого обслуживания.

Обеспечение конфиденциальности, целостности и подлинности передаваемых и сохраняемых данных осуществляется прежде всего правильным использованием криптографических способов и средств защиты информации. Основой большинства криптографических средств защиты информации является шифрование данных.

Под шифром понимают совокупность процедур и правил криптографических преобразований, используемых для зашифровывания и расшифровывания информации по ключу шифрования. Под зашифровыванием информации понимается процесс преобразования открытой информации (исходный текст) в зашифрованный текст (шифртекст). Процесс восстановления исходного текста по криптограмме с использованием ключа шифрования называют расшифровыванием (дешифрованием).

Обобщенная схема криптосистемы шифрования показана на рис. 2.3. Исходный текст передаваемого сообщения (или хранимой информации) M зашифровывается с помощью криптографического преобразования E_{k_1} с получением в результате шифртекста C:

$$C = E_{k_1}(M) \quad (2.2)$$

где k_1 — параметр функции E, называемый ключом шифрования.

Шифртекст C, называемый также криптограммой, содержит исходную информацию M в полном объеме, однако последовательность знаков в нем

внешне представляется случайной и не позволяет восстановить исходную информацию без знания ключа шифрования k_1.

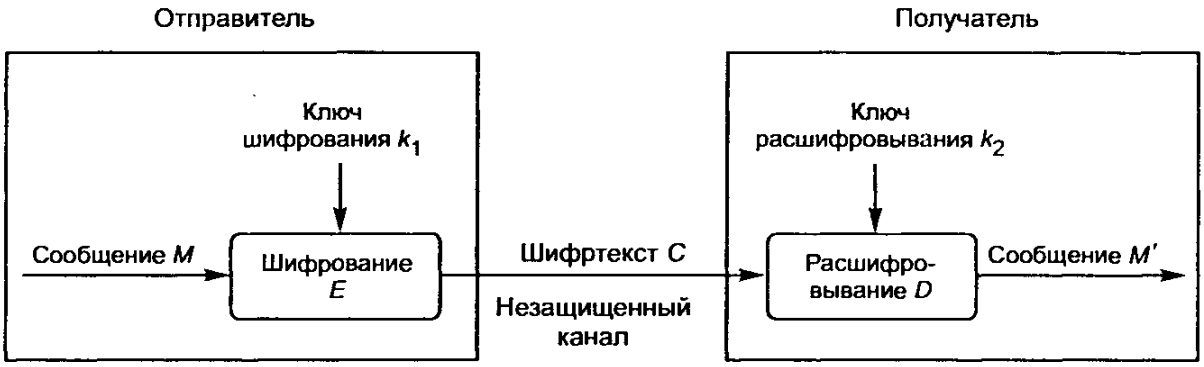

Рис. 2.3. Обобщенная схема криптосистемы шифрования

Ключ шифрования является тем элементом, с помощью которого можно варьировать результат криптографического преобра зования. Данный элемент может принадлежать конкретному пользователю или группе пользователей и являться для них уникальным. Зашифрованная с использованием конкретного ключа информация может быть расшифрована только его владельцем (или владельцами).

Обратное преобразование информации выглядит следующим образом:

(2.4)

Функция D является обратной к функции E и производит расшифровывание шифртекста. Она также имеет дополнительный параметр в виде ключа $к_2$. Ключ расшифровывания $к_2$ должен однозначно соответствовать ключу $к_2$, в этом случае полученное в результате расшифровывания сообщение M' будет эквивалентно M. При отсутствии верного ключа $к_2$ получить исходное сообщение M' = M с помощью функции D невозможно.

Преобразование шифрования может быть симметричным или асимметричным относительно преобразования расшифровывания. Соответственно различают два класса криптосистем:

- симметричные криптосистемы (с единым ключом);
- асимметричные криптосистемы (с двумя ключами).

2.4. ПРОЕКТИРОВАНИЯ СИСТЕМЫ ЗАЩИТЫ ДАННЫХ, ХРАНИМЫХ НА ОПТИЧЕСКИХ НОСИТЕЛЯХ(СЗИХНОН).

На основе сведений приведенных в этой главе, разработаем предварительный дизайн разрабатываемой нами системы. Так как следует защищать информацию от несанкционированного доступа, следует её хранить в зашифрованном виде. Для этого воспользуемся синхронным методом шифрования. Выбор был сделан в пользу синхронного метода шифрования так как он выглядит наиболее привлекательным по сравнению с другими алгоритмами шифрования. Главным критерием при выборе была скорость шифрования.

В СЗИХНОН будут реализованы 2 модели защиты данных:

- Общая модель защиты.
- Конкретизированная модель защиты.

Общая модель представляет собой защиту всей информации хранящуюся на оптическом диске, в момент применения защиты. Существует 2 типа общей зашиты:

- Только чтение.
- Полная защита.

В режиме только для чтения данные хранимые на оптическом носителе будут предоставлены только для чтения. Любые действия направленные на изменения, удаления невозможны.

В режиме полной защиты (рис. 2.7) данные хранимые на оптическом носителе будут скрыты от не авторизованных пользователей. Для того чтобы получить доступ к данным следует ввести пароль который будет введен во время закрытия оптического носителя.

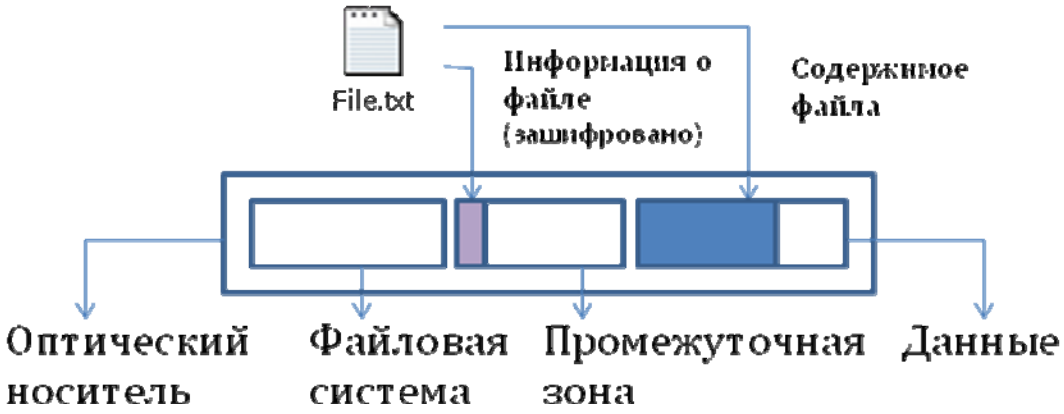

Рисунок 2.7. Абстрактная модель хранения данных в режиме полной защиты.

Конкретизированная защита (рис. 2.8.) представляет собой защиту конкретных файлов/папок. Защита производится посредством шифрования. При этом следует ввести пароль для шифрования. Последующая дешифровка производится посредством копирования файла в жесткий диск, при этом надо ввести пароль, если пароль неверный копирование не производится. В файловой системе доступ к файлу невозможен, вся информация о нем хранится в промежуточной зоне в зашифрованном виде.

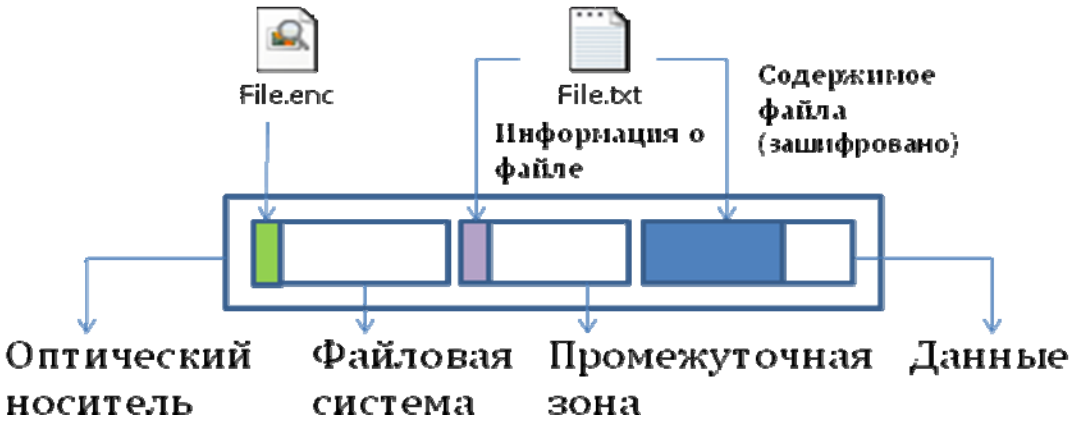

Рисунок 2.8. Абстрактная модель хранения данных в режиме полной защиты.

2.4.1. Технология Промежуточной зоны.

Основной идеей разрабатываемой системы является ввод промежуточной зоны которая будет служить как переключатель между файловой системой и самими данными. В рис. 2.9. показана абстрактная модель хранения данных на оптическом носителе с применением технологии ПЗ. Данные в ПЗ будут шифроваться.

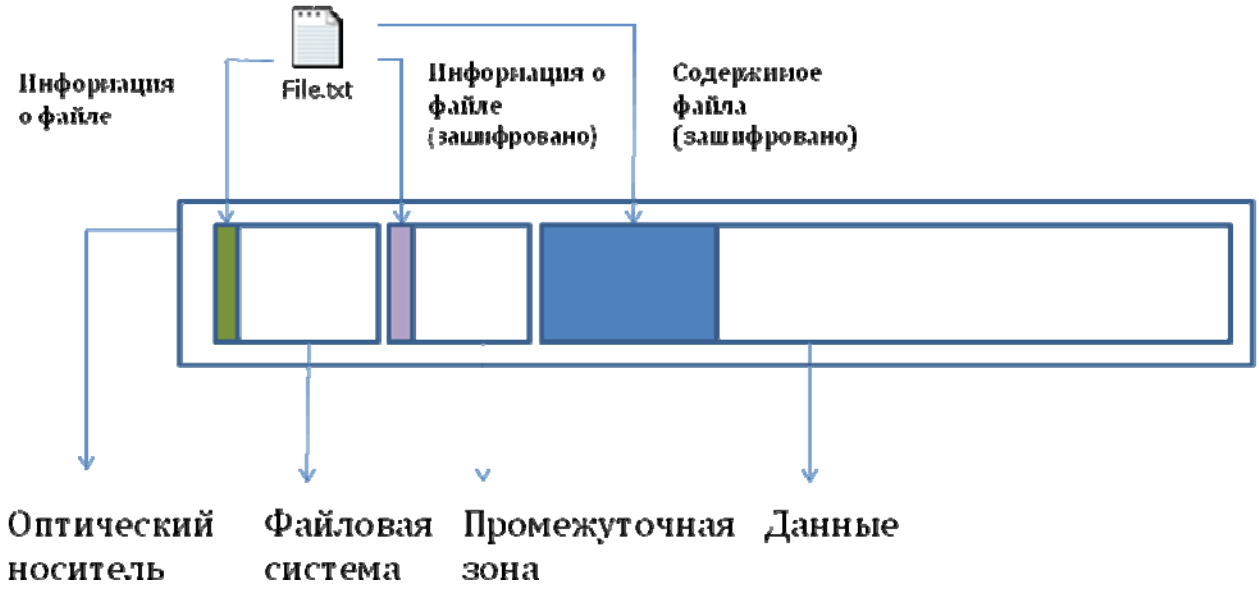

Рисунок 2.9. Абстрактная модель технологии ПЗ.

Выводы.

В данной главе рассмотрены вопросы создания защищенной информационной системы, также сказано о средствах защиты информации. Дано определения понятии криптографии, и его важности в системах защиты информации. Также приведена технология защиты информации на оптических посителях.

3. РАЗРАБОТКА ПРОГРАММНЫХ СРЕДСТВ СИСТЕМЫ ЗАЩИТЫ ДАННЫХ, ХРАНИМЫХ НА ОПТИЧЕСКИХ НОСИТЕЛЯХ.

3.1. РАЗРАБОТКА АРХИТЕКТУРЫ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ.

В соответствии с материалом изложенным в главе 2 архитектура программного средства защиты данных хранимых на оптических носителях будет иметь следующие модули:

- **Модуль файловой системы** - Так как данные будут записываться на оптический носитель следует обеспечить некоторую среду для хранения файлов, обычно для этого служит файловая система. При выборе файловой системы выбор пал на Universal Disc Format (UDF) версии 2.50. UDF 2.50 разработан организацией Optical Storage Technology Association (OSTA). Данная ФС позволяет работать с оптическим носителем как с обычным USB накопителем, также поддерживается фрагментная запись;

- **Модуль работы с устройствами записи** - В данном модуле реализованы функции необходимые для работы с устройствами записи(УЗ). Работа с УЗ производится посредствам интерфейса SCSI (Small Computer System Interface). Команды SCSI посылаются в виде CDB (Command Descriptor Block).

- **Модуль сокрытия данных** - В данном модуле реализованы функции для шифрования и дешифрования данных. В качестве криптографического метода шифрования, был выбран симметричный алгоритм ГОСТ 28147-89. ГОСТ 28147-89 — блочный шифр с 256-битным ключом и 32 циклами преобразования, оперирующий 64-битными блоками. Базовым режимом выбран режим простой замены.

3.2. РАЗРАБОТКА МОДУЛЯ ФОРМИРОВАНИЯ ФАЙЛОВОЙ СИСТЕМЫ.

В качестве языка программирования для данного модуля был выбран язык программирования C++. Основными функциями данного модуля является обеспечения некой среды для хранения файлов в оптическом носителе, т.е. файловая система. Для данной работы была выбрана файловая

система UDF 2.50. В ходе работы были реализованы следующие основные функции:

- FileIdentifierDescriptor;
- ExtendedFileEntry;
- CreateUDFOnDVD;
- ReadUDFInfoFromDVD;

3.2.1. Функция FileIdentifierDescriptor.

Данная функция записывает в буфер File Identifier Descriptor(FID). File Identifier Descriptor хранит в себе информацию о файле (табл. 3.1) . Далее буфер записывается на оптический носитель посредствам функций реализованных в модуле работы с устройствами записи.

Табл. 3.1. Структура File Identifier Descriptor

Позиция Бита	Длина	Название	Содержание
0	16	Идентификатор	Tag[8]
16	2	Номер версии файла	Uint16[8]
18	1	Характеристики файла	Uint8[8]
19	1	Длина идентификатора файла	Uint8[8]
20	16	ICB	Long_ad[8]
36	2	Длина поля для использования разработчиком	Uint16[8]
38	L_IU	Поля для использования разработчиком	Bytes[8]
38 + L_IU	L_FI	Идентификатор файла	d-characters[8]
38+ L_IU + L_FI	*	Заполнение	Bytes[8]

3.2.1.1. Идентификатор.

Данное поле служит для идентификации дескриптора. В нем хранится тип дескриптора, длина, контрольная сумма и т.д.

3.2.1.2. Номер версии файла.

Данное поле содержит номер версии файла который описан данным File Identifier Descriptor. Значения которые может принимать данное поле лежат в промежутке от 1 до 32768.

3.2.1.3. Характеристики файла.

Данное поле будет рассматриваться как последовательность битов, где каждый бит имеет свое значение. К характеристикам файла относятся скрытность, удаленность, системность и т.д.

3.2.1.4. Длина идентификатора файла.

Длина идентификатора файла. иметь тип Uint16[9]. Должен быть кратным 4.

3.2.1.5. ICB

Данное поле содержит адрес описывающий данный файл т.е. где записан Extended File Entry Descriptor. Если файл удален, данное поле заполняется нулями.

3.2.1.6. Длина поля для использования разработчиком.

Длина поля предназначенная для использования разработчиком. Будет иметь тип Uint16[9]. Должен быть кратным 4.

3.2.1.7. Поля для использования разработчиком.

Будет записан идентификатор разработчика. Не будет иметь значение ноль.

3.2.1.8. Идентификатор файла.

Под идентификатором файла понимается его название. Идентификатор может иметь разный формат т.е. иметь ASCII кодировку или Unicode кодировку.

3.2.1.9. Заполнение.

Остающиеся байты будут заполнены нулями.

3.2.2. Функция ExtededFileEntry.

Данная функция записывает в буфер Extended File Entry Descriptor(EFE). Extended File Entry хранит расширенную информацию о файле. Функция реализована как рекурсивная т.е. функция будет вызываться для каждой папки, если в данной папке есть папка, вызывается для нее и т.д. Также для каждого файла вызывается функция File Identifier Descriptor. В рисунке 3.3. показана как для папки Folder вызывается данная функция.

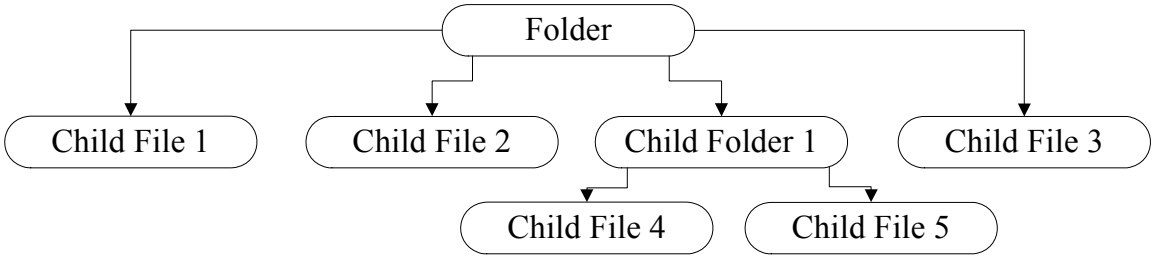

Рисунок 3.2. Структура папки Folder.

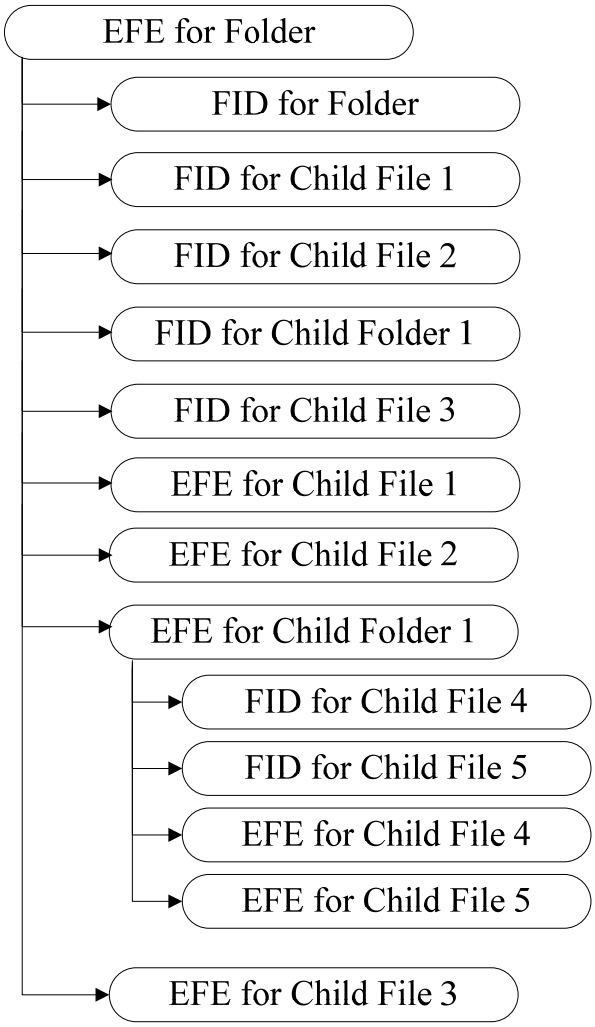

Рисунок 3.3. Последовательность вызовов функций.

3.2.3. Функция CreateUDFOnDVD.

Данная функция служит для создания файловой системы на оптическом носителе, этот процесс также называется финализацией оптического носителя. Информация о файлах которые следует защитить записывается в промежуточную зону с применением функции шифрования, информация об обычных файлах записывается в открытую часть файловой системы. Информация о защищенных файлах также записывается в открытую

часть но уже с изменениями, после которых она становится бесполезной. Алгоритм выполнения имеет следующую последовательность:

1. Расчет требуемого место для файловой системы.
2. Запись информацию о конфиденциальных данных в промежуточную зону, закрытая часть файловой системы.
3. Изменить информацию о файлах записанных в промежуточную зону.
4. Записываются стандартные дескрипторы[10].
5. Запись открытую часть файловой системы.

3.2.3.1. Расчет требуемого место для файловой системы.

В данной части функции производится расчет место для файловой системы. В основном размер файловой системы зависит от количество файлов, также зависит от длины названия файлов. Размер файловой системы измеряется в секторах[8].

3.2.3.2. Запись стандартных дескрипторов.

Записываются дескрипторы указанные в стандарте файловой системы. Существует 2 последовательности дескрипторов: основная и резервная. Резервная служит как страховка, данные считываются с нее только в тех случаях, когда не удалось считать их с основного. Запись резервной последовательности является опциональной. Основным критерием для того чтобы не записывать резервную последовательность является достижения высокой скорости записи файловой системы.

3.2.3.3. Запись информации о файлах пользователя.

Записываются дескрипторы пользовательских файлов. Вызывается Extended File Entry для корневой папки, который далее вызывается для детей и т.д.

3.2.3.4. Виды финализации.

Существует 2 вида финализации:

- Открытый;
- Закрытый;
- Только чтение;

3.2.3.4.1. Открытый вид финализации.

Оптический носитель финализируются обычным образом, все файлы видны и открыты для изменения.

3.2.3.4.2. Закрытый вид финализации.

Оптический носитель финализируются, таким образом что он выглядит пустым для неавторизованного пользователя. Для доступа к данным надо иметь пароль.

3.2.3.4.3. Только чтение.

Оптический носитель финализируются обычным образом, но изменение содержимого запрещяется.

3.2.4. Функция ReadUDFInfoFromDVD.

Данная функция считывает данные из файловой системы для последующего изменения, добавления или удаления файлов. В первую очередь определяется тип файловой системы, если данная файловая система поддерживается, считывается файловая система и формируется дерево содержащее все текущие файлы хранимые на оптическом носителе. В создании дерево использовались контейнеры из стандартной библиотеки шаблонов(STL) входящую в стандартную библиотеку C++.

Файловая система считается поддерживаемой в случиях:

- Данные записаны на оптический носитель, но финализирован не произведена.
- Данные записаны на оптический носитель, процесс финализации произведен.
- Данные записаны на оптический носитель, процесс финализации произведен, добавлены изменения файловой системе другим ПО.

3.3. РАЗРАБОТКА МОДУЛЯ ПОДДЕРЖКИ ОПТИЧЕСКИХ НОСИТЕЛЕЙ.

Данный модуль предусмотрен для работы с устройствами записи на оптическом носителе. Основными функциями данного модуля являются следующие функции:

- WriteDataToDVD;
- ReadDataFromDVD;
- CheckMediaStatus;

3.3.1. Функция WriteDataToDVD.

Записывает данные на оптический носитель. Данные записываются по 32 сектора. Принимает полный путь к файлу, который следует скопировать, функция открывает данный файл как бинарный и копирует его по битам. Функция отправляет CDB команду WRITE(10)[11] устройству. Данная функция

поддерживает фрагментную запись. В табл. 3.4. показана структура команды WRITE(10).

Таблица 3.4. Структура команды WRITE(10).

Номер байта	Назначение
0	Код операции
1	Зарезервирована
2	Адрес блока для записи
3	
4	
5	
6	Зарезервирована
7	Размер передаваемых данных
8	
9	Пользовательская команда
10	Не используется
11	

3.3.2. Функция ReadDataFromDVD.

Данная функция считывает данные с оптического носителя и записывает их в буфер переданный ей в качестве аргумента. Для этого отправляется CDB команда READ(10)[11]. В отличии от WRITE(10) в READ(10) возможно изменять размер передаваемых данных. В табл. 3.5. показана структура команды READ(10).

Таблица 3.5. Структура команды READ (10).

Номер байта	Назначение
0	Код операции
1	Зарезервирована
2	Адрес блока для чтения
3	
4	
5	
6	Зарезервирована
7	Размер данных которые следует считать
8	
9	Пользовательская команда
10	Не используется
11	

3.4. РАЗРАБОТКА МОДУЛЯ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ.

Целью создания данного модуля является сокрытие данных от неавторизованного доступа. В данном модуле реализованы функции для шифрования и дешифрования данных. Применен симметричный метод шифрования ГОСТ 28147-89. Основными функциями данного модуля являются:

- EncryptBuffer;
- DecryptBuffer;

3.4.1. Функция EncryptBuffer.

Данная функция используется для шифрования буфера переданного ей в качестве аргумента. Применение данной функции повышает время работы разрабатываемого ПО, но в конечном итоге это компенсируется безопасностью которая она предоставляет. Но все-таки желательно применять данную функцию только при записи конфиденциальной информации.

3.4.2. Функция DecryptBuffer.

Данная функция используется для шифрования буфера переданного ей в качестве аргумента. Также требуется ключ для дешифрования. Если пароль неверный возбуждается соответствующее исключения.

3.4.3. Как хранится пароль?

Так как хранения пароля на оптическом носителе не является безопасным, он хранится в неявном виде, т.е. определенный текст шифруется с помощью пользовательского пароля, и этот зашифрованный текст записывается на оптический носитель.

3.4.4. Как производится проверка пароля?

При дешифровки данных следует ввести пароль, который будет применен для дешифровки данных. Применяя этот ключ дешифруется текст который записан с шифрованием определенного текста. В случае если исходной текст который был зашифрован и текст после дешифровки идентичны, пароль является верным.

3.5. РАЗРАБОТКА ПОЛЬЗОВАТЕЛЬСКОГО ИНТЕРФЕЙСА.

Пользовательский интерфейс разработан на языке C++ с применением MFC. Основным критерием при разработке была простота использования и понятность всех функций как опытному так и начинающему пользователю персональным компьютером. Интерфейс (рис. 3.6.) состоит из главного окна в котором расположено окно для показа файлов и кнопки для управления выполняемыми функциями.

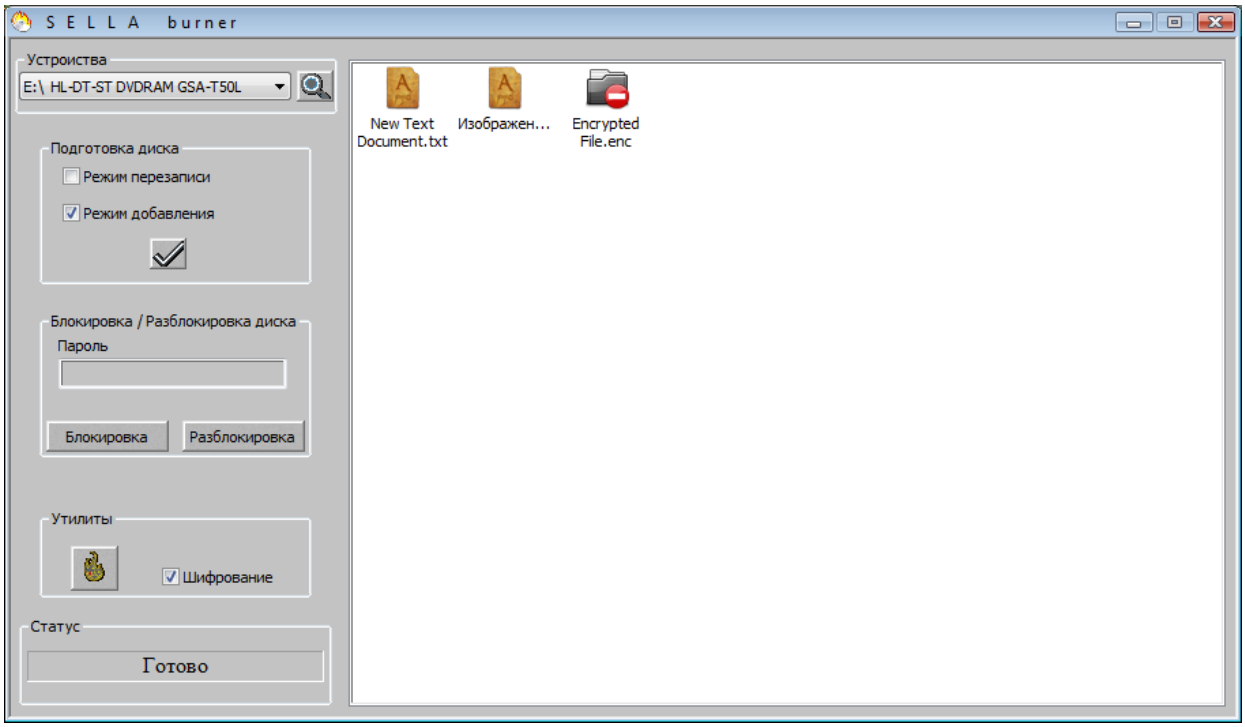

Рисунок 3.6. Вид пользовательского интерфейса

3.5.1. Процесс записи файла с шифрованием.

Для записи файла/папки с шифрованием следует выбрать в утилитах меню «Шифрование» (рис. 3.7), после чего следует выбрать файл/папку и переместить его в окно программы.

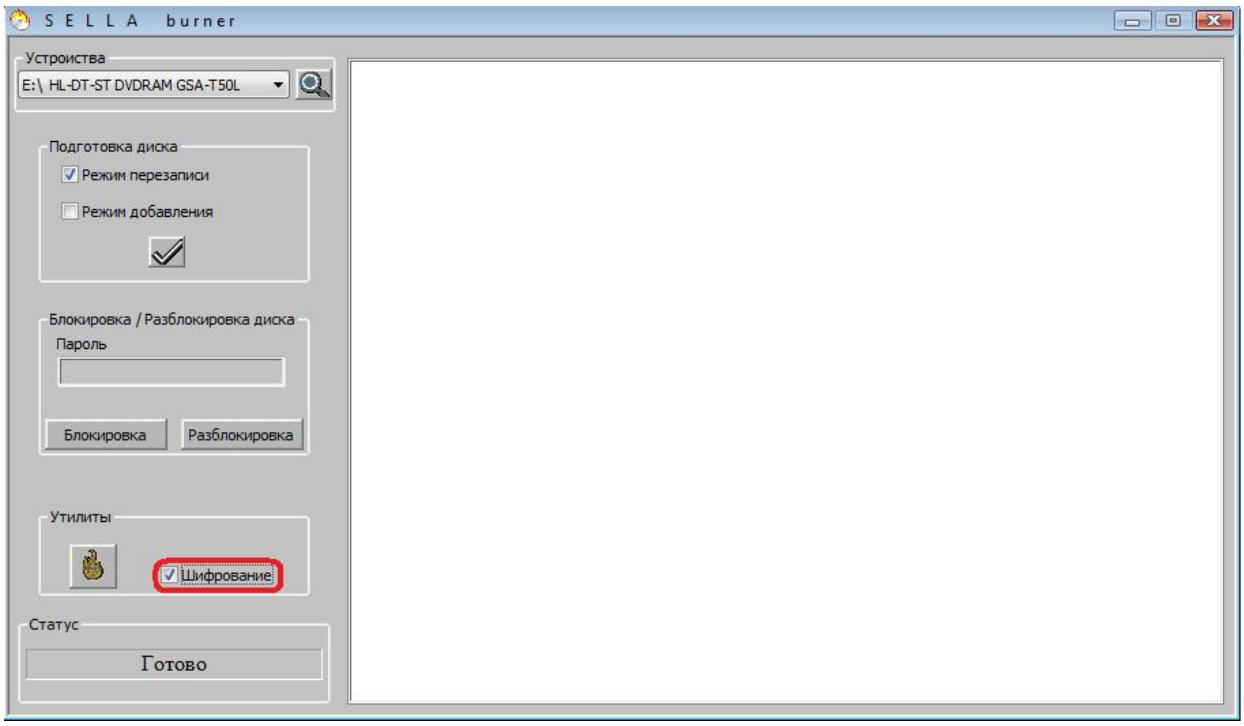

Рисунок 3.7. Выбор меню шифрования.

При этом должна быть выбрана устройства посредствам которого будет производится запись (рис. 3.8) на оптический носитель.

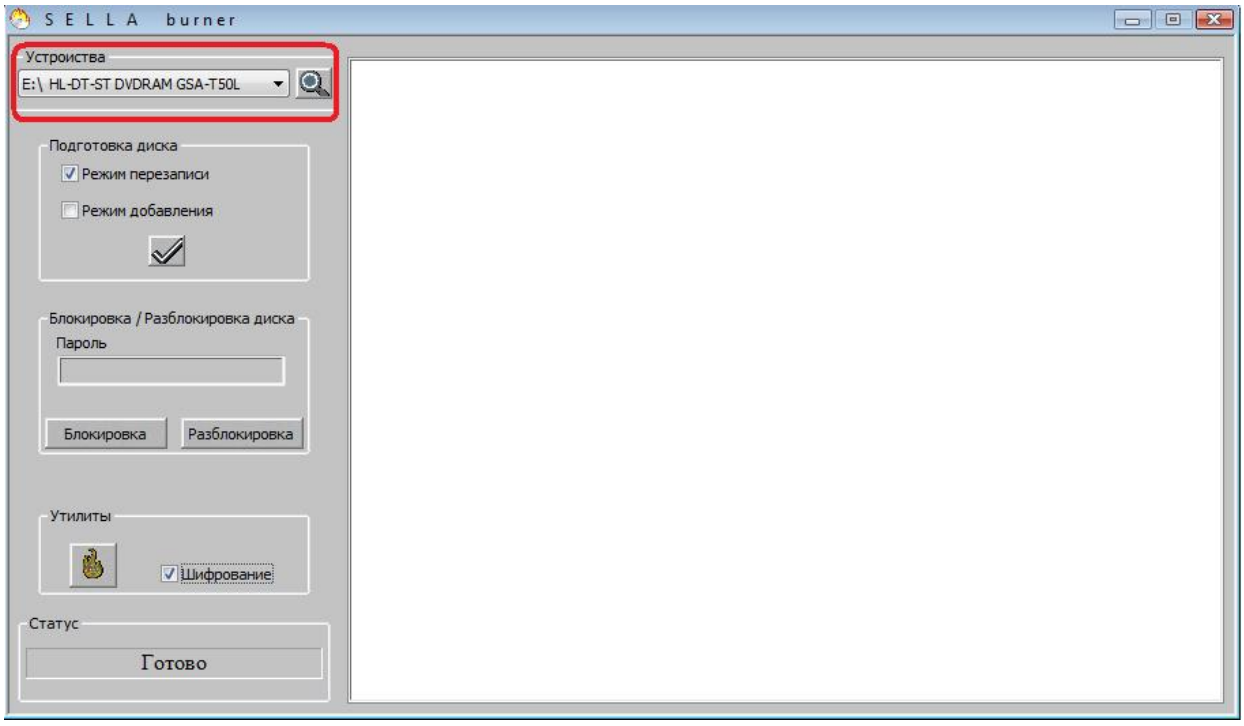

Рисунок 3.8. Выбор устройства записи

Также следует выбрать режим записи (рис. 3.9). После того как данные записаны, следует финализировать оптический носитель.

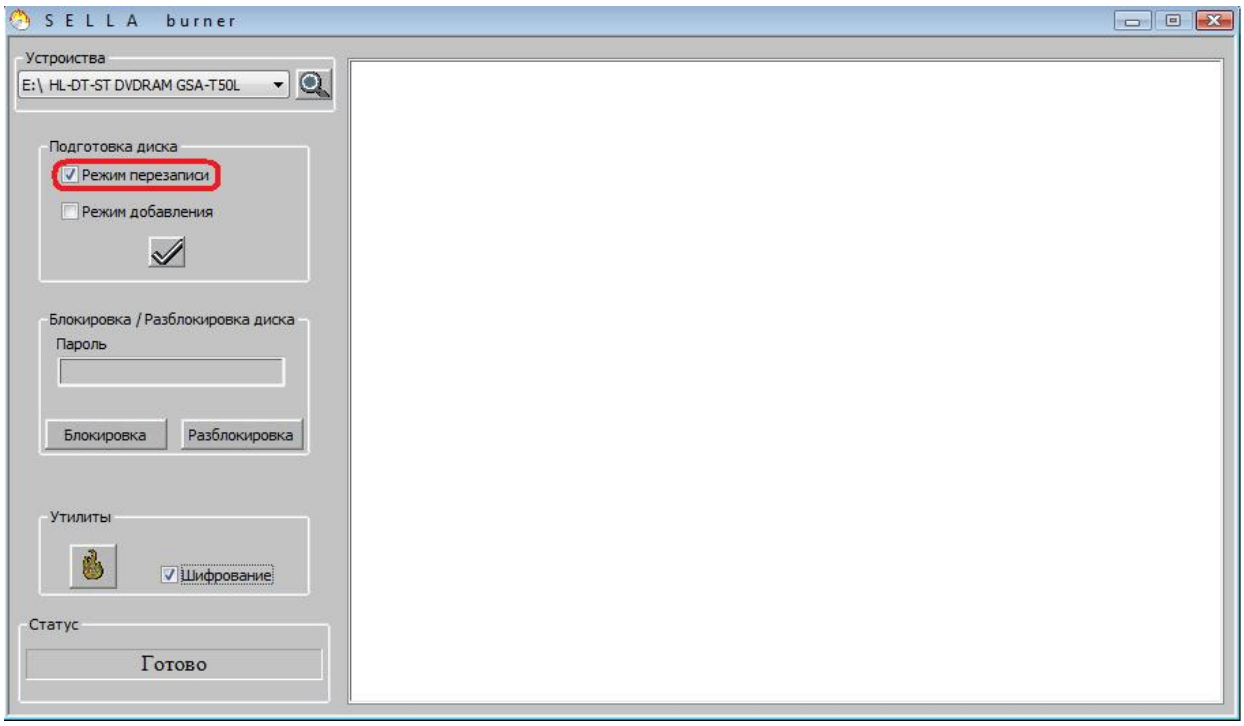

Рисунок 3.9. Выбор режима записи.

Существует 2 типа финализации: открытий и закрытый (рис. 3.10). При открытом режиме шифрования дикс просто финализируется и данные хранимые на диске доступны каждому. При закрытой финализации, следует ввести пароль для диска, доступ к данным на диске можно получить только при наличии данного пароля.

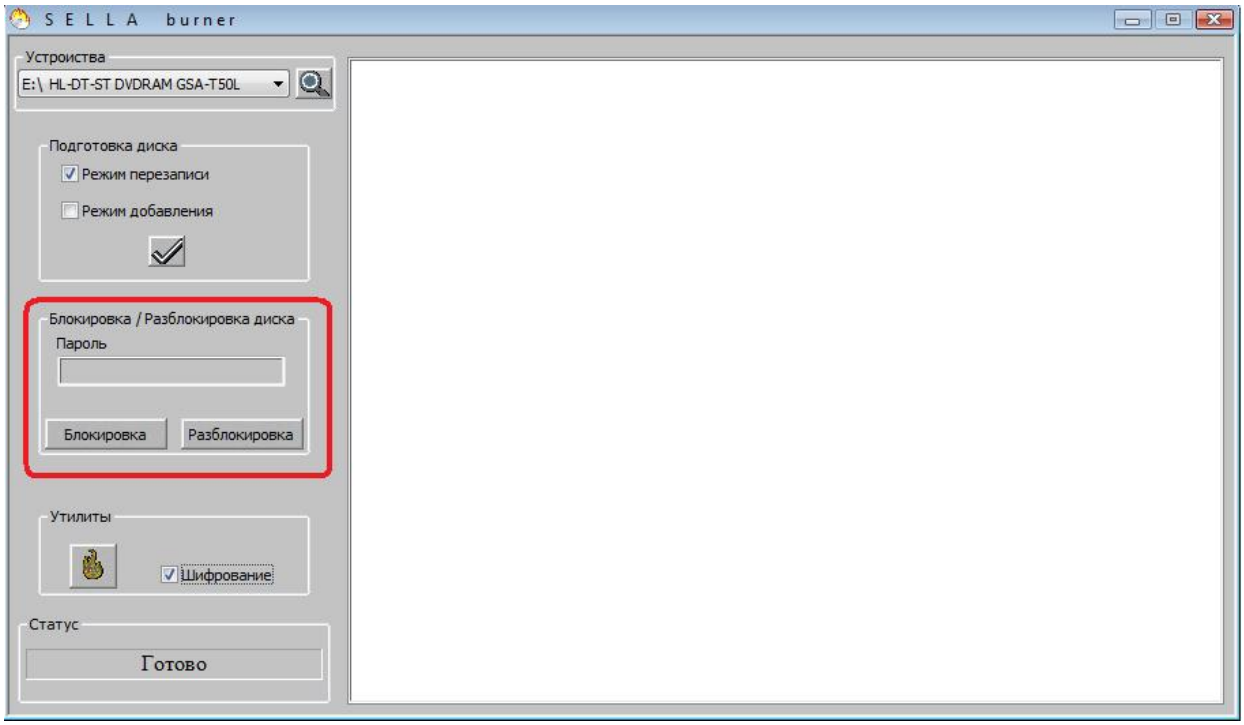

Рисунок 3.10. Выбор типа финализации.

Выводы.

Учитывая все сказанное разработана технология и алгоритм обеспечения безопасности данных на оптических носителях. На вышесказанного разработана программное средство для защиты информации хранимой на оптическом носителе.

4. БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ

4.1. ОРГАНИЗАЦИЯ РАБОЧЕГО МЕСТО ОСНАЩЕННОГО КОМПЬЮТЕРА.

Отправной точкой во всех рассуждениях должны быть два положения:

- удобство выполнения специфической работы конструктора (выполнение и проверка большого количества крупноформатных документов);
- соблюдение всех действующих в настоящий момент норм и правил в части организации рабочего места, оснащенного компьютером (санитарных норм, ГОСТов, пожарных норм и т.д.)

Предлагается использовать комплексный подход к решению данной задачи, т.е. решать задачу размещения неопределенного количества рабочих мест в помещении стандартных размеров. В рис.4.1 представлена модель планировки которой мы воспользуемся.

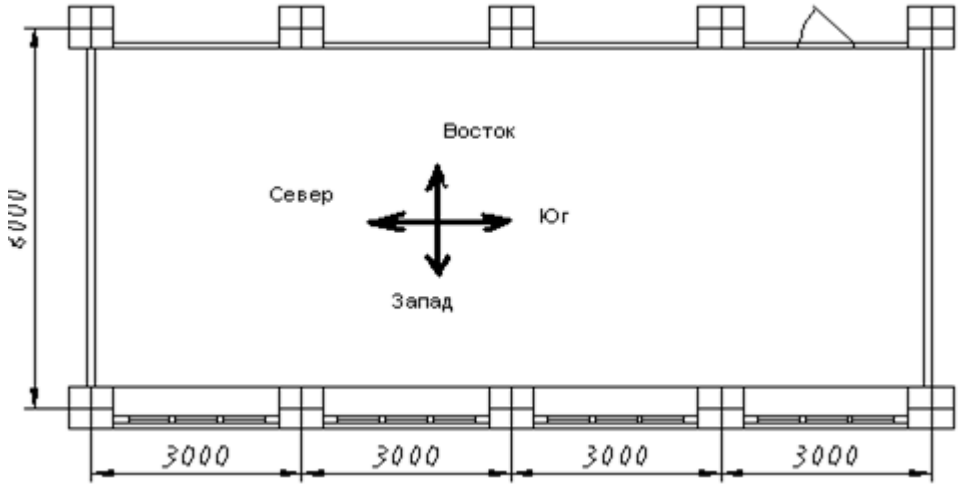

Рисунок 4.1. Модель расстановки компьютеров

Ориентировочная площадь помещения - 62 м2, высота потолков - 3м. И следовательно объем помещения 186м3.

В этом помещении могут быть расположены не более 9 рабочих мест, оснащенных компьютерами.

В нашем случае мы планируем разместить в этом помещении 7 рабочих мест. У входа планируется разместить одно рабочее место руководителя и далее по два рабочих места на одно окно.

Размещение и организация в помещении нескольких рабочих мест с ПЭВМ целесообразности размещения мониторов по примеру помещения показанного в рис. 4.2.

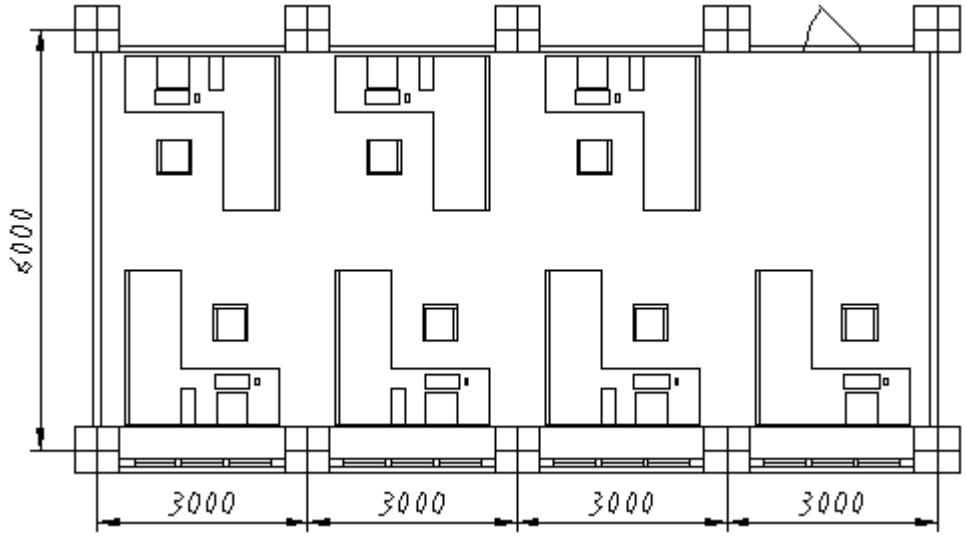

Рисунок 4.2. Пример размещения мониторов.

По размещению мониторов относительно световых проемов. Учитывая, что мы не имеем возможности развернуть наше условное возмещение и световые проемы ориентированы на Запад, мы вынуждены предусмотреть установку жалюзей. Рабочие места разделяем перегородками, устанавливаемыми на краях сторов.

4.2. ОПРЕДЕЛЕНИЕ КАТЕГОРИЙ ПОЖАРНОЙ ОПАСНОСТИ ПРОИЗВОДСТВ И КЛАССА ПОЖАРА-ВЗРЫВООПАСНОСТИ ПОМЕЩЕНИЙ.

В соответствии с общесоюзными нормами технологического проектирования все производственные здания и помещения по взрывопожарной опасности подразделяются на категории А, Б, В1-В4, Г и Д (табл. 1).

Таблица 4.3. Категории помещений по взрывопожарной и пожарной опасности

Категория помещен.	Характеристика веществ и материалов, находящихся (образующихся) в помещении
А взрыво-пожаро-опасная	Горючие газы, легковоспламеняющиеся жидкости с температурой вспышки не более 28°С в таком количестве, что могут образовать взрывоопасные парогазовоздушные смеси, при воспламенении которых развивается расчетное избыточное давление взрыва в помещении, превышающее 5 кПа. Вещества и материалы, способные взрываться и гореть при взаимодействии с водой, кислородом воздуха или друг с другом в таком количестве, что расчетное избыточное давление взрыва в помещении превышает 5 кПа.
Б взрывопожароопасная	Горючие пыли или волокна, легковоспламеняющиеся жидкости с температурой вспышки более 28°С в таком количестве, что могут образовывать взрывоопасные пылевоздушные или паровоздушные смеси, при воспламенении которых развивается расчетное избыточное давление взрыва в помещении, превышающее 5 кПа.
В1–В4 пожаро-опасная	Горючие и трудно горючие жидкости, твердые горючие и трудно горючие вещества и материалы, способные при взаимодействии с водой, кислородом воздуха или друг с другом только гореть при условии, что помещения, в которых они имеются в наличии или применяются, не относятся к категориям А или Б.
Г	Негорючие вещества и материалы в горячем, раскаленном или расплавленном состоянии, процесс обработки которых сопровождается выделением лучистого тепла, искр и пламени; горючие газы, жидкости и твердые вещества, которые сжигаются или утилизируются в качестве топлива.
Д	Негорючие вещества и материалы в холодном состоянии.

Категории В1–В4 определяются величиной удельной пожарной нагрузки g в МДж/м$^{2:}$

$g=Q/S,$

где Q – пожарная нагрузка, МДж; S – площадь размещения пожарной

нагрузки, $м^2$ (но не менее $10м^2$).

Пожарная нагрузка $Q = \sum_{i=1}^{n} G_i \cdot Q_н^p$,

где G_i – количество i-го материала пожарной нагрузки, кг;

Q^p_{ni} - низшая теплота сгорания i-го материала пожарной нагрузки, МДж/кг.

Для категории В1 $g>2200$МДж/$м^2$; В2:$1401<g<2200$; В3:$181<g<1400$; В4;$1<g<180$.

Категория зданий определяется путем последовательной проверки принадлежности помещения к категориям от высшей (А) к низшей (Д). Категорию зданий определяют согласно следующим рекомендациям:

Здание относится к категории А, если в нем суммарная площадь помещения категории А превышает 5% площади всех помещений или 200 $м^2$. Допускается не относить здание к категории А, если суммарная площадь помещений категории А зданий не превышает 25% суммарной площади всех размещенных в нем помещений (но не более 1000 $м^2$), если эти помещения оборудуются установками автоматического пожаротушения.

Здание относится к категории Б, если одновременно выполнены два условия:

а) здание не относится к категории А;

б) суммарная площадь помещений категории А и Б превышает 5% суммарной площади всех помещений или 200 $м^2$.

Допускается не относить здание к категории Б, если суммарная площадь помещений категории А и Б в здании не превышает 25% суммарной площади всех размещенных в нем помещений (но не более 1000 $м^2$), и эти помещения оборудуются установками автоматического пожаротушения.

Здание относится к категории В, если одновременно выполнены два условия:

а) здание не относится к категории А или Б;

б) суммарная площадь помещений категории А, Б, В превышает 5% (10%, если в зданиях отсутствуют помещения категории А и Б) суммарной площади всех помещений.

Допускается не относить здание к категории В, если суммарная площадь помещений категории А, Б, В не превышает 25% суммарной площади всех размещенных в нем помещений (но не более 3500 $м^2$) и эти помещения оборудуются установками автоматического пожаротушения.

Здание относится к категории Г, если одновременно выполняются два требования:

а) здание не относится к категории А, Б, В;

б) суммарная площадь помещений категории А, Б, В и Г превышает 5% суммарной площади всех помещений.

Допускается не относить здание к категории Г, если суммарная площадь помещений категории А, Б, В и Г в здании не превышает 25% суммарной площади всех размещенных в нем помещений (но не более 5000м^2) и помещения категории А, Б, В оборудуются установками автоматического пожаротушения.

Здание относится к категории Д, если оно не относится к категориям А, Б, В и Г.

На объектах разных категорий возникновение отдельных пожаров будет зависеть от степени огнестойкости зданий, а образование сплошных пожаров – от плотности астройки.

Под огнестойкостью понимают способность строительных конструкций сопротивляться возникновению высокой температуры в условиях пожара и выполнять при этом свои обычные эксплуатационные функции.

Предел огнестойкости

время (в минутах) наступления одного или последовательно нескольких нормируемых для данной конструкции признаков предельных состояний:

Потеря несущей способности

обрушение конструкции или возникновение предельных деформаций, обозначается индексом R.

Потеря целостности

проникновение продуктов сгорания за изолирующую преграду, обозначается индексом Е.

Потеря теплоизолирующей способности

повышение температуры на не обогреваемой поверхности конструкции в среднем более чем на 140° или в любой точке поверхности более чем на 180° и обозначается индексом J.

При этом предел огнестойкости окон устанавливается только по времени потери целостности (Е).

4.3. ОПРЕДЕЛЕНИЕ ПРЕДЕЛОВ ОГНЕСТОЙКОЕ СТРОИТЕЛЬНЫХ КОНСТРУКЦИЙ ЗДАНИЙ ОСНОВАНИИ ТРЕБОВАНИЙ НОРМ И ИСХОДЯ ИЗ РАСЧЕТНОЙ ДЛИТЕЛЬНОСТИ ПОЖАРА.

Здания и пожарные отсеки (части здания, выделенные пожарными стенами) согласно СН и П 21-01-97, подразделяются на I, II, III, IV и V степени огнестойкости (см. табл. 2).

Таблица 4.4. Степени огнестойкости зданий.

Степень огнестойкости здания	Несущие элементы здания	Пределы огнестойкости строительных конструкций не менее					
		Наружные несущие стены	Перекрытия междуэтажные	Элементы бесчердачных покрытий		Лестничные клетки	
				настилы			
фермы, балки, прогоны	внутренние стены	марши и площадки лестниц					
I	R 120	E 30	REI 60	RE 30	30	EI 120	60
II	R 90	E 15	REI 45	RE 15	15	EI 90	60
III	R 45	E 15	REI 45	RE 15	15	EI 60	45
IV	R 15	E 15	REI 15	RE 15	15	EI 45	15
V	не нормируется						

К несущим элементам здания относятся конструкции, обеспечивающие его общую устойчивость и герметическую неизменяемость при пожаре - несущие стены, рамы, колонны, балки, фермы, арки и т.п.

Пределы огнестойкости заполнения проемов (дверей, ворот, окон) не нормируются.

Если минимальный предел огнестойкости указан R 15 (RE 15, REI 15) допускается применять незащищенные стальные конструкции, независимо от их фактического предела огнестойкости, но не менее R 8.

Строительные материалы согласно СН и П 21.01-97 подразделяются на две группы: негорючие (НГ) и горючие (Г) (табл. 4.5).

Негорючие материалы под действием огня или высокой температуры не воспламеняются, не тлеют и не обугливаются (минеральные).

Горючий материал под воздействием огня или высокой температуры воспламеняется, обугливается или тлеет и продолжает гореть, тлеть или обугливаться после удаления источника зажигания (органические).

Горючие строительные материалы подразделяются на четыре группы:

Г1 (слабогорючие);

Г2 (умеренногорючие);

Г3 (нормальногорючие);

Г4 (сильногорючие).

Таблица 4.5. Характеристика групп горючести строительных материалов

Группа горючести материалов	Параметры горючести			
	Температура дымовых газов, t, °С	Степень повреждения по длине, S_i, %	Степень повреждения по массе, $S_т$,%	Продолжительность самостоятельного горения, $Т_{сг}$
Г1	< 135	< 65	< 20	0
Г2	< 235	< 85	< 50	< 30
Г3	< 450	> 85	< 50	< 300
Г4	> 450	> 85	> 50	> 300
НГ	Прирост температуры в печи за счет горения образца не превысил 50°С, а продолжительность устойчивого пламенного горения не более 10 мин			

Определение горючести строительных материалов проводят экспериментально.

Для отделочных материалов громе горючести вводится понятие величины критической поверхностной плотности теплового потока (КППТП), при которой возникает устойчивое пламенное горение материала. В зависимости от значения КППТП все материалы подразделяются на три группы воспламеняемости:

В1 (трудновоспламеняемые) – КППТП равна или больше 35 кВТ/м²

В2 (умеренновоспламеняемые) – КППТН > 20, но < 35 кВТ/ м²

В3 (легковоспламеняемые) КППТН <20 кВТ/ м²

Горючие строительные материалы по распространению пламени по поверхности подразделяются на четыре группы:

РП1 (нераспространяющие);

РП2 (слабораспространяющие);

РП3 (умеренно распростораняющие);

РП4 (сильнораспространяющие).

Горючие строительные материалы по дымообразующей способности подразделяются на три группы:

Д1 (с малой дымообразующей способностью);

Д2 (с умеренной дымообразующей способностью);

Д3 (с высокой дымообразующей способностью).

Горючие строительные материалы по токсичности продуктов горения, подразделяются на четыре группы:

Т1 (малоопасные);

Т2 (умеренно опасные);

Т3 (высокоопасные);

Т4 (чрезвычайно опасные).

По пожароопасности строительные конструкции подразделяются на четыре класса:

К0 (непожароопасные);

К1 (малопожароопасные);

К2 (умеренно пожароопасные);

К3 (пожароопасные).

Класс пожароопасности определяется по табл. 4.6.

Таблица 4.6. Класс пожароопасности.

Класс пожароопасности конструкции	Допустимый размер повреждения конструкции, см		Наличие		Дополнительные характеристики поврежденного материала		
					Группа		
	вертикальные	горизонтальные	теплового эффекта	горения	горючести	воспламеняемости	дымообразующей способности
	К0	0		Д.	Д.	–	–

	Допустимый размер повреждения конструкции, см		Наличие		Дополнительные характеристики поврежденного материала		
					Группа		
	вертикальные	горизонтальные	теплового эффекта	горения	горючести	воспламеняемости	дымообразующей способности
К1	До 40	До 25	Д.Р.	Д.Р.	Р.2	Н.Р. В2	Н.Р. Д2
К2	>40, но до 80 “	>25, но до 50 “	Д.Р.	Д.Д.	Р.3	Н.Р. В3	Н.Р. Д2
К3				Р.			

Примечание: Н.Д. – не допускается; Н.Р. – не регламентируется.

Здания и пожарные отсеки по конструктивной пожарной опасности подразделяются на классы, согласно табл. 4.7.

Таблица 4.7. Классы конструктивной пожарной опасности здания

Класс конструктивной пожарной опасности здания	Класс пожарной опасности строительных конструкций				
	Несущие элементы (колонны, фермы и др.)	Стены наружные с внешней стороны	Стены, перегородки, перекрытия и бесчердачные покрытия	Стены лестничных клеток и противопожарные преграды	Марши и площадки лестниц лестничных клеток
С0	К0	К0	К0	К0	К0
С1	К1	К2	К1	К0	К0
С2	К3	К3	К2	К1	К1
С3	Не нормируется			К1	К3

Здания по функциональной пожарной опасности подразделяются на классы в зависимости от способа их использования и безопасности людей в

случае возникновения пожара.

Ф1. Для постоянного и временного проживания.

Ф2. Зрелищные и культурно-просветительные учреждения:

Ф2.1 –. театры, кинотеатры, библиотеки;

Ф2.2 – музеи, выставки, танцевальные залы;

Ф2.3 и Ф2.4 – учреждения соответственно Ф2.1 и Ф2.2, расположенные на открытом воздухе.

Ф3. Предприятия по обслуживанию населения:

Ф3.1 -торговли;

Ф3.2 - общественного питания;

Ф3.3 - вокзалы;

Ф3.4 - поликлиники и амбулатории;

Ф3.5 - помещения посетителе предприятий бытового обслуживания;

Ф3.6 - физкультурно-оздоровительные комплексы.

Ф4. Учебные заведения, научные и проектные организации, учреждения управления:

Ф4.1 - школы, внешкольные учебные заведения;

Ф4.2 - Вузы;

Ф4.3 - органы управления, проектно-конструкторские организации,

Ф4.4 - пожарные депо.

Ф5. Производственные и складские здания:

Ф5.1 – производственные и лабораторные помещения

Ф5.2 – складские здания и помещения, стоянки автомобилей без технического обслуживания, книгохранилища, архивы;

Ф5.3 – сельскохозяйственные здания.

Производственные и складские помещения, лаборатории и мастерские в зданиях классов Ф1, Ф2, Ф3, Ф4, относятся к классу Ф5.

По масштабам и интенсивности пожары можно подразделить на:

отдельный пожар, возникающий в отдельном здании (сооружении) или в небольшой изолированной группе зданий;

сплошной пожар, характеризующийся одновременно интенсивным горением преобладающего числа зданий и сооружений на определенном участке застройки (более 50%);

огневой шторм, особая форма распространяющегося сплошного пожара,

образующаяся в условиях восходящего потока нагретых продуктов сгорания и быстрого поступления в сторону центра огневого шторма значительного количества свежего воздуха (ветер со скоростью 50 км/ч);

массовый пожар, образующийся при наличии в местности совокупности отдельных сплошных пожаров.

Распространение пожаров и превращение их в сплошные определяется плотностью застройки территории объекта. О влиянии плотности размещения можно судить по ориентировочным данным, приведенным ниже:

Расстояние между зданиями, м			0	5	0	0	0	0	0	0
Вероятность распространения пожара, %	00	7	6	7	7	3				

Быстрое распространение пожара возможно при следующих сочетаниях степени огнестойкости и плотности застройки: для зданий I и II степени огнестойкости плотность застройки должна быть не более 30%; для зданий III степени – 20%; для зданий IV и V степени - не более 10%.

Влияние трех факторов (плотности застройки, степени огнестойкости и скорости ветра) на скорость распространения огня можно проследить на следующих цифрах:

при скорости ветра до 5 м/с в зданиях I и II степени огнестойкости скорость распространения пожара составляет примерно 120 м/ч; в зданиях IV степени огнестойкости – примерно 300 м/ч, а в случае сгораемой кровли до 900 м/ч;

при скоростях ветра до 15 м/с в зданиях I и II степени огнестойкости скорость распространения пожара достигает 360 м/с.

ЗАКЛЮЧЕНИЕ.

Данная выпускная квалификационная работа посвящена вопросам защиты информации хранимой на оптическом носителе В соответствии с целью выпускной квалификационной работы разработана программное средство для защиты информации хранимой на оптическом носителе.

Основными теоретическими и практическими результатами выпускной квалификационной работы являются:

1. Выполнен анализ современных угроз информации и информационным системам.
2. Рассмотрены методы и средства защиты информации.
3. Изучены материалы по созданию безопасной информационной системы, требования к безопасным информационным системам.
4. Разработана технология и алгоритмы защиты информации хранимой на оптическом носителе.
5. Разработана программное средство защиты информации хранимой на оптическом носителе.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Каримов И.А. Мировой финансово-экономический кризис, пути и меры по его преодолению в условиях Узбекистана.
2. Белов Е.Б, Лось В.П, Мещеряков Р.В, Шелупанов А.А Основы информационной безопасности. –М.: Горячая линия – Телеком», 2006. – с. 544
3. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. - М.:Горячая линия – Телеком, 2004. – с. 280.
4. Мельников В.П. Информационная безопасность и защита информации. – М.:Академия, 2008, 127 с.
5. Скотт Бармен. Разработка правил информационной безопасности. – М.: Вильямс, 2002, 207 с.
6. Цирлов В.Л. Основы информационной безопасности автоматизированных систем. –М.: Феникс, 2008, с. 173.
7. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей. М.: Форум 2008 – с. 401
8. Ярочкин В.И. Информационная безопасность –М.: Академический Проект; Гаудеамус, 2004 – с.544.
9. ECMA Standardizing Information and Communications Systems, Volume and File Structure for write-once and rewritable media using Non-Sequential Recording for Information Interchange. ECMA, 1997. – с. 150.
10. OSTA Organization, Universal Disk Format Specification Revision 2.50. OSTA, 2003. – с. 165.
11. SFF Committee, INF-8090. ATAPI Multimedia Devices, 2008. – с. 1008.
12. Интернет энциклопедия: http://www.wikipedia.org/

ПРИЛОЖЕНИЕ.

```
	//-------------------------------------------------------------------------
--------SELECT DEVICE
	void CProjectDlg::OnCbnSelendokCombo1()
	{
		SetDlgItemTextW(IDC_STATIC3, L"");
		CWaitCursor cursor;

		m_List.DeleteAllItems();

		if( m_DeviceID != 0 )
		{
			if( ! UnsetDevice(m_DeviceID, &m_iError) )
			{
				SetDlgItemTextW(IDC_STATIC3, L"Ошибка извлечения
устроиства");
				return;
			}
		}

		CString PathName;

		m_Devices.GetLBText(m_Devices.GetCurSel(), PathName);

		if( PathName == L"Выберите устроиство" || PathName == L"Устроиств не
найдено" )
		{
			m_DeviceID = 0;
			return;
		}

		wchar_t Path[6] = {0};
		Path[0] = PathName[0];
		wcscat(Path, L":\\");

		if( ! SetDevice(Path, &m_DeviceID, &m_iError) )
		{
			m_DeviceID = 0;
			SetDlgItemTextW(IDC_STATIC3, L"Ошибка утсроиство");
			return;
		}


		BOOL			bMediaAv;
		MEDIA_STATUS		MediaStatus;
		WRITE_MODE		WriteMode;
		BYTE			byMediaType;

		if( ! CheckMediaStatus(m_DeviceID, &bMediaAv, &MediaStatus,
&WriteMode, &byMediaType) )
		{
			SetDlgItemTextW(IDC_STATIC3, L"Ошибка диска");
			return;
		}
```

```
            if( !bMediaAv )
            {
                  SetDlgItemTextW(IDC_STATIC3, L"Диск не найден");
                  return;
            }

            switch(WriteMode)
            {
            case NOT_SUPPORT:
                  m_Log = L"Диск не поддерживается";
                  break;

            case OVERWRITE:
                  m_Log = L"Диск перезаписываемый";
                  break;

            case APPEND:
                  m_Log = L"Диск добовляемый";
                  if( MediaStatus == PRODVD_MADE_RW_LOCKED )
                        m_Log = L"Диск заблокирован";
                  break;

            case READ_ONLY:
                  m_Log = L"Диск только читаемый";
                  break;

            case FINALIZE_ONLY:
                  m_Log = L"Диск только финализируемый";
                  break;
            }

            SetDlgItemTextW(IDC_STATIC3, m_Log);
      }

      //-------------------------------------------------------------------------
--------OVERWRITE
      void CProjectDlg::OnBnClickedCheck1()
      {
            CButton *p1 = (CButton*)GetDlgItem(IDC_CHECK1);
            CButton *p2 = (CButton*)GetDlgItem(IDC_CHECK2);

            if( p1->GetCheck() )
                  p2->SetCheck(0);
            else
                  p2->SetCheck(1);
      }

      //-------------------------------------------------------------------------
--------APPEND
      void CProjectDlg::OnBnClickedCheck2()
      {
            CButton *p1 = (CButton*)GetDlgItem(IDC_CHECK1);
            CButton *p2 = (CButton*)GetDlgItem(IDC_CHECK2);

            if( p2->GetCheck() )
                  p1->SetCheck(0);
            else
                  p1->SetCheck(1);
      }

      //-------------------------------------------------------------------------
--------GET MEDIA STATUS
      void CProjectDlg::OnBnClickedButton2()
```

```
	{
		SetDlgItemTextW(IDC_STATIC3, L"Подготовка диска");
		CWaitCursor cursor;

		m_List.DeleteAllItems();

		WRITE_MODE wm;
		CButton *p = (CButton*)GetDlgItem(IDC_CHECK1);

		if( p->GetCheck() )
			wm = OVERWRITE;
		else
			wm = APPEND;

		SetRecordMode(m_DeviceID, wm);


		DISC_STATUS ds;
		CHECK_DISC_STATUS cds;

		if( ! GetMediaStatus2(m_DeviceID, NULL, &ds, &cds, TRUE, &m_iError)
)
		{
			SetDlgItemTextW(IDC_STATIC3, L"Ошибка диска");
			SetDlgItemTextW(IDC_EDIT1, L"");
			return;
		}


		m_Path = L"\\";
		InsertItems(m_Path);

		CButton *p2 = (CButton*)GetDlgItem(IDC_CHECK2);
		p->SetCheck(0);
		p2->SetCheck(1);

		SetDlgItemTextW(IDC_EDIT1, L"");
		SetDlgItemTextW(IDC_STATIC3, L"Готово");
	}


	//-------------------------------------------------------------------------
--------BACK
	void CProjectDlg::Back()
	{
		CWaitCursor cursor;

		if( m_Path == L"\\" )
			return;

		int k = 0;
		for(int i = m_Path.GetLength()-1; m_Path[i] != L'\\'; i--, k++)
			;

		wchar_t wchPath[MAX_PATH] = {0};

		wcsncpy(wchPath, m_Path.GetBuffer(), m_Path.GetLength()-k-1);

		if( wcscmp(wchPath, L"") == 0 )
			m_Path = L"\\";
		else
			m_Path = wchPath;
```

```
		InsertItems(m_Path);
	}

	//--------------------------------------------------------------------
--------BLOCK
	void CProjectDlg::OnBnClickedButton3()
	{
		CWaitCursor cursor;
		SetDlgItemTextW(IDC_STATIC3, L"Блокировка диска");

		m_List.DeleteAllItems();

		CString Password;

		GetDlgItemTextW(IDC_EDIT1, Password);

		wchar_t wszVolumeName[] = L"Диск защищён!";

		if( ! FinilizeMediaLock(m_DeviceID, Password.GetBuffer(),
wszVolumeName, NULL, &m_iError) )
		{
			SetDlgItemTextW(IDC_EDIT1, L"");
			SetDlgItemTextW(IDC_STATIC3, L"Ошибка блокирования");
			return;
		}


		DISC_STATUS ds;
		CHECK_DISC_STATUS cds;

		if( ! GetMediaStatus2(m_DeviceID, NULL, &ds, &cds, TRUE, &m_iError)
)
		{
			SetDlgItemTextW(IDC_STATIC3, L"Ошибка диска");
			SetDlgItemTextW(IDC_EDIT1, L"");
			return;
		}


		m_Path = L"\\";
		InsertItems(m_Path);

		SetDlgItemTextW(IDC_STATIC3, L"Готово");
	}

	//--------------------------------------------------------------------
--------UNBLOCK
	void CProjectDlg::OnBnClickedButton4()
	{
		CWaitCursor cursor;
		SetDlgItemTextW(IDC_STATIC3, L"Разблокировка диска");

		m_List.DeleteAllItems();

		CString Password;

		GetDlgItemTextW(IDC_EDIT1, Password);


		CButton *p = (CButton*)GetDlgItem(IDC_CHECK1);
		WRITE_MODE wm;
		if( p->GetCheck() )
			wm = OVERWRITE;
```

```
            else
                  wm = APPEND;

            SetRecordMode(m_DeviceID, wm);

            DISC_STATUS ds;
            CHECK_DISC_STATUS cds;

            if( ! GetMediaStatus2(m_DeviceID, Password.GetBuffer(), &ds, &cds,
TRUE, &m_iError) )
            {
                  SetDlgItemTextW(IDC_EDIT1, L"");
                  SetDlgItemTextW(IDC_STATIC3, L"Ошибка Разблокирования");
                  return;
            }


            m_Path = L"\\";
            InsertItems(m_Path);

            SetDlgItemTextW(IDC_EDIT1, L"");
            SetDlgItemTextW(IDC_STATIC3, L"Готово");
      }




      //-------------------------------------------------------------------------
--------ERASE
      void CProjectDlg::OnBnClickedButton5()
      {
            CWaitCursor cursor;
            SetDlgItemTextW(IDC_STATIC3, L"Стирание диска");

            if( ! EraseMedia(m_DeviceID, QUICK_ERASE, &m_iError) )
            {
                  SetDlgItemTextW(IDC_STATIC3, L"Ошибка диска");
                  return;
            }

            OnBnClickedButton2();

            SetDlgItemTextW(IDC_STATIC3, L"Готово");
      }




      //-------------------------------------------------------------------------
--------ON DROP
      void CProjectDlg::OnDropFiles(HDROP hDropInfo)
      {
            CWaitCursor cursor;
            SetDlgItemTextW(IDC_STATIC3, L"Подготовка");

            wchar_t buff[MAX_PATH] = {0};
            DISC_STATUS discInfo = {0};
            int num = DragQueryFileW(hDropInfo, 0xFFFFFFFF, buff, MAX_PATH);

            if( ! bGetMediaSpaceInfo(m_DeviceID, &discInfo, &m_iError) )
            {
```

```
                SetDlgItemTextW(IDC_STATIC3, L"Ошибка диска");
                return;
        }

        CString wstr;
        DWORD64 size = 0;
        for(int i = 0; i < num; i++)
        {
                DragQueryFileW(hDropInfo, i, buff, MAX_PATH);
                if(buff[0] < L'A' || buff[0] > L'Z')
                        continue;
                wstr = buff;

                if( ! _wchdir(wstr) )                    // folder
                        size += GetFolderSize(wstr);
                else                                             // File
                        size += GetFileSize(wstr);
        }

        if(size/1024 > discInfo.dsAvailableSpace)
        {
                SetDlgItemTextW(IDC_STATIC3, L"Нехватает место на диске");
                return;
        }

        CButton *p1 = (CButton*)GetDlgItem(IDC_CHECK3);

        if( ! p1->GetCheck() )
        {
                vector<CString> vecFolders;
                vector<CString> vecFiles;

                for(int i = 0; i < num; i++)
                {
                        DragQueryFileW(hDropInfo, i, buff, 256);
                        if(buff[0] < L'A' || buff[0] > L'Z')
                                continue;

                        if( ! _wchdir(buff) ) // folder
                                vecFolders.push_back(buff);
                        else
                                vecFiles.push_back(buff);
                }

                SetDlgItemTextW(IDC_STATIC3, L"Копирование");


                for(int i = 0; i < vecFolders.size(); i++)
                {
                        CopyFolderToDVD_W(m_DeviceID, vecFolders[i], m_Path,
NULL, TRUE, &m_iError);
                }

                if( vecFiles.size() > 0 )
                {
                        wchar_t **pp = (wchar_t**)calloc(vecFiles.size(),
sizeof(wchar_t*));

                        for(int i = 0; i < vecFiles.size(); i++)
                        {
                                pp[i] = (wchar_t*)calloc(MAX_PATH,
sizeof(wchar_t));
                                wcscpy(pp[i], vecFiles[i].GetBuffer());
```

```
                        }

                        CopyFilesToDVD_W(m_DeviceID, vecFiles.size(), pp,
m_Path.GetBuffer(), NULL, TRUE, &m_iError);

                        for(int i = 0; i < vecFiles.size(); i++)
                              free(pp[i]);
                        free(pp);
                  }
            }
            else
            {
                  vector<CString> vecFilesAndFolders;

                  for(int i = 0; i < num; i++)
                  {
                        DragQueryFileW(hDropInfo, i, buff, 256);
                        if(buff[0] < L'A' || buff[0] > L'Z')
                              continue;

                        vecFilesAndFolders.push_back(buff);
                  }

                  SetDlgItemTextW(IDC_STATIC3, L"Копирование");

                  if( vecFilesAndFolders.size() > 0 )
                  {
                        wchar_t **pp =
(wchar_t**)calloc(vecFilesAndFolders.size(), sizeof(wchar_t*));

                        for(int i = 0; i < vecFilesAndFolders.size(); i++)
                        {
                              pp[i] = (wchar_t*)calloc(MAX_PATH,
sizeof(wchar_t));
                              wcscpy(pp[i], vecFilesAndFolders[i].GetBuffer());
                        }

                        ParolDlg dlg;
                        dlg.DoModal();

                        CString EncName  = dlg.m_Name;
                        CString Password = dlg.m_Paro;

                        if( EncName == L"" || EncName == L"" )
                        {
                              SetDlgItemTextW(IDC_STATIC3, L"");

                              for(int i = 0; i < vecFilesAndFolders.size(); i++)
                                    free(pp[i]);
                              free(pp);

                              return;
                        }

                        RedrawWindow();

                        if( ! bCopyEncFile(m_DeviceID,
vecFilesAndFolders.size(), pp, m_Path.GetBuffer(), EncName.GetBuffer(),
Password.GetBuffer(), TRUE, &m_iError) )
                        {
                              SetDlgItemTextW(IDC_STATIC3, L"Ошибка
копирования");
```

```
                              for(int i = 0; i < vecFilesAndFolders.size(); i++)
                                    free(pp[i]);
                              free(pp);

                              return;
                        }

                        for(int i = 0; i < vecFilesAndFolders.size(); i++)
                              free(pp[i]);
                        free(pp);
                  }
            }

            OnBnClickedButton2();

            CDialog::OnDropFiles(hDropInfo);
      }

      //-------------------------------------------------------------------------
--------FOLDER SIZE
      DWORD64 CProjectDlg::GetFolderSize(CStringW hddFolderPath)
      {
            WIN32_FIND_DATAW FileData = {0};

            DWORD64 FolderSize = 0;
            CStringW DestFilePath;
            CStringW DestFolderPath;

            if( hddFolderPath[ hddFolderPath.GetLength()-1 ] != '\\' )
                  hddFolderPath += L"\\";

            void * hSearch = FindFirstFileW(hddFolderPath+L"*", &FileData);

            if (hSearch == INVALID_HANDLE_VALUE)
            {
                  return 0;
            }
            else
            {
                  do
                  {
                        if(wcscmp(FileData.cFileName,L".") &&
wcscmp(FileData.cFileName,L".")) //opuskayem ne nujniye papki
                        {
                              if( ( FileData.dwFileAttributes &
FILE_ATTRIBUTE_DIRECTORY ))  //if Folder
                              {
                                    if( hddFolderPath[
hddFolderPath.GetLength()-1 ] != '\\' )
                                          DestFolderPath = hddFolderPath + L"\\"
+ FileData.cFileName;
                                    else
                                          DestFolderPath = hddFolderPath +
FileData.cFileName;

                                    FolderSize += GetFolderSize(DestFolderPath);
                              }
                              else //if File
                              {
                                    if( hddFolderPath[
hddFolderPath.GetLength()-1 ] != '\\' )
                                          DestFilePath = hddFolderPath + L"\\" +
FileData.cFileName;
```

```
                                    else
                                          DestFilePath = hddFolderPath +
FileData.cFileName;

                                    FolderSize += GetFileSize(DestFilePath);
                              }
                        }

                  }while(FindNextFileW(hSearch, &FileData));
            }
            FindClose(hSearch);
            return FolderSize;
      }

      //-------------------------------------------------------------------------
--------FILE SIZE
      DWORD64 CProjectDlg::GetFileSize(CStringW filePath)
      {
            struct _stat32i64 stbuf;
           if( _wstat32i64(filePath, &stbuf) == -1 )
                  return FALSE;
           else
                  return (stbuf.st_size);
      }

      //-------------------------------------------------------------------------
--------COPY TO HDD
      void CProjectDlg::CopyToHDD()
      {
            CWaitCursor cursor;
            SetDlgItemTextW(IDC_STATIC3, L"Копирование на жесткий диск");

            BROWSEINFOW         bi;
            wchar_t             szDisplayName[MAX_PATH];
            LPITEMIDLIST        pidl;
            LPMALLOC                pMalloc = NULL;
            ZeroMemory(&bi, sizeof(bi));
            bi.hwndOwner = NULL;
            bi.pszDisplayName = szDisplayName;
            bi.lpszTitle = TEXT("Select folder");
            bi.ulFlags = BFFM_SELCHANGED;
            pidl = SHBrowseForFolderW(&bi);
            if(! pidl )
                  return;

            SHGetPathFromIDListW(pidl, szDisplayName);

            if(wcscmp(szDisplayName, L"") == 0 )
                  return;

            vector<CString> vecFolders;
            vector<CString> vecFilesName;
            vector<CString> vecFilesPath;
            vector<CString> vecEncFiles;

            POSITION pos = m_List.GetFirstSelectedItemPosition();

            CString     str;
            long  item = 0;
            wchar_t wch[MAX_PATH];
            LVITEM      lv = {0};
            lv.pszText = wch;
            lv.iSubItem = 0;
```

```
		lv.cchTextMax = MAX_PATH;
		lv.mask = LVIF_TEXT;

		DataNode_Ex Node;

		while(pos)
		{
			str = m_Path;

			if( str[str.GetLength()-1] != L'\\' )
				str += L"\\";

			lv.iItem = m_List.GetNextSelectedItem(pos);

			m_List.GetItem(&lv);

			str += lv.pszText;

			GetDataNodeByFullPath(m_DeviceID, str.GetBuffer(), &Node,
&m_iError);

			if( Node.bFolder )
				vecFolders.push_back(Node.wszFullPath);
			else
			{
				if( Node.bIsEncrypted)
					vecEncFiles.push_back(Node.wszFullPath);
				else
				{
					vecFilesName.push_back(Node.wszName);
					vecFilesPath.push_back(Node.wszFullPath);
				}
			}
		}

		CString path = szDisplayName;
		path += L"\\";

		for(int i = 0; i < vecFilesPath.size(); i++)
		{
			CopyFileW2(vecFilesPath[i], path + vecFilesName[i]);
		}

		for(int i = 0; i < vecFolders.size(); i++)
		{
			CopyFolderToHdd(vecFolders[i], szDisplayName);
		}


		for(int i = 0; i < vecEncFiles.size(); i++)
		{
			Parol2 dlg;
			dlg.m_Name = vecEncFiles[i];
			dlg.DoModal();

			if( dlg.m_Parol == L"")
			{
				return;
			}

			CString passwrod = dlg.m_Parol;
			DataNode_Ex Node;
			int iError = 0;
```

```
                  if( failed ExtractEncryptedFile(m_DeviceID,
vecEncFiles[i].GetBuffer(), passwrod.GetBuffer(), &Node, &iError) )
                  {
                        SetDlgItemTextW(IDC_STATIC3, L"Ошибка извлечения");
                        return;
                  }

                  for(int k = 0; k < Node.nCountOfChilds; k++)
                        CopyEncFolderToHdd(L"\\", k, szDisplayName);
            }


            SetDlgItemTextW(IDC_STATIC3, L"Готово");
      }
```