В данной дипломной работе рассмотрены вопросы, связанные с разработкой системы защиты информации на предприятии. В ходе выполнения работы был проведен анализ информационной имеющихся средств защиты информации, в результате которого выявлены состав источников и носителей информации, проведено категорирование информации, выявлены возможные каналы утечки информации. В рамках аудита информационной безопасности была проанализирована текущая деятельность предприятия по вопросам защиты информации, проведена оценка информационной системы организации, в которой циркулирует конфиденциальная информация; были выявлены недостатки системы защиты, способы, устранения которых представлены в работе.

В результате выполнения дипломной работы была разработана комплексная система защиты информации, был произведен подбор технических и программно-аппаратных средств. В экономической части работы рассчитаны затраты на проектирование системы защиты.

ИСПОЛЬЗУЕМЫЕ ОБОЗНАЧЕНИЯ

ИБ –информационная безопасность

НСД –несанкционированный доступ

СЗКИ –средства защиты конфиденциальной информации

АС –автоматизированная система

КИ –кредитная история

БКИ –Бюро кредитных историй

КИ –кредитная история

СЗИ –система защиты информации

ЛВС –локально-вычислительная сеть

АРМ –автоматизированное рабочее место

ТЗ –техническое задание

ПРД –правила разграничения доступа

ЦП –цифровая подпись

ПО –программное обеспечение

ПЭП –простая электронная подпись

НЭП –неквалифицированная электронная подпись

Введение

Информация является ресурсом, который как и любой иной бизнес-ресурс (финансы, оборудование, персонал) имеет для каждого предприятия определенную стоимость и подлежит защите. Обеспечение информационной безопасности заключается в защите информации от различных видов угроз с целью обеспечения нормального режима работы, успешного развития бизнеса, минимизации деловых рисков, обеспечения личной безопасности сотрудников предприятия.

Информация может быть представлена в различных формах. Она может быть напечатана или написана на бумаге, хранится в электронном виде, передаваться по почте или электронным способом, демонстрироваться в фильмах, видеозаписях, фотографиях, слайдах, а также быть высказана в разговорах. Вне зависимости от формы представления информации, в которой она хранится, обрабатывается или передается, информация должна быть должным образом защищена.

Комплексное обеспечение информационной безопасности заключается в сочетании:

- конфиденциальности: предоставлении доступа к информации только авторизованным сотрудникам;

- целостности: защиты от модификации или подмены информации;

- доступности: гарантировании доступа к информации и информационным ресурсам, средствам информатизации авторизованным пользователям.

Информация, информационные ресурсы и средства информатизации подвергаются широкому спектру угроз, включая мошенничество, промышленный шпионаж, саботаж, вандализм, пожары, затопления и пр. Случаи ущерба в результате заражения компьютерными вирусами, внедрения программ-закладок, несанкционированного доступа и/или модификации конфиденциальной информации, атак типа «отказ в обслуживании» становятся все более частыми в деятельности предприятий.

Реализация угроз может нанести значительный ущерб и стать причиной существенных убытков, причиной снижения деловой активности, временного или полного прекращения деятельности. Для предотвращения реализации угроз предпринимаются меры, включая безусловное выполнения определенных политикой безопасности предприятия правил и процедур работы с информационной системой, использование средств защиты информации, контроль со стороны уполномоченных сотрудников за выполнением сотрудниками своих обязанностей по обеспечению информационной безопасности.

Информационной безопасностью называют меры по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе. Информационная безопасность включает в себя меры по защите процессов создания данных, их ввода, обработки и вывода. Целью информационной безопасности является обезопасить ценности системы, защитить и гарантировать точность и целостность информации, и минимизировать разрушения, которые могут иметь место, если информация будет модифицирована или разрушена. Информационная безопасность требует учета всех событий, в ходе которых информация создается, модифицируется, к ней обеспечивается доступ или она распространяется.

1. Анализ вопроса защиты баз данных

1.1 Постановка задачи и целесообразность защиты баз данных

Защита баз данных является одной из самых сложных задач, стоящих перед подразделениями, отвечающими за обеспечение информационной безопасности. С одной стороны, для работы с базой необходимо предоставлять доступ к данным всем сотрудникам, кто по долгу службы должен осуществлять сбор, обработку, хранение и передачу данных. С другой стороны, укрупнение баз данных далеко не всегда имеет централизованную архитектуру (наблюдается ярко выраженная тенденция к территориально распределенной системе), в связи с чем, действия нарушителей становятся все более изощренными. При этом четкой и ясной методики комплексного решения задачи защиты баз данных, которую можно было бы применять во всех случаях, не существует, в каждой конкретной ситуации приходится находить индивидуальный подход.

Долгое время защита баз данных ассоциировалась с защитой локальной сети предприятия от внешних атак на компьютерную сеть и борьбой с вирусами. Последние аналитические отчеты консалтинговых компаний выявили другие, более важные направления защиты информационных ресурсов компаний. Исследования показали, что от утечки информации со стороны персонала и злонамеренных действий привилегированных пользователей не спасают ни межсетевые экраны, ни виртуальные частные сети (VPN), ни даже системы обнаружения вторжений (IDS), ни системы анализа защищенности. Неавторизованный доступ к данным и утечка конфиденциальной информации являются главными составляющими потерь предприятий

вместе с вирусными атаками и кражей портативного оборудования (по данным аналитических отчетов компании InfoWatch).

Предпосылками к утечке информации, содержащейся в базе данных являются:

· многие даже не догадываются о том, что их базы данных крадут;

· кража и причиненный ущерб имеют латентный характер;

· если факт кражи данных установлен, большинство компаний замалчивают причиненный ущерб.

Причины такого положения следующие:

· Высокая латентность подобных преступлений (понесенные потери обнаруживаются спустя некоторое время) и достаточно редко раскрываются. Эксперты называют следующие цифры по сокрытию: США - 80%, Великобритания - до 85%, Германия - 75%, Россия - более 90%. Стремление руководства умолчать, с целью не дискредитировать свою организацию, усугубляет ситуацию.

· Низкий интерес к разработке средств, ликвидирующих или уменьшающих риски, связанные с внутренними угрозами; недостаточная распространенность и популярность таких решений. В результате о средствах и методах защиты от кражи информации легальными сотрудниками знают немногие.

· Недостаточное предложение на рынке комплексных систем для борьбы с внутренними угрозами, особенно в отношении краж информации из баз данных.

Задачами, которые в результате дипломного проектирования необходимо проработать будут: обеспечение защиты

базы данных от кражи, взлома, уничтожения, распространения, что будет решено с помощью таких средств как обеспечения защищенного взаимодействия пользователей с базой данных, разработкой прозрачного для пользователей приложения. Защита должна включать в себя комплекс административных, процедурных, программно-технических способов и средств защиты.

1.2 Структурные уровни и этапы построения защищенной базы данных

предприятия с целью выявления таких угроз, как хищения, утрата, уничтожение, модификация, дублирование, несанкционированный доступ. На втором этапе следует составление математических моделей основных информационных потоков и возможных нарушений, моделирование типовых действий злоумышленников; на третьем - выработка комплексных мер по пресечению и предупреждению возможных угроз с помощью правовых, организационно-административных и технических мер защиты. Однако разнообразие деятельности предприятий, структуры бизнеса, информационных сетей и потоков информации, прикладных систем и способов организации доступа к ним не позволяет создать универсальную методику решения и поставленного в ряде случаев на промышленные рельсы сбыта баз данных, содержащих персональные данные абонентов, клиентов или сотрудников и коммерческие тайны компаний.

Так как необходимо организовать защиту производственной базы данных, то при разработке проекта необходимо соблюсти принципы корпоративной работы предприятия: использование корпоративного сервисного программного обеспечения (далее ПО), единое информационное пространство, интеграция решаемых задач в разных подразделениях, автоматизация формализованных процессов,

повышенные требования к информационной безопасности, ролевой доступ к данным.

Процесс построения защиты базы данных можно разделить на этапы

· анализ предметной области и проектирование базы данных;

· составление пользователей и разделение их обязанностей;

· ввод данных;

· анализ существующих угроз;

· выработка модели нарушителя;

· выработка подхода к построению защиты;

· организация защиты средствами СУБД;

· разработка защищенного приложения, работающего с базой данных;

· защита сетевых ресурсов предприятия;

· аудит.

1.3. Угрозы безопасности баз данных

Одним из важнейших аспектов проблемы обеспечения безопасности компьютерных систем является определение, анализ и классификация возможных угроз безопасности. Перечень угроз, вероятность их реализации, а также модель нарушителя служат основой для проведения анализа риска и формулирования требований к системе защиты.

Особенности современных автоматизированных систем как объекта защиты

Как показывает анализ, большинство современных автоматизированных систем обработки информации в общем случае представляет собой территориально распределенные системы интенсивно взаимодействующих (синхронизирующихся) между собой по данным (ресурсам) и управлению (событиям) локальных вычислительных сетей (ЛВС) и отдельных ЭВМ.

В распределенных АС возможны все "традиционные" для локально расположенных (централизованных) вычислительных систем способы несанкционированного вмешательства в их работу и доступа к информации. Кроме того, для них характерны и новые специфические каналы проникновения в систему и несанкционированного доступа к информации, наличие которых объясняется целым рядом их особенностей.

Перечислим основные из особенностей распределенных АС:

территориальная разнесённость компонентов системы и наличие интенсивного обмена информацией между ними;

широкий спектр используемых способов представления, хранения и передачи информации;

интеграция данных различного назначения, принадлежащих различным субъектам, в рамках единых баз данных и, наоборот, размещение необходимых некоторым субъектам данных в различных удаленных узлах сети;

абстрагирование владельцев данных от физических структур и места размещения данных;

использование режимов распределенной обработки данных;

участие в процессе автоматизированной обработки информации большого количества пользователей и персонала различных категорий;

непосредственный и одновременный доступ к ресурсам (в том числе и информационным) большого числа пользователей (субъектов) различных категорий;

высокая степень разнородности используемых средств вычислительной техники и связи, а также их программного обеспечения;

отсутствие специальной аппаратной поддержки средств защиты в большинстве типов технических средств, широко используемых в автоматизированных системах.

1.4 Уязвимость основных структурно-функциональных элементов

Рабочие станции являются наиболее доступными компонентами сетей и именно с них могут быть предприняты наиболее многочисленные попытки совершения несанкционированных действий. С рабочих станций осуществляется управление процессами обработки информации, запуск программ, ввод и корректировка данных, на дисках рабочих станций могут размещаться важные данные и программы обработки. На мониторы и печатающие устройства рабочих станций выводится информация при работе пользователей (операторов), выполняющих различные функции и имеющих разные полномочия по доступу к данным и другим ресурсам системы. Именно поэтому рабочие станции должны быть надежно защищены от доступа посторонних лиц и содержать средства разграничения доступа к ресурсам со стороны законных пользователей, имеющих разные полномочия. Кроме того, средства защиты должны предотвращать нарушения нормальной настройки рабочих станций и режимов их функционирования, вызванные

неумышленным вмешательством неопытных (невнимательных) пользователей.

Каналы и средства связи также нуждаются в защите. В силу большой пространственной протяженности линий связи (через неконтролируемую или слабо контролируемую территорию) практически всегда существует возможность подключения к ним, либо вмешательства в процесс передачи данных. Возможные при этом угрозы подробно изложены в главе 2.3.

1.5 Основные цели защиты информации на предприятии

Формулирование целей и задач защиты информации, как любой другой деятельности, представляет начальный и значимый этап обеспечения безопасности информации. Важность этого этапа часто недооценивается и ограничивается целями и задачами, напоминающими лозунги. В то же время специалисты в области системного анализа считают, что от четкости и конкретности целей и постановок задач во многом зависит успех в их достижении и решении. Провал многих, в принципе полезных, начинаний обусловлен именно неопределенностью и расплывчатостью целей и задач, из которых не ясно, кто, что и за счет какого ресурса предполагает решать продекларированные задачи.

Цели защиты информации сформулированы в ст. 20 Закона РФ «Об информации, информатизации и защите информации»:

- предотвращение утечки, хищения, искажения, подделки информации;

- предотвращение угроз безопасности личности, общества, государства;

- предотвращение несанкционированных действий по уничтожению, модификации, копированию, блокированию информации, предотвращение других форм незаконного вмешательства в информационные

ресурсы и информационные системы, обеспечение правового режима как объекта собственности;

- защита конституционных прав граждан по сохранению личной тайны, конфиденциальности персональных данных, имеющихся в информационных системах;

- сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством;

- обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологии и средств их обеспечения.

В общем виде цель защиты информации определяется как обеспечение безопасности информации, содержащей государственную или иные тайны. Но такая постановка цели содержит неопределенные понятия: информация и безопасность.

Основной целью защиты информации является обеспечение заданного уровня ее безопасности. Под заданным уровнем безопасности информации понимается такое состояние защищенности информации от угроз, при которых обеспечивается допустимый риск ее уничтожения, изменения и хищения. При этом под уничтожением информации понимается не только ее физическое уничтожение, но и стойкое блокирование санкционированного доступа к ней. В общем случае при блокировке информации в результате неисправности замка или утери ключа сейфа, забытия пароля компьютера, искажения кода загрузочного сектора винчестера или дискетки и других факторах информация не искажается и не похищается и при определенных усилиях доступ к ней может быть восстановлен. Следовательно, блокирование информации прямой угрозы ее безопасности не создает. Однако при невозможности доступа к ней в нужный момент ее пользователь теряет информацию так же, как если бы она была уничтожена.

1.6 Состав и назначение аппаратных и программных средств

@!#!@#!@#!# создана с учетом единых концептуальных положений, лежащих в основе построения современных вычислительных сетей связи. Основу таких положений в первую очередь составляет использование общих принципов построения и однородного активного сетевого оборудования.

Сетевая структура ЛВС компании содержит несколько выраженных иерархических уровней. ЛВС бухгалтерии представляет фрагмент корпоративной сети, данный фрагмент сети состоит из нескольких сегментов, подключенных к магистрали более высокого уровня и осуществляющих доступ информационным ресурсам сети. ЛВС построена на базе стандарта Ethernet 10/100 Base-T.

Стандарт Ethernet 10/100 Base-T подходит для работы с различными операционными системами и сетевым оборудованием. Применение этого стандарта позволяет простыми методами добиться стабильной работы сети.

Для построения сети необходимо выбрать кабель, от качества и характеристик которого во многом зависит качество работы сети. В данном случае использована неэкранированная витая пара категории 5.

Конфигурация сети представлена в таблице 1.

Таблица 1

Компонент/ характеристика	Реализация
Топология	Звезда
Линия связи	Неэкранированная витая пара категории 5
Сетевые адаптеры	Ethernet 10/100

	Base-T
Коммуникационное оборудование	Коммутатор Ethernet 10/100 Base-T
Совместное использование периферийных устройств	Подключение сетевых принтеров через компьютеры к сетевому кабелю. Управление очередями к принтерам осуществляется с помощью программного обеспечения компьютеров.
Поддерживаемые приложения	Организация коллективной работы в среде электронного документооборота, работа с базой данных.

При выборе сетевых компонентов необходимо придерживаться следующих общих требований:

· компьютеры должны обладать хорошим быстродействием, чтобы обеспечить работу всех сетевых служб и приложений в реальном времени без заметного замедления работы;

· жесткие диски компьютеров должны быть максимально надежными для того, чтобы обеспечить безопасность и целостность хранимых данных;

· сетевые принтеры должны устанавливаться в зависимости от местоположения пользователей, активно их использующих;

· коммутатор, являющийся центральным устройством данной сети, необходимо располагать в легкодоступном месте, чтобы можно было без проблем подключать кабели и следить за индикацией.

Перечисленные требования определили следующую конфигурацию сетевых компонентов: все компьютеры сети на базе процессора IntelPentium 4, в качестве сетевого принтера выбрано многофункциональное устройство (лазерное), поскольку они имеют наибольший ресурс и малые затраты на расходные материалы.

1.7 информации, составляющей коммерческую тайну

Коммерческая тайна − форма обеспечения безопасности наиболее важной коммерческой информации, предлагающая ограничение ее распространения. С правовой точки зрения, коммерческая тайна предприятия представляет собой средство защиты против недобросовестной конкуренции в рамках реализации права на интеллектуальную собственность.

Перечень сведений, составляющих коммерческую тайну предприятия:

1. Производство

1.1. Сведения о структуре производства, производственных мощностях, типе и размещении оборудования, запасах сырья, материалов, комплектующих и готовой продукции.

2. Управление

2.1. Сведения о применяемых оригинальных методах управления предприятием.

2.2. Сведения о подготовке, принятии и исполнении отдельных решений руководства предприятия по коммерческим, организационным, производственным, научно-техническим и иным вопросам.

3. Планы

3.1. Сведения о планах расширения или свертывания производства различных видов продукции и их технико-экономических обоснованиях. 3.2. Сведения о планах инвестиций, закупок, продаж. 4. Совещания

4.1. Сведения о фактах проведения, целях, предмете и результатах совещаний и заседаний органов управления предприятия. 5. Финансы

5.1. Сведения о балансах предприятия.

5.2. Сведения, содержащиеся в бухгалтерских книгах предприятия. 5.3. Сведения о кругообороте средств предприятия.

5.4. Сведения о финансовых операциях предприятия.

5.5. Сведения о состоянии банковских счетов предприятия и производимых операциях.

5.6. Сведения об уровне доходов предприятия.

5.7. Сведения о долговых обязательствах предприятия.

5.8. Сведения о состоянии кредита предприятия (пассивы и активы). 6. Рынок

6.1. Сведения о применяемых предприятием оригинальных методах изучения рынка.

6.2. Сведения о результатах изучения рынка, содержащие оценку состояния и перспектив развития рыночной конъюнктуры.

6.3. Сведения о рыночной стратегии предприятия.

6.4. Сведения о применяемых предприятием оригинальных методах осуществления продаж.

6.5. Сведения об эффективности коммерческой деятельности предприятия. 7. Партнеры

7.1. Систематизированные сведения о внутренних и зарубежных заказчиках, подрядчиках, поставщиках, потребителях, покупателях, компаньонах, спонсорах, посредниках, клиентах и других партнерах деловых отношений предприятия, а также о его конкурентах, которые не содержатся в открытых источниках (справочниках, каталогах и др.).

8. Переговоры

8.1. Сведения о подготовке и результатах проведения переговоров с деловыми партнерами предприятия.

9. Контракты

9.1. Сведения, условия конфиденциальности которых установлены в договорах, контрактах, соглашениях и других обязательствах предприятия. 10. Цены

10.1. Сведения о методах расчета, структуре, уровне цен на продукцию и размерах скидок.

11. Торги, аукционы

11.1. Сведения о подготовке к торгам или аукциону и их результатах. 12. Наука и техника

12.1. Сведения о целях, задачах, программах перспективных научных исследований.

12.2. Ключевые идеи НИР.

12.3. Точные значения конструкционных характеристик создаваемых изделий и оптимальных параметров разрабатываемых технологических процессов (размеры, объемы, конфигурация, процентное содержание компонентов, температура, давление, время и т.д.).

12.4. Аналитические и графические зависимости, отражающие найденные закономерности и взаимосвязи.

12.5. Данные об условиях экспериментов и оборудования, на котором они проводились.

12.6. Сведения о материалах, из которых изготовлены отдельные детали.

12.7. Сведения об особенностях конструкторско-технологического, художественно-технического решения изделия, дающие положительный экономический эффект.

12.8. Сведения о методах защиты от подделки товарных знаков.

12.9. Сведения о состоянии программного и компьютерного обеспечения. 13. Технология

13.1. Сведения об особенностях используемых и разрабатываемых технологий и специфике их применения.

14. Безопасность

14.1. Сведения о порядке и состоянии организации защиты коммерческой тайны.

14.2. Сведения, составляющие коммерческую тайну предприятий-партнеров и переданные на доверительной основе.

Правильная организация конфиденциального делопроизводства в фирме является составной частью комплексного обеспечения безопасности информации и имеет важное значение в достижении цели ее защиты. Как известно, специалисты, занимающиеся в области информационной безопасности утверждают, что порядка 80% конфиденциальной информации находится в документах делопроизводства. Поэтому вопросы конфиденциального документооборота в фирме несомненно играют важную роль в достижении ею экономических успехов.

А, следовательно, и документы, содержащие ту или иную информацию подразделяются на секретные и конфиденциальные. Причем, секретные документы могут быть с грифом "Секретно", "Совершенно секретно", "Особой важности". Конфиденциальные документы соответственно с грифами "Коммерческая тайна", "Банковская тайна" и т.д. В настоящее время видов конфиденциальной информации (а, следовательно, и возможных грифованных документов) насчитывается более 30. Что в целом не создает благоприятной атмосферы в смысле обеспечения их безопасности. По этой причине количество видов конфиденциальной информации в перспективе надо полагать уменьшится.

1.9Анализ модели угроз информационного характера

Одной из главных задач при разработке системы защиты

информации является построение модели угроз. Это позволяет в полном объеме оценить слабые места автоматизированной системы.

В соответствии с пунктом 2 статьи 19 ФЗ «О персональных данных» обеспечение безопасности персональных данных достигается, в частности определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных, т.е. разработкой модели угроз. Основными группами угроз, на противостояние которым направлены цели и требования безопасности, являются:

1.Угрозы, связанные с осуществлением несанкционированного доступа (ознакомления) с информацией, содержащей сведения о кредитных историях, при ее обработке и хранении.

2.Угрозы, связанные с несанкционированным копированием (хищением) информации, содержащей сведения о кредитных историях (том числе БД кредитных историй в целом).

3.Угрозы, связанные с осуществлением доступа к информации, содержащей сведения о кредитных историях, без разрешения на то ее владельца (субъекта кредитной истории).

4.Угрозы, связанные с нарушением доступности информации, содержащей сведения о кредитных историях, передаваемой заинтересованным лицам.

5.Угрозы, связанные с перехватом информации, содержащей сведения о кредитных историях, из каналов передачи данных с использованием специализированных программно-технических средств.

6.Угрозы, связанные с потерей (утратой) информации, содержащей сведения о кредитных историях, вследствие сбоев (отказов) программного и аппаратного обеспечения.

7.Угрозы, связанные с нарушением согласованности данных, принимаемых от источников кредитных историй, помещаемых в БД кредитных историй и выдаваемых в Центральный Каталог Кредитных Историй, а также помещаемых в дополнительную часть кредитной истории (в случае обновления кредитной истории).

8.Угрозы, связанные с отрицанием фактов отправления запросов на получение кредитных историй и фактов получения кредитных отчетов.

9.Угрозы, связанные с внедрением компьютерных вирусов и другого вредоносного программного обеспечения.

10.Угрозы, связанные с осуществление несанкционированных информационных воздействий (направленных на «отказ в обслуживании» для сервисов, модификацию конфигурационных данных программно-аппаратных средств, подбор аутентификационной информации и т.п.). Модель угроз является обязательным пунктом в построении системы защиты информации. Данная мера необходима для выявления слабых мест АС БКИ, эффективной постановки задачи. Из вышеперечисленного списка угроз можно сделать вывод, что основными направлениями разработки системы защиты информации будут защита от НСД при приеме, передачи и хранении конфиденциальной информации.

1.8 Методы и средства защиты информации

Можно выделить основные принципы создания СЗИ:

1.Системный подход к построению системы защиты информации, такой подход включает в себя оптимальное сочетание программных, аппаратных, физических и других средств защиты.

2.Принцип постоянного развития системы. Этот принцип является одним из основных в организации системы защиты информации. Способы взлома конфиденциальной информации постоянно развиваются, поэтому обеспечение защищенности информационной системы не может быть статическим. Это динамический процесс, который заключается в анализе и реализации наиболее рациональных методов, способов и путей преобразования системы защиты.

3.Разделение и сведение полномочий по доступу к защищаемой информации к минимуму.

4.Полный контроль и регистрация попыток НСД. Необходимость идентификация и аутентификация каждого пользователяи контролирование его действий с последующим отмечанием фактов совершения различных действий в специализированных журналах. Также ограничение по совершению какого-либо действия в информационной системе без его предварительной регистрации.

5.Обеспечение надежности системы защиты, то есть невозможность снижения уровня надежности при возникновении в системе сбоев, отказов, преднамеренных действий взломщика или непреднамеренных ошибок пользователей.

6.Контроль за корректной работой системы.

7.Обеспечение экономического обоснования использования системы. Это выражается в том, что возможный ущерб от несанкционированного доступа к конфиденциальной информации в ходе реализации угроз значительно превышает над стоимостью разработки и эксплуатации СЗИ. Подводя итог, можно сказать, что построение СЗИ достаточно долгий и трудоемкий процесс. Необходимо учитывать множество аспектов при разработке и реализации системы. Это и правовые нормы, обусловленные законодательством РФ, и экономические аспекты

непосредственно предприятия, для которого разрабатывается система.Так же не стоит забывать и об используемых средствах защиты конфиденциальной информации. Они должны быть обязательно сертифицированы и разработаны только органами, имеющими лицензию на данный вид деятельности. Сертифицированы и разработаны только органами, имеющими лицензию на данный вид деятельности.

Рис. 1.1 Схема организации

СЗИНа рис.1 представлена схема взаимодействия компонентов СЗИ. Можно сделать вывод, что такая система всегда находится в динамическом состоянии.