Учреждение образования

«Белорусский государственный технологический университет»

Кафедра информационных систем и технологий

**«Отчёт по лабораторной работе №1»**

«Разработка и внедрение политики безопасности организации или учреждения»

Выполнил: студент 3 курса

4 группы специальности ПОИТ

Супрунюк Евгений Андреевич

Проверил: преподаватель

Сазонова Дарья Владимировна

Минск 2023

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

**Теоретическое введение**

Основой мер **административного уровня,** то есть мер, предпринимаемых руководством организации, является политика безопасности.

Под **политикой безопасности** понимается совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов.

Политика безопасности определяет стратегию организации в области информационной безопасности, а также ту меру внимания и количество ресурсов, которую руководство считает целесообразным выделить.

Определение политики ИБ должно сводиться к следующим практическим шагам:

1. Определение используемых руководящих документов и стандартов в области ИБ, а также основных положений политики ИБ, включая:

• управление доступом к средствам вычислительной техники, программа и данным;

• антивирусную защиту;

• вопросы резервного копирования;

• проведение ремонтных и восстановительных работ;

• информирование об инцидентах в области ИБ.

2. Определение подходов к управлению рисками: является ли достаточным базовый уровень защищенности или требуется проводить полный вариант анализа рисков.

3. Структуризация контрмер по уровням.

4. Порядок сертификации на соответствие стандартам в области ИБ. Должна быть определена периодичность проведения совещаний по тематике ИБ на уровне руководства, включая периодический пересмотр положений политики ИБ, а также порядок обучения всех категорий пользователей информационной системы по вопросам ИБ.

Для построения системы защиты информации необходимо определить границы системы, для которой должен быть обеспечен режим информационной безопасности. Соответственно система управления информационной безопасности (система защиты информации) должна строиться именно в этих границах.

Описание границ системы, для которой должен быть обеспечен режим информационной безопасности, рекомендуется выполнять по следующему плану.

1. Структура организации. Описание существующей структуры и изменений, которые предполагается внести в связи с разработкой или модернизации автоматизированной системы обработки информации.

2. Размещение средств вычислительной техники и поддерживающей инфраструктуры. Модель иерархии средств вычислительной техники.

3. Ресурсы информационной системы, подлежащие защите. Рекомендуется рассмотреть ресурсы автоматизированной системы следующих классов: средства вычислительной техники, данные, системное и прикладное программное обеспечение. Все ресурсы представляют ценность с точки зрения организации. Для их оценки должна быть выбрана система критериев и методология оценок по этим критериям.

4. Технология обработки информации и решаемые задачи. Для решаемых задач должны быть построены модели обработки информации в терминах ресурсов.

В результате должен быть составлен документ, в котором:

• зафиксированы границы и структура системы;

• перечислены ресурсы, подлежащие защите;

• дана система критериев для оценки их ценности.

Минимальным требованиям к режиму информационной безопасности соответствует базовый уровень. Обычной областью использования этого уровня являются типовые проектные решения. Существует ряд стандартов и спецификаций, в которых рассматривается минимальный (типовой) набор наиболее вероятных угроз, таких как вирусы, сбои оборудования, несанкционированный доступ и т.д. Для нейтрализации этих угроз обязательно должны быть приняты контрмеры вне зависимости от вероятности осуществления угроз и уязвимости ресурсов. Таким образом, характеристики угроз на базовом уровне рассматривать не обязательно.

В случае, когда нарушения информационной безопасности чреваты тяжелыми последствиями, базовый уровень требований к режиму информационной безопасности является недостаточным. Для того, чтобы сформулировать дополнительные требования, необходимо:

• определить ценность ресурсов;

• к стандартному набору добавить список угроз, актуальных для исследуемой информационной системы;

• оценить вероятности угроз;

• определить уровень уязвимости ресурсов.

Политика безопасности строится на основе анализа рисков, которые признаются реальными для информационной системы организации. Когда риски проанализированы, стратегия защиты определена, тогда составляется программа, реализация которой должна обеспечить информационную безопасность. Под эту программу выделяются ресурсы, назначаются ответственные, определяется порядок контроля выполнения программы и т.п.

Существуют различные подходы к оценке рисков. Выбор подхода зависит от уровня требований, предъявляемых в организации к режиму информационной безопасности, характера принимаемых во внимание угроз (спектра воздействия угроз) и эффективности потенциальных контрмер.

Процесс оценивая рисков содержит несколько этапов.

1. Идентификация ресурса и оценивание его количественных показателей (определение негативного воздействия).

2. Оценивание угроз.

3. Оценивание уязвимостей.

4. Оценивание существующих и предполагаемых средств обеспечения.

5. Оценивание рисков.

На основании оценивания рисков выбираются средства, обеспечивающие режим ИБ. Ресурсы, значимые для нормальной работы организации и имеющие определенную степень уязвимости, считаются подверженными риску, если по отношению к ним существует какая либо угроза. При оценивании рисков учитываются потенциальные негативные воздействия от нежелательных происшествий и показатели значимости рассматриваемых уязвимостей и угроз для этих ресурсов.

Риск характеризует опасность, которой может подвергаться система и использующая ее организация. Риск зависит от показателей ценности ресурсов, вероятности реализации угроз для ресурсов и степени легкости, с которой уязвимости могут быть использованы при существующих или планируемых средствах обеспечения информационной безопасности.

Цель оценивания рисков состоит в определении характеристик рисков для информационной системы и ее ресурсов. На основе таких данных могут быть выбраны необходимые средства управления ИБ.

При оценивании рисков учитывается:

• ценность ресурсов;

• оценка значимости угроз;

• эффективность существующих и планируемых средств защиты.

Показатели ресурсов или потенциальное негативное воздействие на деятельность организации можно определять несколькими способами:

• количественными (например, стоимостные);

• качественными (могут быть построены на использовании таких понятий, как, умеренный или чрезвычайно опасный);

• их комбинацией.

Для того, чтобы конкретизировать определение вероятности в течение которого предполагается защитить ресурс. Вероятность того, что угроза реализуется, определяется следующими факторами:

• привлекательность ресурса как показатель при рассмотрении угрозы от умышленного воздействия со стороны человека;

• возможность использования ресурса для получения дохода как показатель при рассмотрении угрозы от умышленного воздействия со стороны человека;

• технические возможности угрозы, используемые при умышленном воздействии со стороны человека;

• вероятность того, что угроза реализуется;

• степень легкости, с которой уязвимость может быть использована.

Вопрос о том, как провести границу между допустимыми и недопустимыми рисками, решается пользователем. Очевидно, что разработка политики безопасности требует учета специфики конкретных организаций.

На основании политики безопасности строится программа безопасности, которая реализуется на процедурном и программно техническом уровнях уровне.

К **процедурному уровню** относятся меры безопасности, реализуемые людьми.

Можно выделить следующие группы процедурных мер:

• управление персоналом;

• физическая защита;

• поддержание работоспособности;

• реагирование на нарушения режима безопасности;

• планирование восстановительных работ.

Управление персоналом заключается в выполнении следующих условий. Во-первых, для каждой должности существовать квалификационные требования по ИБ. Во-вторых, в должностные инструкции должны входить разделы, касающиеся информационной безопасности. В-третьих, каждого работника нужно научить мерам безопасности теоретически и на практике.

Меры физической защиты включают в себя защиту от утечки информации по техническим каналам, инженерные способы защиты и т.д.

Планирование восстановительных работ предполагает:

• слаженность действий персонала во время и после аварии;

• наличие заранее подготовленных резервных производственных площадок;

• официально утвержденную схему переноса на резервные площадки основных информационных ресурсов;

• схему возвращения к нормальному режиму работы.

Поддержание работоспособности включает в себя создание инфраструктуры, включающий в себя как технические, так и процедурные регуляторы и способной обеспечить любой наперед заданный уровень работоспособности на всем протяжении жизненного цикла информационной системы.

Реагирование на нарушение режима безопасности может быть регламентировано в рамках отдельно взятой организации. В настоящее время, осуществляется только мониторинг компьютерных преступлений в национальном масштабе и на мировом уровне.

Основой **программно-технического уровня** являются следующие механизмы безопасности:

• идентификация и аутентификация пользователей;

• управление доступом;

• протоколирование и аудит;

• криптография;

• экранирование;

• обеспечение высокой доступности и т.д.

Важно управлять информационной системой в целом и механизмами безопасности в особенности. Упомянутые меры безопасности должны опираться на общепринятые стандарты, быть устойчивым к сетевым угрозам, учитывать специфику отдельных сервисов.

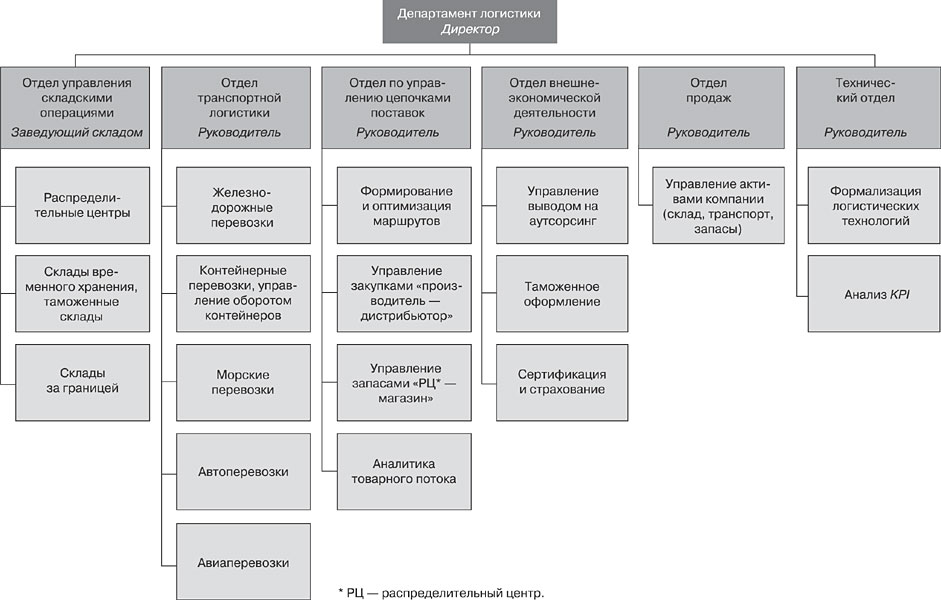


Рис. Структура логистической компании.

Организационная структура компании состоит из следующих основных лиц (отделов):

* Отдел управления складскими операциями;
* Отдел транспортной логистики;
* Отдел по управлению цепочками поставок;
* Отдел внешнеэкономической деятельности;
* Отдел продаж;
* Технический отдел.

Таким образом, вся деятельность компании, связанная с реализацией проектов, сосредоточена в этих 6 отделах.

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

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

**Оценка рисков**

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

* Антропогенные;
* Техногенные;
* Естественные (природные).

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

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

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

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

Источниками внутренних угроз являются:

* Сотрудники организации;
* Программное обеспечение;
* Аппаратные средства.

К информационным угрозам относятся:

* Несанкционированный доступ к информационным ресурсам;
* Незаконное копирование данных в информационных системах;
* Противозаконный сбор и использование информации;
* Использование информационного оружия.

К программным угрозам относятся:

* Использование ошибок и «дыр» в программном обеспечении;
* Компьютерные вирусы и вредоносные программы.

К физическим угрозам относятся:

* Уничтожение или разрушение средств обработки информации и связи.

**Возможные угрозы**: получение доступа к конфиденциальным данным (данные клиентов, данные сотрудников, маршруты доставки товаров и время доставок, данные складов и товаров), нарушение работоспособности систем компании (контроль доставок).

**Разработка мер защиты**

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

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

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

* Установление особого режима конфиденциальности;
* Ограничение доступа к конфиденциальной информации;
* Использование организационных мер и технических средств защиты информации;
* Осуществление контроля за соблюдением установленного режима конфиденциальности.

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

* Организацию охраны помещений, в которых содержатся носители конфиденциальной информации;
* Установление режима работы в помещениях, в которых содержатся носители конфиденциальной информации;
* Установление пропускного режима в помещениях, содержащих носителей конфиденциальной информации;
* Закрепление технических средств обработки конфиденциальной информации за сотрудниками, определение персональной ответственности за их сохранность;
* Установление порядка пользования носителями конфиденциальной информации (учет, хранение, передача другим должностным лицам, уничтожение, отчетность);
* Организацию ремонта технических средств обработки конфиденциальной информации;
* Организацию контроля за установленным порядком.

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

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

Радикальным способом защиты информации от утечки по физическим полям является электромагнитное экранирование технических устройств и помещений, однако это способ требует значительных капитальных затрат и практически не применяется.

Обеспечение требуемой защиты информационных ресурсов предприятий в этих условиях достигается применением дополнительных инструментальных средств. К их числу относятся средства анализа защищенности ОС и средства обнаружения опасных информационных воздействий в сетях.

Средства анализа защищенности операционных систем позволяют осуществлять ревизию механизмов разграничения доступа, идентификации и аутентификации, средств мониторинга, аудита и других компонентов операционных систем с точки зрения соответствия их настроек и конфигурации установленным в организации. Кроме этого, средствами данного класса проводится контроль целостности и неизменности программных средств и системных установок, и проверка наличия уязвимостей системных и прикладных служб. Как правило, такие проверки проводятся с использованием базы данных уязвимостей операционных систем и сервисных служб, которые могут обновляться по мере выявления новых уязвимостей.

В информационной сфере с целью нейтрализации внутренних источников угроз национальной безопасности совершенствуются механизмы реализации прав граждан на получение, хранение, пользование и распоряжение информацией, в том числе с использованием современных информационно-коммуникационных технологий. Государство гарантирует обеспечение установленного законодательством порядка доступа к государственным информационным ресурсам, в том числе удаленного, и возможностям получения информационных услуг. Значимым этапом станет разработка и реализация стратегии всеобъемлющей информатизации, ориентированной на развитие электронной системы осуществления административных процедур, оказываемых гражданам и бизнесу государственными органами и иными организациями, и переход государственного аппарата на работу по принципу информационного взаимодействия. Ускоренными темпами будет развиваться индустрия информационных и телекоммуникационных технологий. Особое внимание будет уделяться последовательному повышению качества, объема и конкурентоспособности национального контента, который призван занимать доминирующее положение внутри страны, и его продвижению во внешнее информационное пространство.

Приоритетным направлением является совершенствование нормативной правовой базы обеспечения информационной безопасности и завершение формирования комплексной государственной системы обеспечения информационной безопасности, в том числе путем оптимизации механизмов государственного регулирования деятельности в этой сфере. При этом важное значение отводится наращиванию деятельности правоохранительных органов по предупреждению, выявлению и пресечению преступлений против информационной безопасности, а также надежному обеспечению безопасности информации, охраняемой в соответствии с законодательством. Активно продолжится разработка и внедрение современных методов и средств защиты информации в информационных системах, используемых в инфраструктуре, являющейся жизненно важной для страны, отказ или разрушение которой может оказать существенное отрицательное воздействие на национальную безопасность.

Специалисты компании IBM выделяют четыре основных этапа построения системы безопасности:

* Идентификация информационных рисков и методов борьбы с ними;
* Описание мер защиты активов в соответствии с задачами и целями компании;
* Описание действий при происшествиях;
* Анализ остаточных рисков и принятие решения о дополнительном капиталовложении в методы обеспечения безопасности.

Ответ на вопрос «Что нужно защищать?» - основной аспект политики информационной безопасности, в соответствии со стратегией IBM. Политика должна создаваться с целью минимальных её изменений в будущем. Эффективная политика безопасности должна содержать:

* Цели и задачи обеспечения информационной безопасности;
* Взаимодействие со стандартами безопасности и законодательством;
* Расширение и ликвидация вирусных атак;
* Обеспечение непрерывности деятельности.

Далее идет процесс создания документации, которая содержит правила анализа рисков компании, описание рекомендуемых методов и средств защиты и так далее. Документация может подлежать изменениям в соответствии с актуальными уязвимостями и угрозами.

Однако, помимо правовой основы, система информационной безопасности и её функции по обеспечению состоянию защищенности объекта должны быть реализованы в соответствии с нижеизложенными принципами:

* Комплексность (разрабатываемая система защиты предусматривает комплексную реализацию методов, обеспечивает защиту информационных ресурсов на техническом и организационном уровнях и предотвращает возможные пути реализации угроз);
* Легитимность (создание системы информационной безопасности, а также реализация мероприятий по защите, не противоречащих законодательству и нормативам);
* Прогрессивность (подразумевает непрерывное развитие средств и методов защиты, в соответствии с развитием технологий и методов атак);
* Постоянность (обеспечивает непрерывную защиту объектов);
* Рациональность (использование экономически выгодных и эффективных средств защиты);
* Ответственность (каждый сотрудник ручается за обеспечение безопасности в рамках своих полномочий);
* Контроль (предполагает постоянных контроль над обеспечением защиты и своевременное выявление угроз);
* Этапность (проектирование системы безопасности делается поэтапно).

Проанализировав существующие политики и стандарты информационной безопасности можно утверждать, что для обеспечения надлежащего уровня информационной защиты требуется комплекс мер, включающий в себя функции программного обеспечения, политики безопасности, методы и организационные структуры. В соответствии с этим и с основной целью необходимо выполнить следующие задачи:

* Изучить исходную информационную и организационную структуру военкомата;
* По результатам анализа исходной информационной системы определить конкретные угрозы и уязвимости информационной безопасности;
* Определить уровень и класс исходной защищенности объекта;
* Выявить актуальные угрозы;
* Составить модель нарушителя;
* Сопоставить исходную систему с требованиями стандартов безопасности;
* Разработать политику безопасности.

Выполнение вышеизложенных целей и задач позволит создать эффективную систему информационной безопасности предприятия, отвечающую требованиям законодательства и стандартам информационной безопасности.

Наибольшая эффективность защиты информации достигается при комплексном использовании средств анализа защищенности и средств обнаружения опасных информационных воздействий (атак) в сетях. Средства обнаружения атак в сетях предназначены для осуществления контроля всего сетевого трафика, который проходит через защищаемый сегмент сети, и оперативного реагирование в случаях нападения на узлы корпоративной сети. Большинство средств данной группы при обнаружении атаки в сети оповещают администратора системы, регистрируют факт нападения в журнале системы и завершают соединение с атакующим узлом. Дополнительно, отдельные средства обнаружения атак позволяют автоматически реконфигурировать межсетевые экраны и маршрутизаторы в случае нападения на узлы корпоративной сети.

В информационной сфере с целью нейтрализации внутренних источников угроз национальной безопасности совершенствуются механизмы реализации прав граждан на получение, хранение, пользование и распоряжение информацией, в том числе с использованием современных информационно-коммуникационных технологий. Государство гарантирует обеспечение установленного законодательством порядка доступа к государственным информационным ресурсам, в том числе удаленного, и возможностям получения информационных услуг. Значимым этапом станет разработка и реализация стратегии всеобъемлющей информатизации, ориентированной на развитие электронной системы осуществления административных процедур, оказываемых гражданам и бизнесу государственными органами и иными организациями, и переход государственного аппарата на работу по принципу информационного взаимодействия. Ускоренными темпами будет развиваться индустрия информационных и телекоммуникационных технологий. Особое внимание будет уделяться последовательному повышению качества, объема и конкурентоспособности национального контента, который призван занимать доминирующее положение внутри страны, и его продвижению во внешнее информационное пространство.

Приоритетным направлением является совершенствование нормативной правовой базы обеспечения информационной безопасности и завершение формирования комплексной государственной системы обеспечения информационной безопасности, в том числе путем оптимизации механизмов государственного регулирования деятельности в этой сфере. При этом важное значение отводится наращиванию деятельности правоохранительных органов по предупреждению, выявлению и пресечению преступлений против информационной безопасности, а также надежному обеспечению безопасности информации, охраняемой в соответствии с законодательством. Активно продолжится разработка и внедрение современных методов и средств защиты информации в информационных системах, используемых в инфраструктуре, являющейся жизненно важной для страны, отказ или разрушение которой может оказать существенное отрицательное воздействие на национальную безопасность.

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

Целями защиты информации являются:

* Предотвращение утечки, хищения, утраты, искажения, подделки информации;
* Предотвращение несанкционированных действий по уничтожению, модификации, копированию информации;
* Предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы.

**Возможные меры защиты**: ограничение доступа к информации для сотрудников компании по уровням, установка систем защиты на информационные системы компании (использование антивирусов, систем резервного копирования информации, надёжных программ для обмена информацией), наличие запасных средств связи, проведение проверок сотрудников на возможные утечки данных.

**Вывод**

Важно помнить, что прежде, чем внедрять какие-либо решения по защите информации необходимо разработать политику безопасности, адекватную целям и задачам современного предприятия. В частности, политика безопасности должна описывать порядок предоставления и использования прав доступа пользователей, а также требования отчетности пользователей за свои действия в вопросах безопасности. Система информационной безопасности окажется эффективной, если она будет надежно поддерживать выполнение правил политики безопасности, и наоборот.

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

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

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