БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

**Лабораторная работа №1**

**«Разработка и внедрение политики безопасности**

**организации или учреждения**»

**Выполнила:**

студентка 3 курса 1 группы

Потапейко Полина Павловна

**Проверил:**

Берников Владислав Олегович

Минск 2021

**Актуальность, цели и задачи разработки ПИБ в организации**

Политика информационной безопасности для логистических компаний в наше время является очень актуальной. Связано это с тем, что логистические компании играют важную роль в экономике как отдельных бизнес-компаний, так и в экономике страны в целом, поэтому являются важным звеном, и безопасность таких компаний нужно поддерживать на высоком уровне.

Сперва при разработке ПИБ необходимо определиться с целями и задачами разработки этой самой ПИБ.

К целям разработки ПИБ относятся:

* постоянная аутентификация и авторизация персонала;
* конфиденциальность данных субъектов компании;
* надежность системы хранения данных;
* обеспечение целостности данных.

К задачам разработки ПИБ можно отнести:

* защита от несанкционированного доступа в информационную среду компании;
* защита от утечки данных;
* минимизация ущерба от информационных атак на логистическую компанию;
* обеспечение аутентификации пользователей.

Далее для разработки политики информационной безопасности необходимо найти различную информацию об источниках угроз, урон, которые эти угрозы могут нанести, риски, которые могут быть при появлении этих угроз. Также необходимо изучить структуру логистической компании, чтобы обозначить определенные, конкретные объекты защиты, на которые необходимо уделить больше внимания, так как именно эти объекты несут наиболее важную ценность для этой организации.

В конце концов необходимо разработать меры, методы политики безопасности, которые позволят контролировать или предотвратить появление угроз. Для этого необходимо продумать все технические, программные, организационные, правовые аспекты безопасности. Каждые из этих аспектов позволят обезопасить организацию с разных сторон от различных угроз, что в итоге хорошо скажется на самой организации.

Рассмотрим каждую из глав политики безопасности по отдельности.

**Объекты защиты**

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

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

Составляющими организационных структур являются:

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

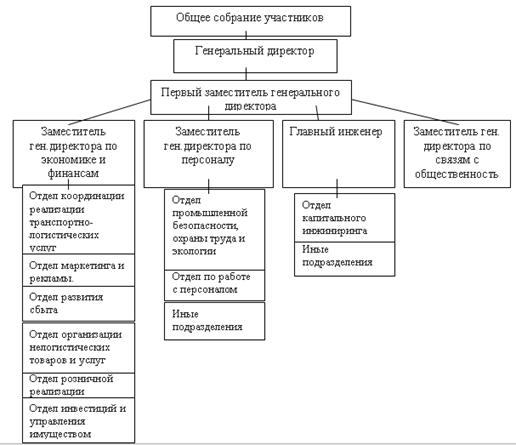


Рисунок 1 – Организационная структура логистической компании

Организационная структура логистической компании – внутренняя организация работы, с помощью которой структурируются и формализуются подходы и методы управления, определяются группы исполнителей, разрабатываются системы контроля и внутриорганизационных взаимоотношений.

С помощью организационной структуры осуществляются все необходимые действия, направленные на достижение целей, которые ставит перед собой логистическая компания.

Таблица 1 – Штатное расписание логистической компании

|  |  |
| --- | --- |
| Наименование должности | Количество должностных единиц |
| 1. Генеральный директор | 1 |
| 2. Первый заместитель генерального директора | 1 |
| 3. Заместитель ген. директора по экономике и финансам | 1 |
| 4. Заместитель ген. директора по персоналу | 1 |
| 5. Заместитель ген. директора по связям с общественностью | 1 |
| 6. Начальник отдела | 9 |
| 7. Главный инженер | 1 |
| 8. Менеджер | 7 |
| 9. Бухгалтер | 2 |
| 10. Диспетчер | 2 |
| 11. Логист | 3 |
| 12. Агент | 3 |
| 13. Водитель | 7 |
| 14. Ревизор автотранспорта | 2 |
| 15. Экспедитор | 2 |
| Итого | 43 |

Существует несколько моделей организационных структур, которые используют логистические компании.

Механистическая структура наиболее традиционная. Каждое отдельное управление специализируется на своем круге задач. Механистические структуры бывают двух видов:

1. Функциональные (или линейно-функциональные) подразделения создаются для решения определенных задач. При такой структуре в крупных логистических компаниях создается вертикальная иерархия управлений, которые делятся на отделы. Функциональное деление чаще всего используется небольшими и средними логистическими компаниями. В его основе –разделение структур по задачам. Например, создаются отдел розничной реализации, маркетинга и рекламы, отдел развития сбыта и т. п.

2. Дивизионная структура, при которой деление организации ориентировано на потребителя, продукт или регион. В обязанности сотрудников соответствующих управлений входит полное обслуживание клиентов по всем видам оказываемых логистической компанией услуг. Они обязаны уметь объяснить правила предоставления услуг и дать свои рекомендации.

Внедрение системы управления рисками нарушения ИБ в логистической компании связано с решением определённых задач:

* выстраивание эффективного процесса управления рисками;
* подбор персонала (оценщиков рисков), обладающего необходимой квалификацией и опытом;
* взаимодействие с бизнес-подразделениями;
* определение (выбор) методики, по которой будет проводиться оценка.

Управление рисками нарушения ИБ включает в себя: определение области оценки рисков, их оценку и обработку, мониторинг и контроль, совершенствование. Это полностью соответствует модели Деминга (см. Схему 1) «планирование – реализация – проверка – совершенствование», которая является основой модели менеджмента стандартов качества.

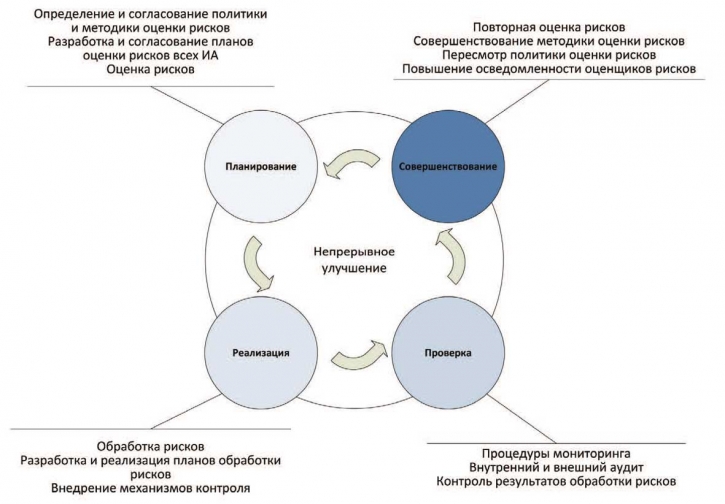


Рисунок 2 – Модель деминга применительно к процессу управления рисками

Политика оценки рисков должна:

* определять механизмы контроля и роли, задействованные в данном процессе, при этом, для предотвращения конфликта интересов, подразделения, осуществляющие контроль обработки рисков, должны быть максимально независимы от подразделений, выполняющих оценку рисков;
* закреплять процедуры обратной связи между всеми участниками процесса управления рисками и порядок планирования процесса;
* формулировать порядок документирования результатов оценки рисков и результатов обработки рисков.

Контроль результатов обработки рисков должен охватывать все этапы и сопоставлять результаты обработки рисков с результатами, полученными от подразделений, занимающихся мониторингом информационной безопасности.

Определение, анализ и изменение бизнес-процессов — стартовый этап управления рисками.

Целью данного этапа являются формализация и детальное описание всех бизнес-процессов, определение критичных бизнес-процессов с позиций максимального ущерба логистической компании в случае их нарушения, а также специфических требований законодательства и стандартов.

На данном этапе задействованы как сотрудники службы информационной безопасности, так и представители бизнес-подразделений, службы внутреннего контроля и юридической службы. Результатом является документирование информационных потоков, определение состава информации в каждом отдельном бизнес-процессе, а также дополнительных признаков информационных активов, таких как критичность процесса для непрерывности бизнеса, обработка инсайдерской информации.

После обработки недопустимых рисков в случае принятия решения о внесении изменений в бизнес-процессы, например, внедрения новых документов (таких как согласие на обработку персональных данных (далее – ПДн), уведомление о включении лица в список инсайдеров и т.д.), все изменения должны быть утверждены руководством, а этап Р0 – проведен заново.

На основании результатов этапа Р0 можно приступать к подготовке полного перечня информационных активов.

Документирование информационных активов.

Для подготовки такого перечня необходимо идентифицировать информационные активы и классифицировать их типы.

Информация, относящаяся к каждому из типов информационных активов, документируется в перечне сведений конфиденциального характера (ограниченного доступа).

Информационный актив – это информация:

* с реквизитами, позволяющими её идентифицировать;
* имеющая ценность для самой компании;
* находящаяся в распоряжении и представленная на любом материальном носителе в форме, пригодной для её обработки, хранения или передачи.

Важными элементами этапа являются разработка техническо-рабочей документации:

* технических паспортов на все информационные системы с отражением основных технических средств, программных средств и средств защиты;
* матриц доступа и т.д.

После составления перечня информационных активов, обрабатываемых в информационных системах, можно переходить к следующему этапу.

Информационные активы логистической компании рассматриваются относительно информационных систем, в которых происходит обработка данных активов, в совокупности с соответствующими объектами среды. При этом обеспечение свойств ИБ для информационных активов выражается в создании необходимой защиты соответствующих им объектов среды в разрезе каждой информационной системы.

Для разных типов активов устанавливаются разные требования к информационной безопасности, в том числе с учётом действующего законодательства.

**Оценка угроз, рисков и уязвимостей.**

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.

К программным угрозам относятся:

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

К физическим угрозам относится уничтожение или разрушение средств обработки информации и связи.

Включая в оценку величину ущерба от угрозы, необходимо так же учитывать вероятность реализации какого-либо ущерба. Данная вероятность зависит от различных факторов:

* выгода от совершения атаки;
* техническая возможность угрозы;
* сложность совершения атаки.

Список угроз может меняться и пополняться по мере развития технической оснащенности потенциальных злоумышленников.

Среди основных типов угроз информационной безопасности логистической компании:

* непреднамеренные, случайные, вызванные ленью или халатностью нарушения установленных регламентов, которые приводят к сбоям в работе системы, нелогичному и нерациональному использованию человеческих и системных ресурсов;
* преднамеренные, вызванные третьими лицами – сотрудниками логистической компании, проникающими в систему защиты компании с целью уничтожения, хищения или разглашения информации, совершения преступлений криминального характера;
* деятельность местных или иностранных криминальных группировок, направленная на добычу информации, уничтожение информационных систем;
* ошибки разработчиков программного обеспечения, авторов системных конфигураций;
* аварии, стихийные бедствия, иные воздействия, имеющие природный или техногенный характер.

При этом наиболее катастрофичными результатами конфигурации угроз становятся:

* нарушение целостности информационных баз, программных ресурсов, фальсификация информации, являющейся основанием для принятия системных решений;
* утечка информации, относящейся к категории охраняемой.

Современные методики очень подробны, содержат громоздкие формулы, используют экспертные оценки, но, к сожалению, не всегда подходят для практической работы из-за трудностей представления руководству результатов оценки рисков.

Главное требование к методике – она должна быть наглядной, охватывающей всю ИТ-инфраструктуру и все бизнес-процессы компании, утвержденной руководством и согласованной с подразделениями, занимающимися оценкой операционных рисков. Следовательно, при выборе методики необходимо убедиться, что методика и ожидаемые результаты устраивают все стороны – и того, кто считает риски (т.е. показывает объективную картину состояния ИБ), и того, кому их демонстрируют (т.е. согласована с операционными рисками и утверждена руководством).

Методика оценки рисков нарушения ИБ, подход к оценке рисков нарушения ИБ компании должны определять способ и порядок качественного или количественного оценивания риска нарушения ИБ. То есть для оценки рисков нарушения ИБ должна использоваться качественная и (или) количественная (выраженная в процентах или деньгах) шкала. Количественные шкалы позволяют сделать результаты оценки рисков более точными, при этом требуя более высокого уровня зрелости существующей СМИБ.

Для управления рисками в методике должен быть закреплен порядок их обработки.

Одним из способов определения очередности является установление приоритетов рисков, которые зависят от критичности обрабатываемого информационного актива, дополнительных признаков информационных активов, опасности конкретной угрозы в конкретной системе.

На основе определенных приоритетов и результатов оценки рисков можно построить карту рисков.

По результатам оценки рисков подготавливается отчёт о проведении оценки рисков нарушения информационной безопасности с указанием количества оценённых рисков, количественных и качественных оценок, детализацией всех недопустимых рисков и рекомендациями по их обработке.

Целью обработки недопустимых рисков является значительное уменьшение рисков при относительно низких затратах и поддержание принятых рисков на допустимом, низком уровне. По результатам оценки рисков определяется способ обработки каждого из них, являющегося недопустимым.

Возможными вариантами обработки рисков являются:

* применение защитных мер, позволяющих снизить величину риска до допустимого уровня;
* уход от риска (например, путем отказа от деятельности, выполнение которой приводит к появлению риска, или изменения бизнес-процессов);
* перенос риска на другие организации;
* осознанное принятие риска (решение должно приниматься руководством).

Решение о применении того или иного способа обработки рисков принимается, исходя из стоимости их реализации, а также ожидаемых выгод от их реализации.

Порядок обработки рисков информационных систем определяется приоритетом риска нарушения ИБ. Так, риски с наивысшим приоритетом должны быть обработаны в первую очередь.

Система управления рисками нарушения ИБ даёт существенный положительный эффект при выстраивании СОИБ, выявлении уязвимостей ИБ и обосновании затрат на информационную безопасность, гарантируя принятие взвешенных решений в области СМИБ и контроль эффективности принятых при обработке рисков решений.

Для изучения рисков необходимо создать несколько таблиц, иллюстрирующие различные метрики, использующиеся при оценке. Первой создадим таблицу для оценки ущерба логистической компании от несанкционированного доступа (таблица 4).

Таблица 4 – Условная численная шкала для оценки ущерба банку от НСД

|  |  |
| --- | --- |
| Величина ущерба | Описание |
| 0 | Ущерб ничтожен |
| 1 | Утечка информации не принесет значительного ущерба |
| 2 | Выполнение задач прерывается на короткий промежуток времени, однако ущерб от такого отключения минимален |
| 3 | Значительные потери в прибыли |
| 4 | Критические потери, компании необходимы крупные займы, и он теряет позиции на рынке |
| 5 | Логистическая компания прекращает существование |

Составим таблицу вероятности того, что угроза будет реализована (таблица 5).

Таблица 5 – Вероятностно-временная шкала реализации несанкционированного доступа к информационным ресурсам

|  |  |
| --- | --- |
| Вероятность события | Средняя частота события (НСД) |
| 0 | Данный вид атаки отсутствует |
| 0,1 | Реже, чем раз в год |
| 0,2 | Около 1 раза в год |
| 0,3 | Около 1 раза в месяц |
| 0,4 | Около 1 раза в неделю |
| 0,5 | Ежедневно |

Используя приведенные выше таблицы, можно составить таблицу рисков (таблица 6). Изначально максимально допустимым порогом задается значение 0.5. Если в итоге какая-либо из атак превысит данный порог, необходимо в первую очередь разработать политику безопасности от данного вида атак.

Таблица6–Оценка риска

|  |  |  |  |
| --- | --- | --- | --- |
| Описание атаки | Ущерб | Вероятность | Риск (Ущерб \* Вероятность) |
| Спам | 1 | 0,4 | 0,4 |
| Кража данных с помощью живого доступа к серверам | 2 | 0,1 | 0,2 |
| Кража данных путем атаки на сервера | 4 | 0,1 | 0,4 |
| DDoS-атаки на сервера | 2 | 0,2 | 0,6 |
| Ограбление офисов логистической компании | 4 | 0,1 | 0,4 |
| Итого | 13 | 0,9 | 2,0 |

Если интегральный риск превысит допустимый уровень, значит необходимо решать ряд мелких проблем комплексно.

**Меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов**

К основным мерам обеспечения информационной безопасности относятся:

* криптографическая защита данных;
* обнаружение атак и защита от них;
* разграничение доступа к информационным системам;
* применение для защиты информационных систем межсетевых экранов;
* антивирусная защита файлов;
* резервное копирование данных и приложений;
* защита от утечек данных;
* протоколирование и аудит;
* защита данных, передаваемых по проводным и беспроводным информационным сетям;
* вооруженная охрана.

Криптография изучает безопасные методы связи па основе математических методов преобразования информации, создания устойчивых к взлому шифров. Задачи, связанные со взломом шифров, решаются методами криптоанализа.

Атаки на информационные системы — это преднамеренные действия, использующие слабые места и уязвимости информационных систем, которые приводят к нарушению их доступности, устойчивости и конфиденциальности обрабатываемой информационной системой информации. К наиболее опасным видам атак относятся DoS- и DDoS-атаки.

Разграничение доступа предусматривает предоставление каждому зарегистрированному в информационной системе пользователю беспрепятственный доступ к информации, приложениям или модулям приложений в пределах его полномочий.

Всем сотрудникам логистической компании, в котором установлена система контроля доступа, выдаются специальные электронные пропуска, например, проксимити идентификаторы, 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.

Межсетевые экраны предназначены для проверки информации, которой информационные системы предприятия обмениваются с внешними по отношению к предприятию системами. Они либо пропускают эту информацию, либо отклоняют ее по критериям, но которым настроен межсетевой экран (брандмауэр). Реализуется экран с помощью программного или аппаратного обеспечения.

Антивирусное программное обеспечение, которое устанавливается на персональные вычислительные устройства пользователя (персональные компьютеры, планшетные компьютеры, смартфоны и др.), осуществляет проверку файлов и других объектов файловой системы на наличие вирусов и других вредоносных программ. В случае их обнаружения оно предпринимает действия, нейтрализующие негативное действие вредоносных программ.

Резервное копирование данных и приложений предназначено для создания резервных копий данных и приложений, для их восстановления в аварийных режимах работы.

Защита от утечек данных (DLP — data leak prevention, data loss prevention — предотвращение утечек данных) предназначена для защиты от утечек корпоративной информации. Реализуется посредством программных или программно-аппаратных средств. Для этого данные относятся к определенным категориям (общедоступная информация, персональные данные, данные, представляющие коммерческую тайну и др.). Данные каждой категории проверяются на соответствие заданным критериям. При соответствии заданным критериям разрешается передача данных, при несоответствии заданным критериям данные могут направляться па дополнительную проверку либо блокироваться.

Протоколирование — сбор и накопление информации о событиях информационной системы. Аудит осуществляет анализ накопленной информации, проводится оперативно или периодически.

Чаще всего специалисты по безопасности:

* разрабатывают внутреннюю документацию, которая устанавливает правила работы с компьютерной техникой и конфиденциальной информацией;
* проводят инструктаж и периодические проверки персонала; инициируют подписание дополнительных соглашений к трудовым договорам, где указана ответственность за разглашение или неправомерное использование сведений, ставших известных по работе;
* разграничивают зоны ответственности, чтобы исключить ситуации, когда массивы наиболее важных данных находятся в распоряжении одного из сотрудников; организуют работу в общих программах документооборота и следят, чтобы критически важные файлы не хранились вне сетевых дисков;
* внедряют программные продукты, которые защищают данные от копирования или уничтожения любым пользователем, в том числе топ-менеджментом организации;
* составляют планы восстановления системы на случай выхода из строя по любым причинам.

К техническим механизмам безопасности, направленных на предотвращение исполнения планов злоумышленников можно отнести:

* аутентификация пользователей;
* шифрование данных;
* использование высококвалифицированного персонала.

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

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

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

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

Обеспечение повышенных требований к ИБ предполагает соответствующие мероприятия на всех этапах жизненного цикла информационных технологий.

Планирование этих мероприятий производится по завершении этапа анализа рисков и выбора контрмер. Обязательной составной частью этих планов является периодическая проверка соответствия существующего режима ИБ политике безопасности, сертификация информационной системы (технологии) на соответствие требованиям определенного стандарта безопасности.

По завершении работ, можно будет определить меру гарантии безопасности информационной среды, основанную на оценке, с которой можно доверять информационной среде объекта. Данный подход предполагает, что большая гарантия следует из применения больших усилий при проведении оценки безопасности.

Адекватность оценки основана на вовлечении в процесс оценки большего числа элементов информационной среды объекта, глубине, достигаемой за счет использования при проектировании системы обеспечения безопасности большего числа проектов и описаний деталей выполнения, строгости, которая заключается в применении большего числа инструментов поиска и методов, направленных на обнаружение менее очевидных уязвимостей или на уменьшение вероятности их наличия.

**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.

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.

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.