2. Краткий отчет о практике

Я проходил технологическую практику на базе ООО «РЕАЛ+».

В современном обществе в связи с растущими потребностями человека возникают проблемы информационного обеспечения всех сфер ее деятельности, то есть предоставление всей необходимой информации. Есть основания считать, что по своей значимости и актуальности проблема информатизации является важной для современного общества. Одной из проблем является надежная защита информации на предприятии, обеспечивающий предупреждение искажение или уничтожение информации, а также делал бы ее злонамеренное получения, использования или несанкционированной модификации, или передачи ее конкурентам. Особую остроту эта проблема приобретает в связи с повсеместной и массовой компьютеризацией информационных процессов, и прежде всего в связи с объединением компьютеров в информационно-вычислительные сети, обеспечивает массовый доступ любых пользователей и их ресурсов.

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

149-ФЗ – регулирует отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации; при применении информационных технологий; при обеспечении защиты информации. Закон дает определения терминам «информация», «информационные технологии», «информационно-телекоммуникационная сеть», «информационная система», «сайт», «поисковая система» и т.п. Согласно закону информация подразделяется на свободно распространяемую, на предоставляемую по соглашению лиц, участвующих в соответствующих отношениях, на информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению, и на ту, распространение которой в РФ ограничивается или запрещается. Среди прочего, закон описывает порядок государственного регулирования случаев

распространения недостоверной информации (например, «фейковых новостей»), а также информации, которая оскорбляет человеческое достоинство, показывает явное неуважение к обществу, государству, официальным символам Российской Федерации или органам, осуществляющим государственную власть в РФ или содержит призывы к массовым беспорядкам, экстремистской деятельности, участию в массовых мероприятиях, проводимых с нарушением установленного порядка. Закон касается кредитных организаций в той же мере, что и других бизнес-единиц, и помимо этого, регулирует отношения, связанные со сбором и

Согласно Уставу, Общество с ограниченной ответственностью «РЕАЛ+» является юридическим лицом, коммерческой организацией. Компания зарегистрирована 18 Декабря 2009г. Реквизиты данной организации: ИНН 3805711108, ОКПО 64842676, ОГРН 1093805001762. Единственным участником данного Общества является генеральный директор Солодовник В.Н., который является владельцем 100% размера уставного капитала, равного 10 000 рублей.

Предметом деятельности данной организации является:

- рекламная деятельность;
- розничная торговля в неспециализированных магазинах замороженными продуктами;
- розничная торговля в неспециализированных магазинах не замороженными продуктами, включая напитки, табачные изделия;
- неспециализированная торговля замороженными пищевыми продуктами;
- неспециализированная оптовая торговля не замороженными пищевыми продуктами, напитками и табачными изделиями.

Таким образом, ООО «РЕАЛ+» осуществляет коммерческую деятельность в сфере торговли. В Уставе также определено, что данная организация может осуществлять помимо вышеуказанных видов любые иные виды деятельности, не запрещенные законом. Так, в последнее время с момента

получения соответствующей лицензии ООО «РЕАЛ+» занимается продажей алкогольной продукции.

Продукция «РЕАЛ+» предназначена для широкого круга потребителей. Основными клиентами данного склада являются розничные предприятия и предприятия общественного питания города Братска.

Коммерческая политика предприятия отдает предпочтение продукции российских производителей, основной упор в коммерческой политике предприятия делается на расширение и углубление ассортимента реализуемой рыбной продукции.

Миссия предприятия - создать базу лояльных потребителей и занять лидирующие позиции в сфере оптовой и розничной торговли алкогольной продукцией, замороженными пищевыми продуктами г. Братска через удовлетворение потребностей покупателей в продукции высокого качества, обеспечивая фирме максимальный годовой доход.

Далее представлена схема, отражающая организационную структуру управления ООО «РЕАЛ+» (см. рис. 1).

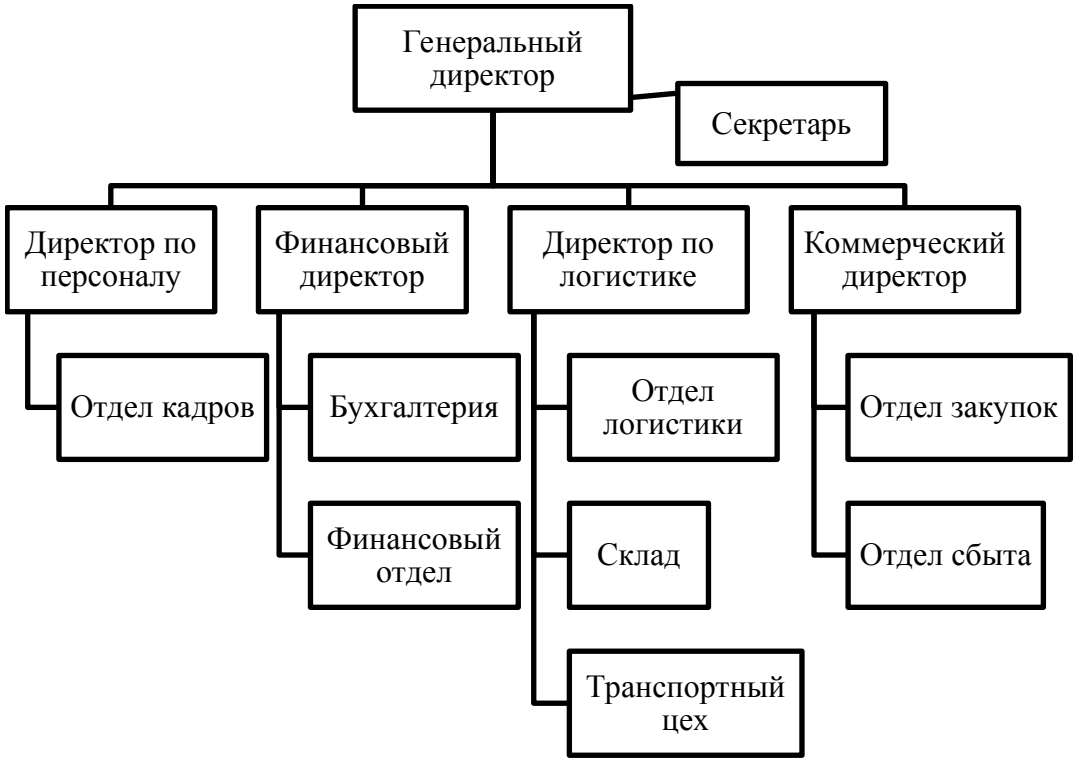

Рис. 1. Организационная структура управления ООО «РЕАЛ+»

Как видно из рис. 1. ООО «РЕАЛ+» имеет линейно-функциональную структуру управления. При данной структуре управления сохраняется преимущество линейной структуры в виде принципа единоначалия, и преимущество функциональной структуры в виде специализации управления.

Многолетний опыт использования линейно-функциональных структур управления показал, что они наиболее эффективны там, где аппарату управления приходится выполнять множество рутинных, часто повторяющихся процедур и операций при сравнительной стабильности управленческих задач и функций: посредством жесткой системы связей обеспечивается четкая работа каждой подсистемы и организации в целом.

К достоинствам линейно-функциональной структуры управления можно отнести:

- более глубокая подготовка решений и планов, связанных со специализацией работников;
- освобождение главного линейного менеджера от глубокого анализа проблем;
- возможность привлечения консультантов и экспертов.

К недостаткам линейно-функциональной структуры управления относятся:

- отсутствие тесных взаимосвязей между производственными отделениями;
- недостаточно четка ответственность, так как готовящий решение, как правило, не участвует в его реализации;
- чрезмерно развитая система взаимодействия по вертикали, а именно: подчинение по иерархии управления, то есть, тенденция к чрезмерной централизации.

Непосредственное управление предприятием осуществляет директор ООО «РЕАЛ+». В непосредственном подчинении директору находятся

директор по персоналу, коммерческий директор, директор по логистике и финансовый директор.

Основную ответственность за осуществление бизнес-процессов по продаже продукции со склада несет коммерческий директор, он отвечает за закупку товаров и их реализацию. На него одного возложены функции по поиску поставщиков и формированию клиентской базы, а также функции по проведению переговоров и заключению договоров. Исполнительские функции в рассматриваемых бизнес-процессах, таких как закупка, хранение и реализации продуктов со склада, распределены оптимально.

Контроль за оперативным и качественным выполнением обеспечивающих функций несет директор по персоналу. На него же возложена ответственность за организацию административно-хозяйственного обеспечения деятельности компании. Он рассчитывает оптимальную сумму денежных средств, которую предприятие может позволить потратить на осуществление данного бизнес-процесса. Он же контролирует целевое использование выделенных денежных средств.

Предприятие «РЕАЛ+» - основными направлениями деятельности является создание, развитие и поддержка функционирования информационно-аналитической системы Министерства финансов, системного и функционального сопровождения приложений и прикладного программного обеспечения, внедрение в деятельность финансовых органов современных информационных технологий, сервисного технического обслуживания и ремонта средств вычислительной техники и других работ, выполняемых для финансовых органов, других органов исполнительной власти и субъектов предпринимательской деятельности.

На предприятии имеются следующие помещения:

-кабинет директора;

-ремонтный отдел;

-бухгалтерия;

Перечень сотрудников:

-программисты;

-бухгалтер;

-мастер по ремонту техники;

-охранник.

Параметры сети:

На предприятии находится 3 компьютера. Роутер DIR-580, настроена внутренняя компьютерная сеть, доступ к интернету.

Защищенная финансовая информация, а также информация по начислении заработной платы рабочим.

В отделении находится служебная и конфиденциальная информация, содержащаяся в электронной и бумажной форме. Это информация финансовые операции, деловые связи, отчеты, и др. Для информации используются физические: это конструкции здания, защитные двери, окна, технические: сейф, камеры наблюдения, средства оповещения; аппаратные: специфическая компьютерная и офисная техника; программные: антивирус.

Для филиала ООО «РЕАЛ+» возможны все угрозы, как внутренние, так и внешние. Однако, учитывая местонахождение здания в городе и климатические условия, можно сказать, что риск природных угроз очень незначительный. Поэтому хотелось бы более обратить внимание на внутренние угрозы и угрозы извне, вызванные деятельностью нарушителя или небрежностью работников.

Для того, чтобы создать на предприятии условия эффективной защиты информации, необходимо объединить отдельные средства защиты в систему. При этом надо помнить, что главным элементом этой системы является человек. Причем человек является ключевым элементом системы и вместе с тем самым трудно формализуемым и потенциально слабым ее звеном.

Создание системы защиты информации (СЗИ) не является главной задачей предприятия, как, например, производство продукции и получение прибыли. Поэтому создаваемая СЗИ не должна приводить к ощутимым трудностям в работе предприятия, а создание СЗИ должно быть экономически

оправданным. Тем не менее, она должна обеспечивать защиту важных информационных ресурсов предприятия от всех реальных угроз.

Главное направление поиска новых путей защиты информации заключается не просто в создании соответствующих механизмов, а представляет собой реализацию регулярного процесса, осуществляемого на всех этапах жизненного цикла систем обработки информации при комплексном использовании всех имеющихся средств защиты. При этом все средства, методы и мероприятия, используемые для ЗИ, наиболее рациональным образом объединяются в единый целостный механизм - причем не только от злоумышленников, но и от некомпетентных или недостаточно подготовленных пользователей и персонала, а также нештатных ситуаций технического характера.

Основной проблемой реализации систем защиты является: с одной стороны, обеспечение надежной защиты, находящейся в системе информации (исключение случайного и преднамеренного получения информации посторонними лицами); С другой стороны, системы защиты не должны создавать заметных неудобств авторизированным пользователям в ходе их работы с ресурсами системы.

Изучение объекта защиты сводится к сбору и анализу следующей информации:

Об организации процесса функционирования объекта. В состав этих данных входят сведения, характеризующие:

-график работы объекта и его отдельных подразделений;

-правила и процедуры доступа на объект, в отдельные помещения и к оборудованию персонала и посетителей (регулярный, случайный, ограниченный доступ);

-численность и состав сотрудников и посетителей объекта (постоянный штат, персонал, работающий по контракту, клиенты);

-процедуру доступа на территорию транспортных средств.

Для получения этих данных можно применять следующие способы: анкетирование сотрудников; опрос сотрудников; личное наблюдение; изучение директивных и инструктивных документов.

Об условиях функционирования объекта. В состав этих данных входят сведения, характеризующие:

-пространство, непосредственно прилегающее к территории объекта;

-ограждение периметра территории и проходы;

-инженерные коммуникации, подземные хранилище и сооружения на территории;

-размещение подразделений и сотрудников по отдельным помещениям (с поэтажными планами);

-инженерные коммуникации в помещениях;

-состояние подвальных и чердачных помещений;

-размещение, конструкции и состояние входов, дверей, окон;

-существующую систему защиты;

-состав и настроение населения, экономические факторы и криминогенную обстановку на прилегающей территории.

На основе результатов анализа всех перечисленных сведений должны быть определены: назначение и основные функции системы защиты; основные виды возможных угроз и субъекты угроз; внешняя среда; условия функционирования системы защиты (наличие энергетических и других ресурсов, естественные преграды и т. п.).

Можно перечислить основные параметры предприятия и показать, каким образом они могут оказывать влияние на разрабатываемую комплексную систему защиты информации:

-характер деятельности предприятия оказывает влияние на организационно-функциональную структуру КСЗИ, ее состав; состав и структуру кадров СЗИ, численность и квалификацию ее сотрудников; техническое обеспечение КСЗИ средствами защиты; количество и характер мер и мероприятий по ЗИ; цели и задачи КСЗИ;

-состав защищаемой информации, ее объем, способы представления и отображения, технологии обработки: состав и структуру СЗИ; организационные мероприятия по ЗИ; состав технических средств защиты, их объем; состав нормативно-правового обеспечения КСЗИ; методы и способы ЗИ; объем материальных затрат на ЗИ;

-численный состав и структура кадров предприятия: численный состав сотрудников СЗИ; организационную структуру СЗИ; объем затрат на ЗИ; техническую оснащенность КПП; объем организационных мероприятий по ЗИ;

-организационная структура предприятия: организационную структуру КСЗИ; количество и состав сотрудников СЗИ;

-техническая оснащенность предприятия: объем и состав технических средств ЗИ; количество и квалификацию технического персонала СЗИ; методы и способы ЗИ; размер материальных затрат на ЗИ;

-нормативно-правовое обеспечение деятельности предприятия влияет на формирование нормативно-правовой базы КСЗИ; регулирует деятельность СЗИ; влияет на создание дополнительных нормативно-методических и организационно-правовых документов СЗИ;

-экономическое состояние предприятия (кредиты, инвестиции, ресурсы, возможности) определяет объем материальных затрат на ЗИ; количество и состав сотрудников и квалифицированных специалистов СЗИ; уровень технической оснащенности СЗИ средствами защиты; методы и способы ЗИ;

-режим работы предприятия влияет на режим функциональности КСЗИ, всех ее составляющих; состав технических средств ЗИ; объем затрат на ЗИ; численность персонала СЗИ;

-местоположение и архитектурные особенности предприятия: состав и структуру СЗИ; состав технических средств ЗИ; объем материальных затрат на ЗИ; численный состав и квалификацию сотрудников СЗИ;

-тип производства: организационно-функциональную структуру СЗИ;

-объем производства: размеры материальных затрат на ЗИ; объем технических средств защиты; численность сотрудников СЗИ;

-форма собственности влияет на объем затрат на ЗИ (например, на некоторых государственных предприятиях затраты на защиту информации (СЗИ) могут превышать стоимость самой информации); методы и способы ЗИ.

Организация КСЗИ на предприятии зависит от параметров рассмотренных характеристик данного предприятия. Однако степень воздействия различных характеристик предприятия на организацию КСЗИ различна. Из числа наиболее влиятельных можно выделить следующие:

-характер деятельности предприятия;

-состав защищаемой информации, ее объем, способы представления и отображения;

-численный состав и структура кадров предприятия;

-техническая оснащенность предприятия;

-экономическое состояние предприятия;

-организационная структура предприятия;

-нормативно-правовое обеспечение деятельности предприятия.

Несанкционированный доступ осуществляется через существующий или специально создаваемый канал доступа, который определяется как путь, используя который, можно получить неразрешенный доступ к конфиденциальной информации.

К каналам несанкционированного доступа к конфиденциальной информации относятся:

-установление контакта с лицами, имеющими или имевшими доступ конфиденциальной информации;

-вербовка и (или) внедрение агентов;

-организация физического проникновения к носителям конфиденциальной информации;

-подключение к средствам отображение, хранения, обработки, воспроизведения и передачи информации средствам связи;

-прослушивание речевой конфиденциальной информации;

-визуальный съем конфиденциальной информации;

-перехват электромагнитных излучений;

-исследование выпускаемой продукции, производственных отходов и отходов процессов обработки информации;

-изучение доступных источников информации;

-подключение к системам обеспечения производственной деятельности предприятия;

-замеры и взятие проб окружающей объект среды;

-анализ архитектурных особенностей некоторых категорий объектов;

-использование того или другого канала осуществляется с помощью определенных, присущих конкретному каналу методов и технологий несанкционированного доступа;

-установление контакта с лицами, имеющими или имевшими доступ к конфиденциальной информации.

Самым распространенным, многообразным по методам несанкционированного доступа, а потому и самым опасным каналом является установление контакта с лицами, имеющими или имевшими доступ к конфиденциальной информации.

В первую группу входят лица, работающие на данном предприятии, а также не работающие на нем, но имеющие доступ к конфиденциальной информации предприятия в силу служебного положения (из органов власти, вышестоящих, смежных предприятий и др.).

Вторая группа включает уволенных или отстраненных от данной конфиденциальной информации лиц, в том числе продолжающих работать на предприятии, а также эмигрантов и перебежчиков. Эта группа наиболее опасна, поскольку нередко имеет дополнительные причины для разглашения информации (обида за увольнение, недовольство государственным устройством и др.).

Контакт с этими людьми может быть установлен различными путями, например, на семинарах, выставках, конференциях и других публичных мероприятиях. Опосредованный контакт, осуществляемый через посредников

(без прямого общения, диалога), устанавливается через коллег, родственников, знакомых, которые и выступают в роли посредников.

Использование данного канала может иметь целью уничтожение или искажение информации с помощью лиц, имеющих к ней доступ, или для получения конфиденциальной информации. При этом применяются различные методы несанкционированного доступа к информации.

Наиболее распространенными методами является:

- Выведывание информации под благовидным предлогом («использование собеседника втемную»). Это может осуществляться в неофициальных беседах на публичных мероприятиях и т. д. с включением в них пунктов, касающихся конфиденциальной информации;

- переманивания сотрудников конкурирующих предприятий с тем, чтобы, помимо использования их знаний и умения, получить интересующую конфиденциальную информацию, относящуюся к прежнему месту их работы;

- покупки конфиденциальной информации активно ищут недовольных заработком, руководством, продвижением по службе;

- принуждение к выдаче конфиденциальной информации шантажом, различного рода угрозами, применением физического насилия как к лицу, владеющему информацией, так и к его родственникам и близким;

- склонение к выдаче конфиденциальной информации убеждением, лестью, посулами, обманом, в том числе с использованием национальных, политических, религиозных факторов.

Организация физического проникновения к носителям конфиденциальной информации.

Организация физического проникновения к носителям конфиденциальной информации сотрудников разведывательных служб - используется сравнительно редко, поскольку он связан с большим риском и требует знаний о месте хранения носителей и системе защиты информации, хотя уровень защиты информации в некоторых государственных и многих

частных структурах дает возможность получать через этот канал необходимую информацию.

Физическое проникновение лиц, не работающих на объекте, включает два этапа:

- проникновение на территорию (в здания) охраняемого объекта.
- проникновение к носителям конфиденциальной информации.

При проникновении на территорию объекта возможно применение следующих методов:

- использование подложного, украденного или купленного (в том числе и на время) пропуска;
- маскировка под другое лицо;
- проход под видом внешнего обслуживающего персонала;
- проезд спрятанным в автотранспорте;
- отвлечение внимания охраны для прохода незамеченным (путем создания чрезвычайных ситуаций, с помощью коллеги и т. д.);
- изоляция или уничтожение охраны;
- преодоление заграждающих барьеров (заборов), минуя охрану, в том числе и за счет вывода из строя технических средств охраны.

Проникновение к носителям конфиденциальной информации может осуществляться путем:

- взлома дверей хранилищ и сейфов (шкафов) или их замков, через окна, ее проникновение производится в нерабочее время, с отключением (разрушением) сигнализации, телевизионных средств наблюдения (при необходимости), или, при проникновении в рабочее время, путем прохода в комнаты исполнителе работающих с конфиденциальными документами, в производственные и складские помещения для осмотра технологических процессов и продукции, а также в помещения, которых производится обработка информации.
- Проникновение к носителям конфиденциальной информации осуществляется и во время их транспортировки с использованием, в

зависимости от вида, условий и маршрута транспортировки, соответствующих методов.

Целью проникновения является, как правило, получение конфиденциальной информации, но она может состоять и в оказании на информацию дестабилизирую воздействий, приводящих к ее уничтожению, искажен, блокированию.

Подключение к средствам отображение, хранения, обработки, воспроизведения и передачи информации средствам связи.

Подключение к средствам отображения, хранения, работки, воспроизведения и передачи информации, средства может осуществляться лицами, находящимися на территории объекта и вне ее.

Несанкционированное подключение, а, следовательно, и санкционированный доступ к конфиденциальной информации может производиться:

- с персонального компьютера с использованием телефонного набора или с несанкционированного терминала со взломом парольно-ключевых систем защиты или без взлома с помощью маскировки под зарегистрированного пользователя;
- с помощью программных и радиоэлектронных устройств;
- с помощью прямого присоединения к кабельным линиям связи, в том числе с использованием параллельных телефонных аппаратов;
- за счет электромагнитных наводок на параллельно проложенные провода или методов высокочастотного навязывания.

Прослушивание речевой конфиденциальной информации - всегда широко использовалось, опасность увеличивается по мере появления новых технических средств прослушивания. При этом речь идет о прослушивании не агентами, находящимися внутри помещения, а лицами, расположенными вне задания, иногда на значительном расстоянии от него.

Такое прослушивание чаще всего осуществляется по двум направлениям:

- подслушивание непосредственных разговоров лиц, допущенных к данной информации;
- прослушивание речевой информации, зафиксированной на носителе, с помощью подключения к средствам ее звуковоспроизведения.

Визуальный съем конфиденциальной информации может осуществляться следующими методами:

- чтением документов на рабочих местах пользователей (в том числе с экранов дисплеев, с печатающих устройств) в присутствии пользователей и при их отсутствии;
- осмотром продукции, наблюдением за технологическим процессом изготовления продукции;
- просмотром информации, воспроизводимой средствами видеовоспроизводящей техники и телевидения;
- чтением текста, печатаемого на машинке и размножаемого множительными аппаратами;
- наблюдением за технологическими процессами изготовления, обработки, размножения информации;
- считыванием информации в массивах других пользователей, в том числе чтением остаточной информации.

Под эффективностью системы обычно понимают ее приспособленность к выполнению своей целевой функции.

Различают два вида эффективности: результативная - эффективность в смысле результативности; экономическая - эффективность в смысле экономичности.

Оценка эффективности - процедура, направленная на определение качественных и количественных показателей эффективности, выявление критических элементов системы, а также определение интегрального показателя эффективности системы в целом.

Оценка эффективности ведется по определенным показателям:

Показатель эффективности - величина, характеризующая степень достижения системой любой из поставленных перед ней задач. Значение показателя эффективности, при котором система удовлетворяет предъявляемым к ней требованиям, называется критерием эффективности.

Все показатели эффективности можно разделить на 2 группы:

-Единичные, отражают какую-либо из значимых сторон функционирования системы (вероятность обнаружения нарушителя, вероятность нейтрализации нарушителя силами охраны и т.п.);

-Комплексные (обобщенные), представляют собой комбинацию частных показателей.

На сегодняшний день существует несколько методических подходов к оценке эффективности:

-Детерминистический подход;

-Логико-вероятный метод;

-Вероятно-временной анализ.

Детерминистический подход связан с задачей и последующей проверкой обязательных требований, содержащихся в ведомственных руководящих документах, на проектирование, рабочем проекте. Этот подход предусматривает проведение комплексных проверок с различной регулярностью.

Логико-вероятный метод. Целью исследования является определение степени риска, присутствующего в системе. Количественная оценка степени риска производится с помощью теории вероятности.

Недостатком метода является трудоемкость логико-вероятностных преобразований, а также проблема достоверности вероятности инициирующих событий.

Вероятно-временной анализ. Основной метод, который используется в настоящее время для оценки эффективности СЗИ. Эффективность рассматривается как вероятная величина. При этом определяется выполнение следующего условия: $T = To-Tн < 0$, где To - суммарное время реагирования

охраны на дестабилизирующие действия, Тн - суммарное время воздействия нарушителя. $T = \Sigma t_i$. Если ti независимые и их количество велико, то события Т оказываются распределены по нормальному закону.

ООО «РЕАЛ+» - небольшое предприятие, но в нем нужно защищать конфиденциальную информацию о всех пользователях, которые пользуются его услугами.

Оптимальное распределение задач между техникой и человеком - предотвращение воздействия человеческой фактора за счет автоматизации процессов управления оборудованием и внутреннего учета. Комплекс организационных мероприятий, которые рекомендованы дополнительно к техническим средствам для их эффективного использования.

Я советовал бы улучшить внешнюю систему защиты установкой камер и контрольно пропускной пункт, улучшить программное обеспечение и поставить сетевую защиту (Firewall).

Информационную безопасность предприятия определяет используемая им информационная технология, представляет собой информационный процесс, реализуемый на распределенных по территории предприятия технических средств, а также наличие точек доступа или утечки информации, создают потенциальную возможность реализации угроз; и наличие эффективных средств защиты.

Наиболее эффективными мерами, проведение которых целесообразно в первую очередь, представляются создание средств защиты от хищения носителей информации и обеспечения их надежности в эксплуатации. Средства защиты (защитные барьеры) предназначены для того, чтобы ликвидировать или уменьшить до приемлемого уровня последствия вредных воздействий на информационный процесс.

Определение мер по обеспечению необходимого уровня защищенности предполагает определение структуры, состава и размещения средств защиты информации, при которых обеспечивается необходимый уровень защищенности предприятия от реального спектра угроз безопасности. Задача

синтеза системы защиты информации на предприятии должна проводиться на основе количественных показателей, полно и достоверно отражают уровень информационной безопасности предприятия.

Разработка документа «Технический проект» (ТП) является завершающим этапом документирования проекта по созданию ИС. Если техническое задание документирует требования к системе и отвечает на вопрос: ЧТО должна обеспечивать проектируемая система, то ТП определяет, КАК будут реализованы эти требования. Цель разработки ТП - сформировать окончательные технические решения, дающие полное представление об ИС.

Стандарт ГОСТ 34.003-90 определяет технический проект автоматизированной системы как комплект проектных документов на ИС (АС), утвержденный в установленном порядке и содержащий основные проектные решения по системе в целом, ее функциям и всем видам обеспечения АС.

Технический проект является источником информации для создания рабочей документации (РД) - комплекта документов, достаточных для монтажа, наладки, функционирования ИС, организации ее тестирования и обеспечения работоспособности. Технический проект используется разработчиками при программировании спроектированного программного продукта, руководителями проектов в процессе обсуждения и согласования ключевых проектных решения с заказчиком. Технический проект применяют в своей работе бизнес-аналитики, системные аналитики, специалисты по тестированию и внедрению ИС.

При разработке технического проекта выполняют работы, необходимые для обеспечения предъявляемых к изделию требований и позволяющие получить полное представление о конструкции разрабатываемого изделия, оценить его соответствие требованиям технического задания, технологичность, степень сложности изготовления, способы упаковки, возможности транспортирования и монтажа на месте применения, удобство эксплуатации, целесообразность и возможность ремонта и т.п.

Согласно ГОСТ 2.120-2013, и. 1.2, «При разработке технического проекта выполняют работы, необходимые для обеспечения предъявляемых к изделию требований и позволяющие получить полное представление о конструкции разрабатываемого изделия, оценить его соответствие требованиям технического задания, технологичность, степень сложности изготовления, способы упаковки, возможности транспортирования и монтажа на месте применения, удобство эксплуатации, целесообразность и возможность ремонта и т.п.».

В соответствии с ГОСТ 34.601-90 определяются следующие этапы формирования ТП:

- разработка проектных решений для АС и ее составляющих;

- разработка документации на АС и ее составляющие;

- формирование документации на поставку изделий для комплектации АС;

- разработка заданий на проектирование в смежных частях проекта объекта автоматизации.

На первом этапе разрабатываются общие решения по системе и ее частям. Формируются функции персонала и решения по организационной структуре, решения по структуре технических средств, по алгоритмам решения задач и применяемым языкам, по организации и ведению информационной базы, решения по системе классификации и кодированию информации, ПО.

На следующем этапе выполняются разработка, оформление, согласование и утверждение документации. Перечень подлежащих разработке документов определен техническим заданием в разделе «Требования к документированию».

На этапе разработки и оформления документации выполняются подготовка и оформление документации на поставку изделий для комплектования АС и формируются технические требования и ТЗ на разработку изделий, не изготовляемых серийно.

На последнем этапе формирования ТП осуществляются разработка, оформление, согласование и утверждение заданий на проектирование

строительных, электротехнических, санитарно-технических работ и других подготовительных работ, связанных с созданием АС.

Для обсуждения этапов и технологий создания современных информационных систем начнем с определения Автоматизированной Информационной Системы.

Под Автоматизированной Информационной Системой (АИС) мы будем понимать комплекс, который состоит из:

1. Аппаратно-технических средств, включающих компьютеры, периферию, системное и программное обеспечение.

2. Программного комплекса, который осуществляет механизм управления.

3. Информационной модели, представляющей совокупность правил и алгоритмов функционирования системы, объединяющей все формы данных и документов.

4. Эксплуатационно-технических кадровых ресурсов, обеспечивающих функционирование информационной системы.

5. Обратной связи или взаимообратной системы, позволяющей вносить изменения и коррекцию в работу системы.

Понятие - автоматизированная, предполагает использование современных технических и программных средств, без которых современные информационные системы, учитывая объемы и скорости обработки данных, просто не смогут существовать.

Таким образом, АИС - это система, которая предназначена для сбора, передачи, обработки, хранения и выдачи информации. АИС состоит из технических, программных, информационных и кадровых ресурсов.

Информационная система может функционировать как самостоятельно, так и являться составной частью или подсистемой для более сложной архитектуры.

Современные комплексные АИС позволяют решать задачи исследовательского, управленческого характера, планирования ресурсов

предприятия, контроля деятельности различных функциональных частей. Учитывая размеры и характер решаемых задач, используют новейшие сетевые технологии и называют такие системы - Корпоративными Информационными Системами или КИС.

В моделировании предметной области используют следующие виды моделей: структурированные, слабоструктурированные, формальные, неструктурированные, а также модели данных.

В структурированных моделях выделяется регулярная структура предметной области. Здесь выбираются сущности одного типа с одинаковым набором свойств, между различными типами сущностей строятся бинарные и n-арные связи. Примером такого подхода в моделировании является объектно-ориентированный, который позволяет наглядно моделировать не только структуру предметной области, но и все процессы взаимодействия определенных типов (в объектном программировании все операции с представителями различных классов или типов объектов называются методами).

При использовании структурированного подхода выделяют два уровня моделей: интенсионал предметной области и экстенсионал.

Интенсиональная модель определяет типы сущностей и связей между ними вне зависимости от времени. Более реальная модель второго уровня - экстенсионал предметной области. Она определяет связи между реальными экземплярами сущностей в зависимости от времени.

Системы баз данных основаны на структурированных моделях.

В некоторых информационных системах не требуется строгая типизация сущностей и связей, иначе говоря, регулярная структура не определена. Представление предметной области определяется одним уровнем, экстенсионалом или рассматриваются конкретные сущности и связи между ними. Такие слабоструктурированные модели используются в системах, созданных на различных языках разметки, например, HTML.

Формальные модели используют для информационных систем, написанных на формальных языках. Формальное представление предметной области делится на два уровня. В данном случае интенсионал представляет набор аксиом, описывающий отношения между различными типами сущностей. Экстенсионал представлен множеством фактов. Для таких систем используют логические языки (Пролог, Лисп). Этот тип моделей используется в экспертных системах.

Неструктурированные модели описывают предметную область на естественных языках, в виде текстов. Системы, работающие с таким уровнем моделей типа тезауруса, с лингвистической поддержкой. Такие неструктурированные модели называются вербальными. Системы текстового поиска используют этот тип моделей.

Модели данных - инструменты моделирования, созданные с помощью различных программных средств. Используя объектный подход, который используется во всех современных технологиях, модель данных можно рассматривать как систему типов данных. В системах базы данных интенсиональная модель предметной области представляется схемой базы данных. На основе этой схемы проектируется приложение для управления данными базы. Терминология модели данных используется не только для проектирования баз данных, но и в WEB-технологиях, а также языке XML.

В процессе практики были закреплены теоретические знания, полученные во время обучения. Решение практических задач позволило установить, как на самом деле, на конкретном предприятии, решаются вопросы управления предприятием.

В заключении можно сказать, что весь период прохождения практики был насыщенным аналитической работой по различным пунктам деятельности компании. Эти сферы деятельности включали в себя не только систему управления персоналом, но также и экономические и финансовые вопросы функционирования компании на рынке. Мною были приобретены практические

навыки работы в коллективе организации. Выполненная работа была занесена в дневник практики.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Трудовой кодекс Российской Федерации – Официальный текст. – М.; «Издательство ЭЛИТ», 2017.

2. Барсуков В.С., Водолазний В.В. Современные технологии безопасности. - М.: «Нолидж», 2018. - 496 с.

3. Как построить защищенную информационную систему/ Под науч. ред. Зегжды Д.П. и Платонова В.В. - СПб.: Мир и семья, 2019.

4. Программно-аппаратные средства обеспечения информационной безопасности. Защита программ и данных: Учебное пособие для вузов/ Белкин П.Ю., Михальский О.О., Першаков А.С. и др. - М.: Радио и связь, 2018. - 168 с.

5. Алексенцев А. И. Понятие и назначение комплексной системы защиты информации // Вопросы защиты информации. - № 2. - 2018.

6. Мельников. Информационная безопасность и защита информации, - Academia, M., 2017.

_____ _____

подпись ФИО студента