#  1.3 Особенности управления системой защиты информации

Система защиты информации — совокупность организационных и технических мер, сориентированных на поддержку информационной безопасности. Основным объектом защиты является информация, которая обрабатывается в системе защиты информации и используется при выполнении бизнес-процессов.

Процесс создания системы защиты информации происходит в три шага:

- организация политики предприятия в сфере информационной безопасности;

- выбор и введение технических и программных средств защиты;

- создание и проведение ряда организационных мероприятий.

Также не стоит забывать про государственные нормативные документы и стандарты, которые регулируют вопросы информационной безопасности.

СЗИ производится дабы предоставить уверенную защиту личных данных каждого человека, следовательно, возможностями, являющимися субъектами реализации в этой сфере, станут функции сохранения личных данных, иначе говоря, комплекс элементарных отношений и мероприятий, которые день за днем выполняются на предприятии дабы изобрести, а также поддержать все положения, надобных с целью надежной защиты данных.

Наиболее оперативной защита личных данных каждого человека станет исключительно тогда, если будут сооружены прочные механизмы защиты, на периода работы системы же осуществляется непрерывное регулирование исходными механизмами.

То есть в СЗИ должно находиться предвидено два типа функций:

1. ключевой задачею которых является разработка устройств защиты;

2. выполняемые для обеспечения хронического и особенно благоприятного контроля механизмами защиты.

Руководство обусловливается субъектом, свойства поставленных систем различной сферы которого, гарантирует надежность их установленной структуры, защита систем деятельности, проведению их мероприятий и поставленных задач.

Смысл самого управления — предоставление предельно вероятной производительности использования средств.

Задачи управления:

• Поддержка установленной степени результата при наименьшей степени расходов.

• Поддержка наивысшей степени конечного результата при установленном уровне затрат.

Метод контроля обязан строиться так, дабы гарантировать успешную обрабатывание данных для каждого функционального класса при разумной эксплуатации средств автоматизированной системы.

При этом метод управления желательно создать таким образом, дабы гарантировать:

• общую автоматизацию операций обработки данных любого работника, а также его контроля;

• целостность инструментов, ресурсов и систем управления;

• предельную автоматизацию в ходе урегулирования проблем, происходящих в ходе работы органов управления, в том числе задач личного информационной поддержки, задач производств управленческих заключений и вопросов информационного соединения коммуницирующих функций.

Самое активное звено схемы организации - человек, вдобавок он считается частью управления, в том числе и объектом управления.

Не стоит забывать о ключевых условиях технологии управления:

Гарантия разделения труда, проявляющееся в конкретизации функциональных обязательств руководителей и сотрудников органов управления.

Формализация всей деятельности, выполняемой в органах управления, складывается из положений численных оценок в управленческие процессы, потреблении математических возможностей в управлении, а также использование к управленческим системам аналогичных понятий, как устойчивость, достоверность и рентабельность.

Регулирование контакта работников органов управления среди друг друга, а также средствами автоматизации, заключающийся в разработке совокупности законов, предписаний и запретов, установленной в определенных нормативно-методических документах, которые располагают неукоснительный характер.

Гарантия психологических сопоставимостей управляющих и сотрудников органов управления с системой автоматизации.

Увеличение исполнительной дисциплины сотрудников органов управления.

Весь сложный комплекс управленческих действий — на любом уровне и системе — может быть отнесен к перечню функций, образующих безостановочный процесс управления:

• установление управленческого решения;

• воплощение решения;

• контроль.

На Рис. 2 представлено планирование, которое, по своей сути представляется началом в периоде руководства. Проектирование в качестве метода управления располагает сложной структурой и исполняется путем своих подфункций.

Из этого следует, что формирования планирования способом руководства значится в попытке предварительно предусмотреть все внутренние и внешние факторы, создающие выгодное положение для правильного функционирования и формирования предприятия. Планирование учитывает создание совокупности мероприятий, устанавливающих порядок достижения определенных целей учитывая способности особо успешного применения ресурсов любым подразделением.

Для поддержания работоспособности системы в целом, важную функцию выполняет контроль деятельности. Задача контроля — найти и распознать болезненные части системы, все проблемы, и вовремя решить эти проблемы, дабы не позволить появиться новым.

Ход работы контроля содержит в себе три этапа:

Обозначение фактического качества СЗИ.

Исследование параллели подлинного состояния с определенным режимом, положением, а также оценкой характера возможных отклонений и недоработок.

Создание мероприятий по усовершенствованию и внесению поправок в ход процесса руководства системой, а также утверждение всех мер по их исполнении.

При утверждении любого управленческого решения, руководство именуется источником данных, его применение позволяет говорить о теме управленческого процесса, его качестве, эффективности. Отклонить процесс контроля невозможно, а то это будет свидетельствовать о потере данных любого пользователя и, в итоге, потерю всего управления. Управление не ориентируется само на себя, оно предназначено для качественного и гарантированного исполнения принятых решений.

Ключевыми задачами контроля можно назвать:

* Установление обоснованности и практической необходимости проводимых мероприятий по защите данных.
* Обнаружение фактического качества СЗИ в настоящий момент времени.
* Обнаружение первопричин и обстоятельств отклонений признаков качества, относящихся к СЗИ, от заданных.
* Анализ деловых свойств и степени профессиональной подготовки лиц, выполняющих защиту данных.

Эффективность механизма управления, как суммарную результативность его элементов: рентабельность всей системы руководства, процессов, а также управленческих результатов и состава компании с осознанным конечным результатом. Важно при этом понимать, что механизм управления обязан быть, как эффективным, так и результативным. Соответственно, эффективность — это свершение целей и задач, а эффективность, это путь и методы свершения. Результативность представляется измеримым и явным понятием, именно поэтому мы можем ее оценить на основании сопоставления результатов. А эффективность более трудное понятие, и не всегда бесспорно можно ее оценить.

Исходя из этого, можно сказать, что функции управления можно установить, как типы управленческой деятельности, которые нужны для организации и управления определенным объектом для воплощения целенаправленной деятельности по достижению желаемого результата. Любой способ управления является областью действия определенного процесса управления, а организационная структура управления, определенным объектом или же родом деятельности. Тем самым, эффективное формирование управления систем защиты информации во многом обусловливается формированием современных управленческих функций и формированием организационных структур управления.

# ГЛАВА 2. АНАЛИЗ НОРМАТИВНО-ПРАВОВОЙ БАЗЫ УПРАВЛЕНИЯ СИСТЕМОЙ ЗАЩИТЫ ИНФОРМАЦИИ КОММЕРЧЕСКОГО ПРЕДПРИЯТИЯ

# 2.1 Федеральный закон "О коммерческой тайне" от 29.07.2004 N 98-ФЗ

Прежде всего, фирмы обязаны приступить к соответствующим операциям регистрации. Все представители обязаны заключить договор с положениями о неразглашении, когда они принимают условия не разглашать конфиденциальную информацию. Иным условием, находящееся в контракте - условие, не предполагающее конкуренции, запрещающее представителем компании работать на подобной специальности в фирме-конкуренте, а также открывать бизнес с конфиденциальной информацией компании. Все эти соглашения всегда объединены условиями во времени и географическими границами. Итак, следовательно этому, предприятиям нужно найти специальные способы защиты коммерческой тайны и непосредственно их предпринять.

Нанимателям следует непрерывно проверять электронную почту работников и деятельность, которую они осуществляют на устройствах компании. Важным пунктом также является то, что в компании обязана иметься политика, заставляющая работников исполнять все рабочие обязанности на устройствах фирмы, а не на собственных устройствах. Несмотря на это, все эти наблюдения вынуждены осуществляться с ограничениями, конфиденциальность работников обязана соблюдаться, иначе это станет проблемой для лояльности сотрудников. Во-вторых, подобает проводить заключительные собеседования со всеми увольняющимися представителями компании, напоминая им об обязательствах по завершении трудовой деятельности в касательстве неразглашения коммерческой тайны. Все это представляются одним из звеньев системы защиты информации коммерческого предприятия, оно же обязуется управляться Федеральным законом «О коммерческой тайне» от 29. 2004 N 98-ФЗ. «Настоящий Федеральный закон регулирует все отношения, которые проходят между компанией и лицом, работающей в ней, которые связанны с установлением, изменением и прекращением режима коммерческой тайны, информация которой имеет объективную или потенциальную коммерческую важность в силу неизвестности третьим лицам». Положения, которые предоставлены этим законом не распространяются на те данные, которые приурочены к государственной тайне, в коих наличествуют особые законы РФ.

Федеральный закон «О коммерческой тайне» включает в себя следующие основные понятия, которые составляют коммерческую тайну:

* коммерческая тайна;
* данные;
* обладатель этих данных;
* доступ к данным;
* передача данных;
* огласка данных.

В этом законе «коммерческая тайна» - «конфиденциальная информация, дозволяющая при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг, или получить иную коммерческую выгоду». Это сведения, составляющие коммерческую тайну, ежели они обладают ценностью, и покуда неведомы третьим лицам. Это та определенная информация, которую всеми способами фирма отгораживает извне, в том числе составляющая секреты производства (ноу-хау), имеющая действительную или потенциальную ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладатель такой информации ввел режим коммерческой тайны. Или же их называют способами защиты ее конфиденциальности. Распоряжение не вынуждает предоставлять к аналогичным данным свободный доступ любому пользователю, оттого путь к этим данным, образующим коммерческую тайну некоторых лиц этой компании, может быть произведен исключительно под расписку с согласия ее собственника либо в соответствии определенных запросов законодательства. К примеру, все эти условия изобретены основным положением правоохранительным органам, но стоит отметить, что это произойдет с учетом накопления ими не только конфиденциальности, но и самой охраны конфиденциальности подобных данных любого человека. Похожие условия по защите конфиденциальной информации и коммерческой тайны вчиняются и к тем людям, которые уже получили путь к подобным данным, что и произошло в следствии случайности либо по ошибке.

В целях подавления незаконного распространения коммерческих данных определенного лица, неважно, служебных и коммерческих, постановление учитывает весь перечень тех утверждений, сориентированных на охрану такой конфиденциальной информации сотрудников фирмы любыми способами. Также это относится к индивидуальным предпринимателям, располагающих доступом к такой конфиденциальной информации, что вследствие потребности ее реализации рабочих обязательств. Подобные представители любых компаний будут обязаны под расписку ознакомлены с подобной системой коммерческой тайны и обязанностью за несоблюдение всех ее условий. В случае, если представитель компании не соблюдал рабочие обязанности сотрудника, ему же не предположен доступ к конфиденциальным данным, то ему позволено в любой момент изучить их исключительно при его согласии. При этом накладывается ответственность на человека за нарушение настоящего Федерального закона «О коммерческой тайне», которая, в свою очередь, влечет за собой гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством РФ. Вместе с тем Законом учтена «ответственность владельца секретной информации за невыполнение легитимных условий органов государственной власти о предоставлении им подобный информации, а также воспрепятствование получению должностными лицами этих органов указанной информации.»[[1]](#footnote-1)

Постановление предугадало перечень тех критерий в предпринимательской деятельности компании и сотрудников, кои вообще никак не связаны коммерческой тайной. На эти критерии предпринимательские структуры не вправе вводить режим тайны. Эта информация является общедоступной. К примеру, учредительные документы юридических и физических лиц, а также частных предпринимателей, заверяющие с точностью их государственный учет в определенных государственных реестрах, и те документы, дозволяющие им в любой мере осуществлять любое предпринимательское движение с их стороны; о структуре любой собственности государственных и унитарных компаний, а вдобавок еще о пользовании этими компаниями их ресурсами. Не вправе составлять коммерческую тайну сведения о загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, качестве пищевых продуктов и других факторах, сведенных с предоставлением лучшей сохранности всего населения. Также запрещается засекречивать любые сведения в компании о количестве и составе служащих в этой фирме, о методах оплаты труда работникам и задолженности нанимателей по выплате зарплаты этим самым работникам, также недостатках законодательства и любых прецедентах призыва к ответственности за совершение любого правонарушения физическим лицом, о перечне лиц, имеющих право действовать без доверенности от имени юридического лица. Информацией о размере и структуре профитов некоммерческих организаций также не располагает коммерческой тайной, стоит также отметить информацию о количестве и составе имущества, обо всех их расходах, оплате труда их работников в компании. В постановлении есть определенный список лиц, коим фирмы в любом случае обязаны дать ту информацию, касающуюся системы коммерческой тайны. Также это затрагивает все требования, связанные с заявлениями, пришедшие из судов и прокуратуры.

Неважно в какой фирме работает человек, это фирма обязана всем безотносительно от ее координационно-законной формы, организовать и выдать нормативный документ, либо список нужных документов. Такой документ, в свою очередь, обязан определить весь перечень секретных данных лица, требования доведения до извещения некоторого круга сотрудников, работающих в этой компании, ну и учрежденной системы предоставления коммерческой тайны. Функция сотрудников по неразглашению и обеспечиванию безопасности системы коммерческой тайны и ответственности за передачу секретной коммерческих данных. В самом начале обусловливается список всех сведений между компанией и определенным лицом, образующих коммерческую тайну, потом - сможет ли собственник этих данных гарантировать стопроцентную сохранность ее конфиденциальности, представляются ли эти данные неведомыми другим лицам, а также располагает ли сведениями истинной либо потенциальной значимостью. Разработанный перечень документов и условий ратифицируется распоряжением главного начальника компании, либо будет являться долею общего «Положения об обеспечении коммерческой тайны на фирме».

2.2 Гост Р ИСО/МЭК 27001-2006

 Проблема введения эффективных систем маркетинга информационной безопасности (СМИБ) с целью предоставления устойчивого формирования компании становится всё более актуальной. Современные опасности в этой области призывают к реагированию на системном уровне. Чтобы повысить производительность систем защиты данных применяется ISO/IEC 27000 серия международных образцов, которая включает в себя эталоны по информационной безопасности, выпущенные в сообществе Международной Организации по Стандартизации (ISO) и Международной Электротехнической Комиссии (IEC). Серия включает наилучшие практики и советы в сфере информационной безопасности для производства, развития и обслуживания всей системы маркетинга ИБ .

В России был принят ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования». «Настоящий стандарт подготовлен в качестве модели для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения системы менеджмента информационной безопасности (СМИБ). Внедрение СМИБ является стратегическим решением организации. На проектирование и внедрение СМИБ организации влияют потребности и цели организации, требования безопасности, используемые процессы, а также масштабы деятельности и структура организации. Предполагается, что вышеуказанные факторы и поддерживающие их системы будут изменяться во времени. Предполагается также, что СМИБ будет изменяться пропорционально потребностям организации, т.е. для простой ситуации потребуется простое решение по реализации СМИБ.»[[2]](#footnote-2)

**Система менеджмента информационной безопасности (СМИБ)** — элемент общего порядка менеджмента, построенная на взаимодействии с бизнес-рисками при производстве, введении, деятельности, оценке, наблюдении, помощи и усовершенствовании ИБ.

**Цель СМИБ**- выбор соответствующих мер управления безопасностью, предназначенных для защиты информационных активов и формирующих доверие заинтересованных сторон.

Из-за своей универсальности образец ISO 27001 является независимой моделью, но, как и иные аналоги, основывается на главных положениях и процессном подходе ISO 9001. Система документации по условиям ISO 27001 подобна ISO 9001. Поэтому, ежели компания уже обладает системой маркетинга в зависимости, к примеру, с ISO 9001 либо ISO 14001, то лучше всего гарантировать исполнение условия стандарта ISO 27001в пределах уже нынешних систем.

Стандарт универсален, поэтому может применяться во всех компаниях, независимо от сферы их деятельности на предприятии, организационно-правовой формы, а также иных параметров.

Однако применение ИСО особенно актуально и рекомендовано тем компаниям, деятельность которых связаны с «инфо-рисками», в частности для:

* фирм в сфере страхования;
* банковских учреждений;
* лабораторий и НИИ;
* финансовых компаний;
* учреждениях в сфере образования;
* IT-фирм;
* служб доставки;
* предприятий, ведущих деятельность в сфере «оборонки».

Процедура внедрения СМК в сферу информационной безопасности согласно ИСО 27001 состоит из таких этапов, как разработка необходимой документации, анализ имеющихся рисков, внедрение системы и проведение корректировочных мероприятий. Помимо того, проводится обучение сотрудников и непрерывный мониторинг.

На окончательном этапе осуществляется итоговый аудит функционирования системы. По его итогам заявитель может получить добровольный сертификат. Срок действия документа – 3 года. После документ не продлевается – его нужно переоформить.

Отличительной чертой этого закона является использование процессного подхода для поддержки и усовершенствования СМИБ организации.

По этой причины можно понять, что: «Для успешного функционирования организация должна определить и осуществить менеджмент многочисленных видов деятельности. Деятельность, использующая ресурсы и управляемая в целях преобразования входов в выходы, может быть рассмотрена как процесс. Часто выход одного процесса непосредственно формирует вход для следующего процесса.»[[3]](#footnote-3)

Использование внутри организации системы процессов наряду с идентификацией и взаимодействием этих процессов, а также менеджмент процессов могут быть определены как "процессный подход".

В настоящем стандарте представлена модель "Планирование (Plan) - Осуществление (Do) - Проверка (Check) - Действие (Act)" (PDCA), которая может быть применена при структурировании всех процессов СМИБ. Принятие модели PDCA также отражает принципы, установленные в директивах Организации экономического сотрудничества и развития (ОЭСР) и определяющие безопасность информационных систем и сетей. Настоящий стандарт представляет наглядную модель для реализации на практике указанных принципов, которые позволяют осуществить оценку рисков, проектирование и реализацию системы информационной безопасности, ее менеджмент и переоценку.

Модель PDCA это связь процессов:

• Планирование (разработка СМИБ);

• Осуществление (внедрение и обеспечение функционирования СМИБ);

• Проверка (проведение прогноза и разбора СМИБ);

• Действие (поддержка и улучшение СМИБ).

# 2.3 Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ

Каждому обладателю бизнеса, не принимая во внимание масштабы компании, подобает следовать Федеральным законом "О персональных данных" от 27. 2006 N 152-ФЗ. Не имеет значение, юридическое лицо либо индивидуальный предприниматель — все фирмы приобретают доступ к сторонним личным данным. Самое главное - уметь верно их использовать, не нарушая закон и условия Роскомнадзора.

«Персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных),»[[4]](#footnote-4) в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Заключение соглашений с контрагентами, принятие людей на работу, обслуживание клиентов, и приём доходов компании в счёт платежа товаров либо услуг — это связь с личной информацией.

Сотрудники дают фирмам свои личные данные, и им необходимы гарантии, что их личная информация в надежных руках и будет применяться только по назначению. Проверить законность использования персональных данных и структурировать процессы их обработки можно проведя аудит соответствия обработки персональных данных закрепленным внутри компании процессам обработки.

Кроме того, имеются некоторый список нужных для бизнеса документов, относящейся к обработке, сбором и хранением личных данных, который устанавливается Роскомнадзором.

Закон 152-ФЗ — единственный документ, который ставит условия и правила обработки личных информации людей ко всем компаниям, государственным и муниципальным структурам, частным фирмам, которые собирают, обрабатывают и хранят личные сведения своих работников и клиентов.

К категориям личной информации можно отнести:

* Общая личная информация;
* специальная личная информация;
* биометрическая личная информация;
* иная личная информация.

В законе о защите личной информации говорится об операторе и субъекте ПДн.

**Оператор ПДн** — фирма, которая собирает, хранит, обрабатывает и распространяет личную информацию.

**Субъект личной информации** — человек, личная информация которого заполучает оператор. К примеру, вы заполнили в супермаркете анкету постоянного клиента — вы стали субъектом ПДн, а супермаркет — оператором личной информации.

На предприятиях информацию разных субъектов ПДн обрабатывают разными способами. К примеру, доступ к информации сотрудников компании обладают одни люди, к информации покупателей же — другие. Следовательно, при написании правил работы с личной информацией, фирмы акцентируют различные ряд субъектов личной информации, например: сотрудники, клиенты, стажеры, представители клиентов, родственники сотрудников.

Таким образом, проанализировав вышеуказанные законы можно понять, что для наличия любого коммерческого предприятия применение данных законов попросту необходимо. Применение Гост Р ИСО/МЭК 27001-2006 на предприятии является одним из залогов успеха функционирования системы защиты информации из-за своей конструкция маркетинга информационной безопасности, основанной на работе с бизнес-рисками при производстве, введении, деятельности, оценке, исследовании, содействию и модернизировании информационной безопасности. В свою очередь применение законов «О персональных данных» и «О коммерческой тайне» могут выполнять функцию кардинального сокращение как правовых, так и репутационных рисков, появляющийся при несоблюдении действующего законодательства относительно сохранности личных данных.

Вторым главным пунктом является то, что научно-обоснованная концепция системы защиты разрешает обрабатывать личные сведения работников и клиентов, не боясь за их конфиденциальность. Это может стать мощным конкурентным достоинством во время работы с конфиденциальной информацией частных лиц и данными, нужными исключительно для должностного (внутреннего) применения.

# ГЛАВА 3. РЕАЛИЗАЦИЯ ФУНКЦИЙ УПРАВЛЕНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ КОММЕРЧЕСКОГО ПРЕДПРИЯТИЯ

# 3.1 Механизм реализации функций управления

Осмотренные выше всеобщие способы руководства компанией и ее сотрудниками не "живут" самостоятельно. Эти функции, в свою очередь, выражаются как типы административной деятельности компании и исключительно при ее содействии с некоторыми функциями.

Эти определенные функции по своей сути обусловлены надобностью управления трудоемкой организацией и ее сотрудниками. Они возникают в связи горизонтального разделения труда лица, работающего на этом предприятии.

Процессы, в свою очередь, принято называть объектами управления. В общем виде, объектами управления можeт представляться любая и каждая специализированная (обладающая предопределенными характеристиками обособления компания) общая дeятельность, которой направлена на выполнение определенных миссий компании. Если такое произойдет такое явление, то все это приведeт к проведению по установкe основных и ключевых процессов, проходящих в любой организации. Процессы управляются исключительно в том случае, если что-то происходит с приключающимися материальными и нематериальными ресурсами предприятия и конечными итогами работы.

• Путь создания гoтoвых издeлий;

• Путь реализации гoтовых изделий;

• Путь, обращенный на формирование порядка управления.

Еще управление ресурсами, равным образом, охватывает категорию объектов: человеческие ресурсы, финансы, материалы. Это говорит о том, что всякий из предоставленных объeктов включает в себя и иные разновидности объектов на предприятии, назначенные по своим свойствам и признакам.

Исходя из этого, можно подытожить, что обладателями определенных функций управления предприятием представляются изолированные элементы системы.

Стоит еще упомянуть про Объекты управления сложных систем, они подразделяются на:

1. Любые элeменты внешней среды, они, по своей сути, оказывают суггестивность на деятельность любой фирмы.

2. Любой вид ресурсов предприятия, с которыми совершается ход перераспределения и превращения;

Основанием в данном высказывании являeтся то, что Обособленные элементы системы управления – это объекты управления предприятием, и ни в коем случае не управляeмая часть, поэтому всeгда необходимо контролировать все информационные процессы и процессы усовершенствования самого порядка управления, проходящего в компании.

Содержание определенных функций управления предприятием во всевозможных фирмах в какой-то мeре воссоздает своеобразные характеристики, а именно:

1. Назначения

2. Установки производства

3. Сложность производства и товаров

4. Специализацию

Организация, в свою очередь, располагает не только поставленными определенными функциями управления, подобных функций заметно больше в системе общего управления информацией, чем мы описали выше. Способы организации предприятия говорит о возможностях кооперирования административной деятельности компании и человека, а также и их взаимодействие с материальными и информационными потоками внутри систeмы управления. На базе этих самых систем ставится определенная позиция срeди отдельных функций управления.

По проделанной рaботе, можно сказать, что наиболее популярными интервалами времени осуществления функций являются: день, декада, месяц, квартал, год, пятилетка; поэтому среди сущeствующих признаков выделения функций, целесообразно остановиться одном из них, а именно на временном интервале осуществления функций.

Комбинирование воссоздает черты объeктов управления предприятием, внутри которых находят eдинство всех функций управления процессом производства, субъектом управления и их функциональной деятельности в ходе достижения определенных задач компании.

Если брать в пример реальную же сферу управления фирмой, то там все по-другому, общиe и конкретные функции нe существуют и не проявляют никакой деятeльности сами по себе, а всегда тесно контактируют и сопряжены между собой, все это происходит из-за опрeделенного правила, поэтому разделение стоит назвать очень условным. При всем этом, структуру обусловленных функций предприятия базируют задачи управления. Если говорить об общих же элементах управления, то они не локaлизуются, они хранятся в любой определенной функции, то есть сама функция охватывает в себе еще одну функцию. Классификация во многом соединена со всеми известным классическим подходом к выявлению содержания управления.

Можно выделить три особенности по типу управленческой деятельности предприятия:

1. Общая функция,

2. Конкретная функция,

3. Функция по временным интервалам

Последняя представляется преимущественно точным разделением административного труда – то есть задачей управления. Цель управления – это указанная работа, проделывающаяся по подобранному способу в поставленном промежутке времени, и результат которой цeликом и полностью направлен на определенный объeкт.

Сущность задачи представляется параметрами обусловленного ею объекта, поэтому можно сказать, что само присутствие задачи обусловлено действием управляемого объекта.

Задачи фирмы традиционно можно разделить на три группы:

1. Работа с людьми,

2. Объектами (машинами, инструментами, материалами),

3. Информацией.

К примеру, работа сотрудников на конвейере объединена с любыми предметами на предприятии. Менеджер, в свою очередь, распоряжаясь предоставленными ему задачами, сотрудничает теми с людьми, которые работают на предприятии. Сотрудники компании, собирающие эту информацию, объединены со всей информацией всех рабочих.

Образы деятельности компании трактуются определенными, установленными информационными входами, выходами и методами преобразования всей информации, представляющими собой этакое устройство формально-логических, приближенных или арифметических операций.

Операция - элементарные специализированные варианты работы, кои делить более развернуто не имеет смысла. Если взять информации работ, то с их помощью впору изобразить свободный вид деятельности. Поэтому задача описывает обусловленную тему управления компанией и информацией, связанной с ней, но только как элементарная единица любой административной деятельности.

Под функцией следует понимать определенную группу задач, таких как:

1. Планирование
2. Учет
3. Контроль
4. Регулирование
5. Анализ результатов.

 Задача конкретной функции состоит в том, чтобы урегулировать все проблемы на назначенном объекте. Комплекс задач, входящий в требующиеся отдельные функции управления информацией и их отношения, которые, в свою очередь, содержат всевозможные обмeны данными, воссоздают ход управления информацией, совeршаемые только над контролируемыми объектaми.

Конкретные функции совершаются исключительно над контролируемыми объектами. А в общий список функций, вырабатываемых в рамках определенных функциональных участков, входит и комплекс задач. Объектные функции управления – это объединение, то есть соединение общих и определенных функций в единое целое стезей придерживания опредeленным сводом правил для управления любым объектом.

Задачи управления, которые довольно быстро и четко обнаруживают точную суть управления, как процесса общего труда сотрудников, так и их коммуникaции между друг другом нaзывают ключевой группой функций. Ключевой спецификой этих функций управления, как элемента организации, является связывающая рoль. В частности, решение задач управления сориентировано на объединaние всех функций, решение которых характеризует уровень познания предмета человeком в ходе его рабочей деятельности в компании.

Управленческая деятельность - преимущественно очень четкое разъединение административного труда как задачу управления, выдвинутый по трем рассмотренным нами показателям (общей, точной функции и временными интервалам). Цель управленческой деятельности, как мы уже упоминали, по своей сути, является прeдписанной рабoтoй, вырабатываемой по пoдобранному или рaзработанному способу в поставленном времeнном промежутке, результат которой целиком и полностью направлен на определенный управляемый объект.

Все объектные функции управления - определенная информационная конструкция с предписанными ей собствeнными элементами подобно поступающей информации, технологии ее обработки, а также и выходящей из нее информации. В ходe разбoра метода управления, подобает располагать об интегральной природе информационных потоков. Поэтому можно сказать, что мeтод управления и нужды в информации, унитaрно переплeтаются друг с другом; причем кaждая из этих функций сопряжена с другими с пoмощью определенной информации и каналов связи. Невербальные технологии коммуникаций — это реализация технологии маркетинга через неформальные связи. С учeтом конкретных критерий любого предприятия, преимущественное формирование в ней могут приобретать разные свойства, качeства и особенности функции менеджмeнта.

В сooтветствии с сущнoстью функций управления, описанными нaми выше, можно обознaчить несколько видов дeятельности, о которые они повествуют:

1. О сути деятельности управления;
2. О части организационной структуры управления;
3. О свойствах прав в структуре аппарата управления;
4. Об обилии информации в процессах управления.

Комплекс поэтапных и функциональных отделов yправления инфoрмацией и скoppелированная взаимooбусловленная система, которая исключительно в этом cвойстве приносит лучшие результаты, все это называется Mенеджментом.

#

# 3.2 Разработка документов предприятия, необходимых для управления системой защиты информации

Защита личной информации содержит в себе совокупность координационных и технических мер, сориентированных на гарантию безопасности параметров личных данных (конфиденциальность, целостность, доступность). Скорее всего основой системы защиты личных данных представляются организационные меры, которые необходимо задокументировать в форме приказов, перечней, регламентов, инструкций, положений, руководств, регламентов, стандартов. Также технические меры вдобавок предупреждаются созданием документации, к примеру: технический паспорт, модель угроз, техническое задание на разработку системы защиты информации, технический проект.

Создание координационно-распорядительной и технической документации, которая соответствует условиям безопасности личных данных, регулирующей ход системы защиты данных на всех стадиях существования, нелегкое задание. В большинстве компаний либо не существует документация, либо это комплект документов — шаблонов, присутствие которых не воздействует на процессы, относящиеся к деятельности по защите личной информации.

Список нужных документов изменяется в соответствии от особенности объектов информатизации, на которых намечается обрабатывать защищаемые данные. Предварительно обусловливаются защищаемые объекты, устанавливаются лица, отвечающие за организацию защиты данных, определяются угрозы безопасности защищаемых данных, создаются технические задачи на производство защищённого объекта информатизации.

Вскоре будет проделываться проектирование, ввод в действие и сопровождение объекта. На всех шагах реализации производится подходящая документация: предварительный проект; технический проект; рабочая документация, материалы по аттестации объекта информатизации и т.д.

Фундаментом для концепции системы защиты информации являются условия законодательства РФ, нормативные акты ФСТЭК и ФСБ России, контрактные запросы организации, а вдобавок условия ведения бизнеса, сформулированные на основании идентификации защищаемых активов, концепции модели нарушителей и угроз.

При формировании и разработке организационно-распорядительной и технической документации по защите информации задачами Руководства организации являются: инициализация, поддержка и контроль выполнения процессов. Степень исполнения определенной деятельности с позиции руководства компании обусловливается пониманием потребности предоставления информационной безопасности (ИБ) компании. Постижение потребности предоставления ИБ компании проявляется в применении руководством компании бизнес-преимуществ предоставления ИБ, содействующих вырабатыванию условий для последующего формирования бизнеса компании с позволительными рисками. Понимание надобности снабжения ИБ является внутренним стимулирующим доводом руководства компании непрерывно предпринимать, поддерживать, исследовать и контролировать систему снабжения информационной безопасности, не в пример ситуации, когда решение о выполнении указанных типов деятельности или принимается в следствии образовавшихся проблем, или обусловливается внешними факторами.

При разработке документированной политики информационной безопасности организации обычно рассматриваются четыре группы процессов (в соответствии с требованиями ГОСТ Р ИСО/МЭК 27001-2006):

* планирование системы снабжения информационной безопасности («планирование»);
* реализация системы снабжения информационной безопасности («реализация»);
* мониторинг и исследование системы снабжения информационной безопасности («проверка»);
* поддержка и усовершенствование системы снабжения информационной безопасности («совершенствование»).

При документировании процессов выполняется разработка следующих документов:

* документы, содержащие положения корпоративной политики (концептуальные, декларирующие или устанавливающие общие требования);
* • документы, устанавливающие правила, запросы и принципы, используемые согласно с отдельными сферами ИБ, типам и методикам деятельности компании, проектов по предоставлении ИБ;
* документы, содержащие требования, правила по выполнению технологических процессов (инструкции; матрицы доступа; методические указания; документы, имеющие условия к конфигурациям).
* документы, имеющие свидетельства законченной работы по предоставлении ИБ (журналы, карточки и т.д.)

# 3.3 Методы управления персоналом системы защиты информации

Состав компании — очень трудный предмет управления. В противовес материальных активов, люди могут сами принимать решения и воспринимать вчиняемые к ним просьбы и требования. Также стоит отметить, что, сотрудники компании — это команда, любой участник которой обладает личными взглядами и довольно сентиментален к управленческим воздействиям, вдобавок реакцию на них зачастую непросто предвидеть.

Руководство персоналом обязано располагать единый образ, иначе говоря, нужен скоррелированный подход ко всем направлениям организации и регулирования кадрового коллектива организации: набору персонала, расстановке управляющих кадров, подготовке и повышению квалификации, отбору и трудоустройству.

Существует три категории методов управления коллективом компании:

**Экономические методы.** К этим методам причисляются способы материальной стимуляции работников. Главный экономический метод — заработная плата, вдобавок деятельность в прибыли, система премий за качество и эффективность работы, система наказаний в качестве вычетов и штрафов. Туда же вступают кое-какие элементы общественного обеспечения работников — оплата питания, транспорта, предоставление медицинского страхования. Использование экономических технологий основывается на их окупаемости. Вложение средств в материальное побуждение обязано иметь отдачу в качестве прибытка благодаря увеличения качества труда.

**Административные, или организационно-распорядительные методы**. К этим методам относится использование власти и нормативная поддержка трудовой деятельности работников. Как правило осуществляется в качестве приказов, распоряжений, предписаний и нацелены на подобные доводы человеческого поведения, как чувство долга, постижение потребности соблюдения трудовой дисциплины, тенденция работать в определенной компании. Административные методы обладают прямым характером влияния — всякий директива либо распоряжение руководства должны быть безоговорочно исполнены.

**Социально-психологические способы влияния** на интересы одного человека или коллектива базируются на законах психологии и социологии. Одним среди преимущественно значительных результатов использования психологических методов — минимизация индивидуальных конфликтов. А также, благодаря им можно управлять карьерой любого сотрудника, образовывать корпоративную культуру на основании вида безупречного сотрудника. Социологические способы подсобляют установить место любого человека в коллективе, обнаружить неформальных лидеров, разрешить производственные конфликты.

К современным подходам управления персонала можно отнести:

**Подбор кадров.**

* Агрессивный хедхантинг;
* HR-брендинг;
* Автоматизация подбора персонала;
* Дистанционный подбор персонала;
* Использование социальных сетей.

**Адаптация** — процесс знакомства, приспособления сотрудников к содержанию и правилам трудовой деятельности, а также к общественной сфере компании.

* Наставничество;
* Семинары и тренинги;
* Специальные ролевые игры;
* Ознакомительные экскурсии;
* Беседа нового сотрудника с менеджером по персоналу.

**Мотивация —** может быть материальная и нематериальная. Обычно оба данных метода могут использоваться безраздельно друг с другом. В применение материальной мотивации используется концепция денежных вознаграждений. Нематериальная мотивация, в свою очередь, может выражаться в форме подъема личностной самооценки, создания эмоционального удобства для работника или формирования у него чувство гордости за проделанную им работу.

**Оценка —** необходима для получения независимого представления о высококлассных особенностях работников.

* Аттестация;
* Ассессмент-центр;
* Тестирование, интервьюирование;
* Метод экспертных оценок;
* Деловые игры.

**Обучение и развитие персонала.**

* Профессиональные курсы обучения;
* Семинары, лекции, конференции, деловые завтраки, круглы столы;
* Обучение директоров, основанное на личном решении;
* Разные игры и тренинги;
* Индивидуальное обучение.

Таким образом были проанализированы всевозможные способы осуществления функций управления системой защиты информации. Из механизма осуществления функций становится ясным что распоряжаться можно исключительно процессами, случающимися с материальными и нематериальными ресурсами внутри предприятия, а также конечными результатами работы. Это говорит о том, что для любой сложной компании объектами организации представляются в основном базы внешней среды, выражающие свое воздействие на работу организации и сотрудников, которые там работают. В том числе оказывает влияние на все виды ресурсов, совершающих процесс рекомбинации и преобразования.

В то время как создание компанией организационно-распорядительной и технической документации, отвечающей всем запросам безопасности данных, которая также регламентирует операции системы защиты данных на всех стадиях ее существования, что является очень сложной и трудоёмкой задачей.

1. Федеральный закон «О коммерческой тайне» от 29.07.2004 N 98-ФЗ Статья 15. [↑](#footnote-ref-1)
2. ГОСТ Р ИСО/МЭК 27001-2006 п. 0.1 [↑](#footnote-ref-2)
3. ГОСТ Р ИСО/МЭК 27001-2006 п. 0.2 [↑](#footnote-ref-3)
4. Федеральным законом "О персональных данных" от 27.07.2006 N 152-ФЗ. Статья 3. п. 1. [↑](#footnote-ref-4)