Практическая работа № 1

Классификация защищаемой информации

Задачи практической работы:
– Классифицировать защищаемую информацию по конфиденциальности;
– Определить категории лиц, имеющих доступ к защищаемой информации и ресурсам.

Ход выполнения практической работы:

1. Повторить теоретические вопросы о категорировании информации.

Информация, обрабатываемая в ИС
Обрабатываемая в ИС информация включает в себя:
– открытую (общедоступную) информацию;
– информацию ограниченного доступа (персональные данные).
Персональные данные, обрабатываемые в типовой ИС, могут включать в себя:
– персональные данные сотрудников:
а) биографические данные;
б) опознавательные данные;
в) личные характеристики;
г) сведения о семейном положении;
д) сведения о финансовом положении;
е) сведения об образовании;
ж) сведения о профессиональных навыках;
з) сведения о состоянии здоровья;
– персональные данные иных субъектов, в том числе:
а) информация о гражданах (персональные данные);
б) персональные данные о гражданах в их заявлениях и жалобах;
в) сведения, содержащиеся в записях актов гражданского состояния;
г) сведения о населении, содержащиеся в переписных листах;
д) иные персональные данные.
Таким образом, в типовых ИС обрабатываются персональные данные следующих категорий:
– *категория 1* - персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;
– *категория 2* - персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1;
категория 3 - персональные данные, позволяющие идентифицировать субъекта персональных данных.

Информация составляет СЛУЖЕБНУЮ или КОММЕРЧЕСКУЮ ТАЙНУ в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании, и обладатель информации принимает меры к охране ее конфиденциальности. Сведения, которые не могу составлять СЛУЖЕБНУЮ или КОММЕРЧЕСКУЮ ТАЙНУ, определяются законом и иными правовыми актами.

Коммерческая тайна - управленческая, производственная, научно-техническая, финансовая, экономическая, торговая и иная документированная информация, используемая для достижения целей предпринимательской деятельности (получение прибыли, предотвращение ущерба и упущенной выгоды, получение добросовестного преимущества над конкурентами), которую предприниматель относит к конфиденциальной.

Конфиденциальная информация - документированная информация, правовой режим которой установлен специальными нормами действующего законодательства в области государственной, коммерческой, промышленной и другой общественной деятельности.

Указом Президента Российской Федерации от 6 марта 1997 года № 188 утвержден перечень

сведений конфиденциального характера:

1. Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.

2. Сведения, составляющие тайну следствия и судопроизводства.

3. Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна).

4. Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее).

5. Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна).

6. Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

Предварительный Перечень сведений, составляющих служебную или коммерческую тайну, формируется под руководством начальников структурных подразделений организации в соответствии с указаниями начальника службы безопасности (заместителя по режиму) и Положением о порядке и методических указаниях по его формированию.

При разработке предварительного Перечня в структурных подразделениях должны руководствоваться:

• Конституцией Российской Федерации, принятой 12 декабря 1993 года;

• Законом Российской Федерации «О государственной тайне» № 5485-1 от 21.07.93;

• Федеральным законом Российской Федерации «Об информации, информатизации и защите информации» № 24-ФЗ от 20.02.95;

• Указом Президента Российской Федерации «Об утверждении Перечня сведений, отнесенных к государственной тайне» № 1203 от 30.11.95;

• Указом Президента Российской Федерации «Об утверждении Перечня сведений конфиденциального характера» № 188 от 06.03.97;

• Постановлением Правительства Российской Федерации «О Перечне сведений, которые не могут составлять коммерческую тайну» № 35 от 05.12.91;

• анализом характера возможного ущерба в случае несанкционированного распространения сведений конфиденциального характера;

• анализом преимуществ и недостатков для работы с открытым и закрытым (внутренним) применением таких сведений.

Примерный перечень сведений, составляющих служебную или коммерческую тайну организации:

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

Сведения о применяемых оригинальных методах управления организацией. Сведения о подготовке, принятии и исполнении отдельных решений руководства организации по коммерческим, организационным, научно-техническим и иным вопросам.

Сведения о планах расширения или свертывания производства различных видов продукции и их технико-экономических обоснованиях. Также сведения о планах инвестиций, закупок и продаж.

Сведения о фактах проведения, целях, предмете и результатах совещаний и заседаний органов управления организации.

Сведения о кругообороте средств организации, финансовых операциях, состоянии банковских счетов организации и проводимых операциях, об уровне доходов организации, о состоянии кредита организации (пассивы и активы). Главная книга организации.

Сведения о применяемых организацией оригинальных методах изучения рынка (маркетинга).

Сведения о результатах изучения рынка, содержащие оценки состояния и перспектив развития рыночной коньюктуры. Сведения о рыночной стратегии организации, о применяемых организацией оригинальных методах осуществления продаж, об эффективности служебной или коммерческой деятельности организации.

Обобщенные сведения о внутренних и зарубежных заказчиках, подрядчиках, поставщиках, потребителях, покупателях, компаньонах, спонсорах, посредниках, клиентах и других партнерах, состоящих в деловых отношениях с организацией.

Обобщенные сведения о внутренних и зарубежных предприятиях как потенциальных конкурентах в деятельности организации, оценке качества деловых отношений с конкурирующими предприятиями в различных сферах деловой активности.

Сведения о подготовке, проведении и результатах переговоров с деловыми партнерами организации.

Сведения об условиях конфиденциальности, из которых можно установить порядок соглашения и другие обязательства организации с партнерами (клиентами, контрагентами).

Сведения о методах расчета, структуре, уровне реальных цен на продукцию и размеры скидок.

Сведения о подготовке к участию в торгах и аукционах, результатах приобретения или продажи на них товаров.

Сведения о целях, задачах, программах перспективных научных исследований. Ключевые идеи научных разработок, точные значения конструкционных характеристик, создаваемых изделий и оптимальных параметров разрабатываемых технологических процессов (размеры, объемы, конфигурация, процентное содержание компонентов, температура, давление, время и т. д.). Аналитические и графические зависимости, отражающие найденные закономерности и взаимосвязи, данные об условиях экспериментов и оборудовании, на котором они проводились. Сведения о материалах, из которых изготовлены отдельные детали, об особенностях конструкторско-технологического, художественно-технического решения изделия, дающие положительный экономический эффект.

Сведения о методах защиты от подделки товарных и фирменных знаков, о состоянии парка ПЭВМ и программного обеспечения.

Сведения об особенностях используемых и разрабатываемых технологий и специфике их применения, об условиях их производства и транспортировке продукции.

Сведения о порядке и состоянии организации защиты служебной или коммерческой тайны, о порядке и состоянии организации охраны, системы сигнализации, пропускном режиме.

Сведения, составляющие служебную или коммерческую тайну организаций, предприятий-партнеров и передаваемые ими в пользование на доверительной основе.

2. Используя документы «Должностные инструкции», определить наличие информации с ограниченным доступом для каждой должности. Определить конфиденциальность информации и принадлежность её к определенному виду тайны. Результаты исследований поместить в таблицу 1. Перечень законов по информационной безопасности приведён в Приложении Г.

Таблица 1 – Классификация информации по конфиденциальности

Должность	Документ	Реквизиты документов	Конфиденциальная информация. Вид тайны.	Закон, на основании которого у информации статус конфиденциальной
Начальник отдела кадров	Анкета По должностной инструкции	Фамилия Имя Отчество	Персональные данные Коммерческая тайна	Ст11ФЗ «Об информации, информатизации и защите информации»

3. Ответить на вопросы по теоретическому материалу

ПРИЛОЖЕНИЕ А

ПОЛИТИКИ БЕЗОПАСНОСТИ НА ПРЕДПРИЯТИИ «ЗАО «СПЕЦСТРОЙ»»

Абонентский пункт (АП) - автоматизированная система, подключаемая к Сети с помощью коммуникационного оборудования и прёдназначенная для работы абонента Сети.

Защищаемые помещения (ЗП) - помещения (служебные кабинеты, актовые, конференц-залы и т.д.), специально предназначенные для проведения конфиденциальных мероприятий (совещаний, обсуждений, конференций, переговоров и т.п.).

Контролируемая зона (КЗ) - это пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание сотрудников и посетителей организации, а также транспортных средств.

Границей КЗ могут являться:

• периметр охраняемой территории организации;

• ограждающие конструкции охраняемого здания или охраняемой части здания, если оно размещено на неохраняемой территории.

В отдельных случаях, на период обработки техническими средствами конфиденциальной информации, границы КЗ временно могут расширяться. При этом должны приниматься организационные и технические меры, исключающие или существенно затрудняющие возможность ведения перехвата информации в этой зоне.

Вход в здание предприятия «ЗАО «Спецстрой»» осуществляется по карточкам (система электронная проходная). Так же на входе сидят два охранника, по периметру здания установлено видеонаблюдение.

На предприятии «ЗАО «Спецстрой»» документально определен перечень ЗП (защищенных помещений) и лиц, ответственных за их эксплуатацию в соответствии с установленными требованиями по защите информации, а также составлен технический паспорт на ЗП.

Защищаемые помещения размещаются в пределах контролируемой зоны (КЗ) организации. Окна ЗП закрываются жалюзи.

При эксплуатации ЗП предусмотрены организационные меры, направленные на исключение несанкционированного доступа в помещение:

• двери ЗП в период между мероприятиями, а также в нерабочее время, запирают на ключ;

• выдача ключей от ЗП производится лицам, работающим в нем или ответственным за это помещение;

• установка и замена оборудования, мебели, ремонт ЗП производится только по согласованию и под контролем подразделения (специалиста) по защите информации.

Системы пожарной и охранной сигнализации ЗП строится по проводной схеме сбора информации (связи с пультом) и размещается в пределах одной с ЗП контролируемой зоне.

Для исключения возможности утечки информации за счет электроакустического преобразования оконечные устройства телефонной связи, имеющие прямой выход в городскую АТС, оборудовано сертифицированными средствами защиты информации от утечки за счет электроакустического преобразования.

Во время проведения конфиденциальных мероприятий запрещается использование в ЗП радиотелефонов, оконечных устройств сотовой, пейджинговой и транкинговой связи, не защищенных переносных магнитофонов и других средств аудио - и видеозаписи. При установке в ЗП телефонных и факсимильных аппаратов с автоответчиком или спикерфоном, а также телефонных аппаратов (ТА) с автоматическим определителем номера, их отключают из сети на время проведения этих мероприятий или использовать соответствующие средства защиты.

Основными направлениями защиты информации на предприятии «ЗАО «Спецстрой»» являются:

• обеспечение защиты информации от хищения, утраты, утечки, уничтожения, искажения, подделки и блокирования доступа к ней за счет НСД и специальных воздействий;

• обеспечение защиты информации от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи.

В качестве основных мер защиты информации на предприятии «ЗАО «Спецстрой»»:

• организовано документальное оформление перечня сведений конфиденциального характера, в том числе с учетом ведомственной и отраслевой специфики этих сведений;

• организована реализация разрешительной системы допуска исполнителей (пользователей, обслуживающего персонала) к информации и связанным с ее использованием работам, документам;

• организовано ограничение доступа персонала и посторонних лиц в ЗП и помещения, где размещены средства информатизации и коммуникационное оборудование, а также хранятся носители информации;

• организовано разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;

• организована регистрация действий пользователей АС и обслуживающего персонала, контроль несанкционированного доступа и действий пользователей, обслуживающего персонала и посторонних лиц;

• организован учет и надежное хранение бумажных и машинных носителей конфиденциальной информации и их обращение, исключающее хищение, подмену и уничтожение;

• организовано резервирование технических средств, дублирование массивов и носителей информации;

• организовано использование сертифицированных средств защиты информации;

• организовано использование сертифицированных систем гарантированного электропитания (источников бесперебойного питания);

• использование защищенных каналов связи

Основные требования и рекомендации по защите информации

АС, обрабатывающие информацию на предприятии «ЗАО «Спецстрой»» содержащую сведения, составляющие служебную тайну, или персональные данные, имеют класс защищенности не ниже 3Б, 2Б и 1Г. и 3Б, 2Б и 1Д соответственно.

Для повышения уровня защищенности информации используются сертифицированные по требованиям безопасности информации СВТ.

Для передачи информации по каналам связи, выходящим за пределы КЗ, используются защищенные каналы связи, в том числе защищенные волоконно-оптические линии связи, а при использовании открытых каналов связи, применяются криптографические средства защиты информации. Применяемые средства защиты информации сертифицированы.

Носители информации на магнитной (магнитооптической), оптической и бумажной основе учитываются, хранится и уничтожатся в подразделениях организаций в установленном порядке.

Порядок обеспечения защиты информации при эксплуатации АС на предприятия «ЗАО «Спецстрой»»

Для обеспечения защиты информации в процессе эксплуатации АС на предприятия «ЗАО «Спецстрой»» предусмотрены следующие основные положения и требования:

• допуск к защищаемой информации лиц, работающих в АС (пользователей, обслуживающего персонала), производится в соответствии с порядком, установленным разрешительной системой допуска;

• на период обработки защищаемой информации в помещениях, где размещаются ОТСС, находятся только лица, допущенные в установленном порядке к обрабатываемой информации, допуск других лиц для проведения необходимых профилактических или ремонтных работ осуществляется в эти помещения только с разрешения руководителя организации или руководителя службы безопасности;

• по окончании обработки информации пользователь производит стирание остаточной информации на несъёмных носителях (жестких дисках) и в оперативной памяти;

• изменение или ввод новых программ обработки защищаемой информации в АС осуществляется совместно разработчиком АС и администратором АС, при этом АС подлежит переаттестации;

• при увольнении или перемещении администраторов АС руководителем организации по согласованию со службой безопасности принимаются меры по оперативному изменению паролей и идентификаторов.

Учет съемных носителей информации, а также распечаток текстовой, графической и иной информации на бумажной или пластиковой (прозрачной) основе, осуществляется по карточкам или

журналам установленной формы, в том числе автоматизировано с использованием средств вычислительной техники.

Защита информации в локальных вычислительных сетях

Конфиденциальная информация предприятия «ЗАО «Спецстрой»» обрабатывается только в ЛВС, расположенных в пределах КЗ.

Средства защиты информации от НСД на предприятии «ЗАО «Спецстрой»» используются во всех узлах ЛВС, независимо от наличия (отсутствия) конфиденциальной информации в данном узле ЛВС. Постоянно квалифицированно контролируются настройки СЗИ системными администраторами.

Состав пользователей ЛВС устанавливается письменным распоряжением руководителя организации (структурного подразделения) и контролируется. Все изменения состава пользователей, их прав и привилегий регистрируются.

Каждый администратор и пользователь имеет уникальные идентификатор и пароль.

Защита информации при работе с системами управления базами данных

При работе с системами управления базами данных (СУБД) и базами данных (БД) учитываются следующие особенности защиты информации от НСД:

• в БД может накапливаться большой объем интегрированной информации по различным тематическим направлениям, предназначенной для различных пользователей;

• БД могут быть физически распределены по различным устройствам и узлам сети;

• БД могут включать различную конфиденциальную информацию;

• разграничение доступа пользователей к объектам БД (таблицам, схемам, процедурам, записям, полям записей в базах данных и т.п.), осуществляется только средствами СУБД;

• регистрация действий пользователей при работе с объектами БД осуществляется и средствами СУБД;

• СУБД обеспечивают одновременный доступ многих пользователей (клиентов) к БД с помощью сетевых протоколов, при этом - запросы пользователя к БД обрабатываются на сервере и результаты обработки направляются пользователям (клиентам).

Рекомендации по обеспечению защиты конфиденциальной информации, содержащейся в негосударственных информационных ресурсах, при взаимодействии абонентов с информационными сетями общего пользования.

Методами обеспечения безопасности информации при взаимодействии АП с Сетью на предприятии «ЗАО «Спецстрой»» являются:

• межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрытия структуры АП;

• мониторинг вторжений в ЛВС, нарушающих или создающих предпосылки к нарушению установленных в организации требований по защите информации;

• анализ защищенности АП, предполагающий применение специализированных программных средств (сканеров безопасности), позволяющих осуществлять анализ защищенности АП;

• шифрование информации при ее передаче по Сети, а также использование электронно-цифровой подписи для контроля целостности и подтверждения подлинности отправителя и/или получателя информации;

• использование смарт-карт, электронных замков и других носителей информации для надежной идентификации и аутентификации пользователей;

• использование средств антивирусной защиты;

• централизованное управление системой информационной безопасности АП.

ПРИЛОЖЕНИЕ Б

ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ БУХГАЛТЕРА

1. **Общие положения**

Бухгалтер руководствуется в своей деятельности:

- законодательными актами РФ;
- Уставом компании, Правилами внутреннего трудового распорядка, другими нормативными актами компании;
- Положением о бухгалтерии организации;
- приказами и распоряжениями руководства;
- настоящей должностной инструкцией.

2. Должностные обязанности бухгалтера

Бухгалтер исполняет следующие должностные обязанности:

2.1. Выполняет работу по ведению бухгалтерского учета имущества, обязательств и хозяйственных операций (учет основных средств, товарно-материальных ценностей, затрат на производство, реализации продукции, результатов хозяйственно-финансовой деятельности; расчеты с поставщиками и заказчиками, за предоставленные услуги и т.п.).

2.2. . Осуществляет прием и контроль первичной документации по соответствующим участкам бухгалтерского учета и подготавливает их к счетной обработке.

2.4. Отражает на счетах бухгалтерского учета операции, связанные с движением основных средств, товарно-материальных ценностей и денежных средств.

2.10. Выполняет работы по формированию, ведению и хранению базы данных бухгалтерской информации, вносит изменения в справочную и нормативную информацию, используемую при обработке данных.

2.11. Выполняет отдельные служебные поручения своего непосредственного руководителя.

3. Права бухгалтера

Бухгалтер имеет право:

3.1. Получать информацию, в том числе и конфиденциальную, в объеме, необходимом для решения поставленных задач.

3.2. Вносить предложения по совершенствованию работы, связанной с предусмотренными настоящей инструкцией обязанностями.

3.3. В пределах своей компетенции сообщать своему непосредственному руководителю о всех выявленных в процессе своей деятельности недостатках и вносить предложения по их устранению.

3.4. Запрашивать лично или по поручению главного бухгалтера от руководителей подразделений и специалистов информацию и документы, необходимые для выполнения его должностных обязанностей.

3.5. Требовать от руководства предприятия оказания содействия в исполнении своих должностных обязанностей и прав.

4. Ответственность бухгалтера

Бухгалтер несет ответственность:

4.1. За невыполнение и/или несвоевременное, халатное выполнение своих должностных обязанностей.

4.2. За несоблюдение действующих инструкций, приказов и распоряжений по сохранению коммерческой тайны и конфиденциальной информации.

4.5. За причинение материального ущерба - в пределах, определенных действующим трудовым и гражданским законодательством Российской Федерации.

Перечень документов, с которыми работает бухгалтер:

- расходный кассовый ордер;

- приходный кассовый ордер;
- товарная накладная.

ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ НАЧАЛЬНИКА ОТДЕЛА КАДРОВ

1. Общие положения

2. Должностные обязанности начальника отдела кадров

Начальник отдела кадров выполняет следующие должностные обязанности:

2.1. Определяет совместно с руководителями структурную подразделений текущую потребность в кадрах, принимает участие в разработке кадровой политики предприятия.

2.2. Возглавляет работу по подбору, отбору и расстановке кадров на основе оценки их квалификации, личных и деловых качеств.

2.3. Обеспечивает прием, размещение и расстановку молодых специалистов, совместно с руководителями подразделений организует их стажировку и адаптацию в компании.

2.4. Организует проведение аттестации сотрудников компании, ее методическое и информационное обеспечение, принимает участие в анализе результатов аттестации, разработке мероприятий по реализации решений аттестационных комиссий, определяет круг специалистов, подлежащих повторной проверке.

2.5. Участвует в разработке систем комплексной оценки работников и результатов их деятельности, служебно-профессионального продвижения персонала, подготовке предложений по совершенствованию проведения аттестации.

2.6. Организует своевременное оформление приема, перевода и увольнения работников в соответствии с трудовым законодательством, положениями, инструкциями и приказами руководителя предприятия.

2.7. Контролирует ведение кадрового делопроизводства в компании.

2.8. Осуществляет методическое руководство и координацию деятельности специалистов и инспекторов по кадрам подразделений предприятия, контролирует исполнение руководителями подразделений законодательных актов и постановлений правительства, постановлений, приказов и распоряжений руководителя предприятия по вопросам кадровой политики и работы с персоналом.

2.9. Проводит систематический анализ кадровой работы на предприятии, разрабатывает предложения по ее улучшению.

2.10. Разрабатывает мероприятия по укреплению трудовой дисциплины, снижению текучести кадров, потерь рабочего времени, контролирует их выполнение.

2.11. Обеспечивает составление установленной отчетности по учету персонала и работе с кадрами.

3. Права начальника отдела кадров

Начальник отдела кадров имеет право:

3.1. Знакомиться с проектами решений руководства компании, касающимися деятельности отдела кадров и работы с персоналом.

3.4. Подписывать и визировать документы в пределах своей компетенции.

3.5. Запрашивать от руководителей структурных подразделений предприятия, специалистов и рабочих необходимую для исполнения своих должностных обязанностей информацию.

4. Ответственность начальника отдела кадров

Начальник отдела кадров несет ответственность:

4.2. За несоблюдение действующих инструкций, приказов и распоряжений по сохранению коммерческой тайны и конфиденциальной информации.

ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ ИНЖЕНЕРА-ПРОЕКТИРОВЩИКА

1. Общие положения

.

.2. Должностные обязанности проектировщика

Проектировщик выполняет следующие должностные обязанности:

2.1. На основе новейших научно-технических достижений, передового отечественного и зарубежного опыта проектирования, строительства и эксплуатации объектов и с использованием средств автоматизации проектирования разрабатывает отдельные разделы (части) проекта.

2.2. Принимает участие в подготовке заданий на разработку проектных решений.

2.3. Участвует в сборе исходных данных для проектирования, в решении технических вопросов по закрепленным объектам на протяжении всего периода проектирования, строительства, ввода в действие объекта и освоения проектных мощностей.

2.4. Увязывает принимаемые проектные решения с проектными решениями по другим разделам (частям) проекта.

2.5. Проводит патентные исследования с целью обеспечения патентной чистоты новых проектных решений и патентоспособности.

2.6. Обеспечивает соответствие разрабатываемых проектов и технической документации стандартам, техническим условиям и другим нормативным документам по проектированию и строительству, а также заданию на их разработку.

2.7. Осуществляет авторский надзор за строительством проектируемых объектов, консультирует по вопросам, входящим в его компетенцию.

2.8. Участвует в анализе и обобщении опыта разработки проектов и их реализации в строительстве и на этой основе готовит предложения о целесообразности корректировки принятых общих и принципиальных проектных решений.
2.9. Принимает участие в составлении заявок на изобретения, подготовке заключений и отзывов на рационализаторские предложения и изобретения, проекты стандартов, технических условий и других нормативных документов, в работе семинаров и конференций. 2.10. Выполняет отдельные служебные поручения своего непосредственного руководителя.

3. Права проектировщика

Проектировщик имеет право:

3.1.Вносить на рассмотрение руководства предложения по совершенствованию работы, связанной с предусмотренными настоящей инструкцией обязанностями.

3.2.Привлекать специалистов всех структурных подразделений с разрешения руководства к решению задач, возложенных на него.

3.3.Запрашивать лично или по поручению руководства предприятия у руководителей структурных подразделений и специалистов информацию и документы, необходимые для выполнения должностных обязанностей.

4. Ответственность проектировщика

Проектировщик несет ответственность за:

4.1. Причинение материального ущерба — в пределах, определенных действующим трудовым и гражданским законодательством Российской Федерации.

4.2. Разглашение коммерческой тайны предприятия.

ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ СИСТЕМНОГО АДМИНИСТРАТОРА

1. Общие положения

1.1. Системный администратор руководствуется в своей деятельности:

- законодательными актами РФ;
- Уставом компании, Правилами внутреннего трудового распорядка, другими нормативными актами компании;
- приказами и распоряжениями руководства;
- настоящей должностной инструкцией.

2. Должностные обязанности системного администратора

Системный администратор выполняет следующие должностные обязанности:

2.1.Устанавливает на серверы и рабочие станции сетевое программное обеспечение.

2.2. Конфигурирует систему на сервере.

2.3. Обеспечивает интегрирование программного обеспечения на файл-серверах, серверах систем управления базами данных и на рабочих станциях.

2.4. Поддерживает рабочее состояние программного обеспечения сервера и рабочих станций.

2.5. Регистрирует пользователей, назначает идентификаторы и пароли.

2.6. Обучает пользователей работе в сети, ведению архивов; отвечает на вопросы пользователей, связанные с работой в сети; составляет инструкции по работе с сетевым программным обеспечением и доводит их до сведения пользователей.

2.7. Контролирует использование сетевых ресурсов.

2.8. Организует доступ к локальной и глобальной сетям.

2.9. Устанавливает ограничения для пользователей по:

- использованию рабочей станции или сервера;
- времени;
- степени использования ресурсов.

2.10. Обеспечивает своевременное копирование и резервирование данных.

2.11. Участвует в восстановлении работоспособности системы при сбоях и выходе из строя сетевого оборудования.

2.12. Проводит мониторинг сети, разрабатывает предложения по развитию инфраструктуры сети.

2.13. Обеспечивает:

- сетевую безопасность (защиту от несанкционированного доступа к информации, просмотра или изменения системных файлов и данных);
- безопасность межсетевого взаимодействия.

3. Права системного администратора

Системный администратор имеет право:

3.1. Устанавливать и изменять правила пользования сетью.

3.2. Знакомиться с проектами решений руководства предприятия, касающимися его деятельности.

3.3. Сообщать своему непосредственному руководителю о всех выявленных в процессе своей деятельности недостатках и вносить предложения по их устранению.

3.5. Запрашивать лично или по поручению руководства предприятии от руководителей структурных подразделений и специалистов информацию и документы, необходимые для выполнения его должностных обязанностей.

4. Ответственность системного администратора

Системный администратор несет ответственность:

4.1. За несоблюдение действующих инструкций, приказов и распоряжений по сохранению коммерческой тайны и конфиденциальной информации.

ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ СМЕТЧИКА

1. Общие положения

2. Должностные обязанности сметчика

Сметчик выполняет следующие должностные обязанности:

2.1. Составляет сметно-финансовую документацию на ремонт оборудования, зданий и сооружений, реконструкцию действующих объектов и на работы по повышению эффективности производства.

2.2. Рассматривает и анализирует утвержденные титульные списки на капитальный ремонт, ведомости дефектов, ремонтные ведомости и рабочие чертежи объектов, подлежащих ремонту и реконструкции.

2.3. Подготавливает на основании анализа стоимости ремонта исходные данные для

определения сметной стоимости всех видов ремонтных (строительных, монтажных, сантехнических и т. п.) работ.

2.4. Вносит соответствующие уточнения и коррективы в сметно-финансовые расчеты в случае изменения цен или объемов работ.

2.5. Проверяет правильность составления смет расходов проектными организациями и готовит заключения по ним.

2.6. Участвует в определении стоимости ремонтных, монтажных и строительных работ, не предусмотренных утвержденными сметами, а также при замене материалов и оборудования.

2.7. Принимает участие в составлении титульных списков на объекты ремонта и реконструкции.

2.8. Согласовывает сметы с подрядными организациями и осуществляет контроль за соблюдением ими нормативов, заложенных в сметы расходов, составляет акты выполненных работ.

2.9. Участвует в разработке мероприятий по снижению стоимости ремонтно-строительных работ.

2.10. Ведет учет сметной документации, систематизирует сметно-финансовые расчеты на периодически повторяющиеся работы с целью создания типовых смет.

2.11. Подготавливает необходимые справки о сметной стоимости работ.

2.12. Соблюдает требования правил и норм охраны труда и пожарной безопасности.

3. Права сметчика

Сметчик имеет право:

3.1. Знакомиться с проектами решений руководства организации, касающихся его деятельности.

3.2. Вносить предложения по совершенствованию работы, связанной с предусмотренными настоящей должностной инструкцией обязанностями.

3.3. В пределах своей компетенции сообщать непосредственному руководителю обо всех недостатках в деятельности организации (структурного подразделения, отдельных работников), выявленных в процессе исполнения своих должностных обязанностей, и вносить предложения по их устранению.

ПРИЛОЖЕНИЕ Г

Можно использовать перечень нормативно-правовых актов, из дисциплины Организационно-правовое обеспечение ИБ

Классификация информации ограниченного доступа

Информация с ограниченным доступом	Нормативные и законодательные акты
Государственная тайна	Закон РФ «О государственной тайне», ст. 275, 276, 283, 284 УК РФ
Конфиденциальная информация	Ст. 10 ФЗ «Об информации, информатизации и защите информации»
Персональные данные	Ст. 11 ФЗ «Об информации, информатизации и защите информации»
Личная и семейная тайна	Ст. 23 Конституции Российской Федерации, ст. 11 ФЗ «Об информации, информатизации и защите информации», ст. 150 Гражданского кодекса Российской Федерации, ст. 137 УК РФ
Служебная тайна	Ст. 139 Гражданского кодекса Российской Федерации, ст. 155, 311 УК РФ
Служебная информация	Ст. 31 ФЗ «О рынке ценных бумаг»
Коммерческая тайна	Ст. 139 Гражданского кодекса Российской Федерации, ст. 183 УК РФ
Сведения о сущности изобретения («ноу-хау»)	Указ Президента Российской Федерации № 188 от 6.03.1997 г. «Об утверждении перечня сведений конфиденциального характера»
Тайна следствия и судопроизводства	Указ Президента Российской Федерации № 188 от 6.03.1997 г. «Об утверждении перечня сведений конфиденциального характера», ст. 310 УК РФ
Тайна связи	Ст. 63 ФЗ «О связи», ст. 11 ФЗ «Об информации, информатизации и защите информации», ст. 138 УК РФ
Тайна страхования	Ст. 946 Гражданского кодекса Российской Федерации
Тайна усыновления	Ст. 139 Семейного кодекса Российской Федерации, ст. 155 УК РФ
Тайна исповеди	Ст. 3 ФЗ «О свободе совести и религиозных объединениях»
Банковская тайна	Ст. 857 Гражданского кодекса Российской Федерации, ст. 26 ФЗ «О внесении изменений и дополнений в Закон РСФСР "О банках и банковской деятельности в РСФСР"», ст. 183 УК РФ
Нотариальная тайна	Ст. 16, 29 Основ законодательства Российской Федерации о нотариате, ст. 202 УК РФ
Адвокатская тайна	Закон РФ «Об адвокатской деятельности и адвокатуре в Российской Федерации»
Врачебная тайна	Ст. 161 Основ законодательства Российской Федерации об охране здоровья граждан, ст. 14 Закона Российской Федерации «О трансплантации органов и (или) тканей человека»