## 1. Кто такой менеджер по информационной безопасности?

Почему он так необходим на предприятии.

**Информация** является одним из самых главных деловых ресурсов, который обеспечивает организации добавочную стоимость, и вследствие этого нуждается в защите. Слабые места в защите информации могут привести к финансовым потерям, и нанести ущерб коммерческим операциям. Поэтому в наше время вопрос разработки системы управления информационной безопасностью и ее внедрение в организации является концептуальным

**Менеджер по информационной безопасности (BISO - Business Information Security Officer) –** это представитель Службы (отдела) информационной безопасности на уровне подразделения (например, отдела информационных технологий или автоматизации) который занимается практическим внедрением и исполнением политик и регламентов, разработанных Директором по информационной безопасности (CISO Chief Information Security Officer)). Это специалист, отвечающий за информационную безопасность и имеющий полный контроль над информационной системой на предприятии (или вверенном ему филиале/подразделении) в рамках его функциональных обязанностей и компетенции.

Менеджеры по информационной безопасности создают системы защиты для конкретных предприятий, защищают локальные компьютерные сети от вирусных атак или взлома хакеров. Они предотвращают утечку важной информации, подлог данных и некомпетентность (злой умысел) собственных сотрудников.

Важные качества менеджера по информационной безопасности – это коммуникабельность и умение работать в команде. Создание и наладка систем защиты - это коллективная работа нескольких специалистов: руководителя защищаемой компании, аналитика, проектировщиков систем, программистов и т.д.

В основу работы менеджера по информационной безопасности положена деятельность, направленная на **обеспечение комплекса мероприятий в деятельности организации, связанная со следующими факторами (целями) информационной безопасности:**

- конфиденциальность – доступность к информации, которую имеют в своем распоряжении только те лица, кто владеет соответствующими полномочиями;
- целостность – возможность внесения изменений в информацию только теми лицами, которые на это уполномочены;
- доступность – возможность получения авторизованного доступа к информации со стороны уполномоченных лиц в соответствующий санкционированный для работы период времени.
- учет – все значимые действия лица, выполняемые им в рамках, контролируемых системой безопасности должны быть зафиксированы и проанализированы;
- неотрекаемость или апеллируемость, т. е. лицо, направившее информацию другому лицу, не может отречься от факта направления информации, а лицо, получившее информацию, не может отречься от факта ее получения.

Учет обычно ведется средствами электронных регистрационных журналов, которые используются в основном только уполномоченными службами, и его основное отличие – в регулярности анализа этих журналов.

Апеллируемость обеспечивается средствами криптографии (электронно-цифровой подписью), и ее характерная черта – возможность использования в качестве доказательного материала во внешних инстанциях, например в суде, при наличии соответствующего законодательства.

Перечисленные выше факторы (цели) информационной безопасности обеспечиваются применением следующих **механизмов или принципов**:

- политика – набор формальных (официально утвержденных либо традиционно сложившихся) правил, которые регламентируют функционирование механизма информационной безопасности;
- идентификация – определение (распознавание) каждого участника процесса информационного взаимодействия перед тем как к нему будут применены какие бы то ни было понятия информационной безопасности;
- аутентификация – обеспечение уверенности в том, что участник процесса обмена информацией идентифицирован верно, т. е. действительно является тем, чей идентификатор он предъявил;
- контроль доступа – создание и поддержание набора правил, определяющих каждому участнику процесса информационного обмена разрешение на доступ к ресурсам и уровень этого доступа;
- авторизация – формирование профиля прав для конкретного участника процесса информационного обмена (аутентифицированного или анонимного) из набора правил контроля доступа;
- аудит и мониторинг – регулярное отслеживание событий, происходящих в процессе обмена информацией, с регистрацией и анализом предопределенных значимых или подозрительных событий. Понятия "аудит" и "мониторинг" при этом несколько различаются, так как первое предполагает анализ событий постфактум, а второе приближено к режиму реального времени;
- реагирование на инциденты – совокупность процедур или мероприятий, которые производятся при нарушении или подозрении на нарушение информационной безопасности;
- управление конфигурацией – создание и поддержание функционирования среды информационного обмена в работоспособном состоянии и в соответствии с требованиями информационной безопасности;
- управление пользователями – обеспечение условий работы пользователей в среде информационного обмена в соответствии с требованиями информационной безопасности.

Современные компании все чаще сталкиваются с необходимостью обеспечить конфиденциальность данных, предотвратить утечку или несанкционированный доступ к информации. Задача обеспечить комплексную защиту информации ложится на плечи специалиста по информационной безопасности, который должен провести аудит существующей системы безопасности, проанализировать информационные риски и в соответствии с этим разработать и внедрить мероприятия по обеспечению информационной

безопасности компании, в частности, выбрать, установить и настроить технические средства защиты информации. Процесс защиты информации сопровождается активным составлением нормативно-технической документации. В обязанности специалиста по информационной безопасности также входит постоянный мониторинг системы информационной безопасности и поддержка технических средств ее защиты. Кроме того сотруднику, ответственному за информационную безопасность, приходится обучать других сотрудников соблюдению основ информационной безопасности.

**Серия стандартов ISO/IEC 27000 по информационной безопасности:**

ISO/IEC 27001 – Система управления информационной безопасностью – Требования (Содержит требования для создания, внедрения, поддержки и развития системы управления информационной безопасностью (СУИБ));

ISO/IEC 27002 – Практические правила управления информационной безопасностью (Предоставляет организациям рекомендации для отбора контролей процесса внедрения СУИБ, выступает в качестве ориентира внедрения общепринятых контролей информационной безопасности для организаций);

ISO/IEC 27003 – Рекомендации по внедрению СУИБ (Предоставляет руководство по внедрению для поддержания требований СУИБ, дает советы и рекомендации по безопасности, которые полезны для всех организаций, независимо от их размера, сложности и рисков);

ISO/IEC 27004 – Метрики и измерения (Руководство по разработке стандартов измерения для системы управления информационной безопасностью для измерения эффективности внедрения СУИБ (процессов и контролей));

ISO/IEC 27005 - Управления рисками информационной безопасности (Охватывает процесс управления рисками:

Оценка рисков;

Обработка рисков;

Выбор контролей;

Действующие меры управления рисками).

ISO/IEC 27006 – Требования к организациям, которые проводят аудит и сертификацию СУИБ (Требования к организациям, которые проводят аудит и сертификацию системы управления информационной безопасностью);

ISO/IEC 27015 – Рекомендации по управлению ИБ для организаций предоставляющих финансовые услуги (Руководство по внедрению СУИБ согласно стандартам серии ISO/IEC 27000 для организаций предоставляющих финансовых услуги).

2. **Сформировать список задач менеджера по информационной безопасности и их краткое описание.**

Менеджеры по информационной безопасности принимают непосредственное участие в создании системы защиты информации, ее аудите и мониторинге, анализируют информационные риски, разрабатывают и внедряют мероприятия по их предотвращению. В их компетенцию также входит установка, настройка и сопровождение технических средств защиты информации. Менеджеры по безопасности обучают и консультируют сотрудников по вопросам обеспечения информационной защиты, разрабатывают нормативно-техническую документацию.

**Обязанности менеджера по информационной безопасности:**

Данная должностная инструкция определяет функциональные обязанности и ответственность специалиста по информационной безопасности в предприятия (организации).

**Менеджер по информационной безопасности должен знать:**

- законы и иные нормативные правовые акты, регулирующие отношения, связанные с защитой государственной тайны и иной информации ограниченного доступа; нормативные и методические документы по вопросам, связанным с обеспечением безопасности информации;

- структуру управления, связи и автоматизации и основные элементы ключевой системы информационной инфраструктуры предприятия;

- подсистемы разграничения доступа, подсистемы обнаружения атак, подсистемы защиты от преднамеренных воздействий, контроля целостности информации;

- порядок создания защищенного канала между взаимодействующими объектами через систему общего пользования с использованием выделенных каналов связи;

- порядок осуществления аутентификации взаимодействующих объектов и проверки подлинности отправителя и целостности передаваемых через систему общего пользования данных;

- оснащенность предприятия основными и вспомогательными техническими средствами и системами, перспективы их развития и модернизации;

- перспективы и направления развития методов и средств технических и программно-аппаратных средств защиты информации от деструктивных информационных воздействий;

- порядок проектирования и аттестации объектов информатизации; контроль эффективности защиты информации на объектах информатизации;

- методы и средства выявления угроз безопасности информации, методики выявления каналов утечки информации;

- методы проведения научных исследований, разработок по технической защите информации;

- порядок обследования ключевых систем информационной инфраструктуры, составления актов проверки, протоколов испытаний, предписаний на право эксплуатации

специальных средств обеспечения безопасности информации, а также положений, инструкций и других организационно-распорядительных документов;

- полномочия по вопросам обеспечения безопасности информации, возможности и порядок применения штатных технических средств обеспечения безопасности информации, и контроля их эффективности;

- методы анализа результатов проверок, учета нарушений требований по обеспечению безопасности информации;

- методику подготовки предложений, методы и средства выполнения вычислительных работ в интересах планирования, организации и проведения работ по обеспечению безопасности информации на предприятии;

- достижения науки и техники в стране и за рубежом в области технической разведки и защиты информации;

- методы оценки профессионального уровня специалистов по обеспечению безопасности информации, аттестации специалистов;

- основы трудового законодательства;

- правила по охране труда и пожарной безопасности.

**Менеджер по информационной безопасности обязан:**

- выполнять мероприятия по обеспечению информационной безопасности на предприятии;

- определять возможные угрозы безопасности информации, уязвимость программного и аппаратного обеспечения, разрабатывать технологии обнаружения вторжения, оценивать и переоценивать риски, связанные с угрозами деструктивных информационных воздействий, способных нанести ущерб системам и сетям вследствие несанкционированного доступа, использования раскрытия, модификации или уничтожения информации и ресурсов информационно-управляющих систем;

- определять ограничения по вводу информации и предотвращать инциденты нарушения информационной безопасности;

- определять порядок подключения к открытым информационным системам с учетом обеспечения безопасности, связанной с соглашениями о доступе и приоритезации внешних ресурсов;

- определять требования к местам резервного хранения информации, ее обработки и копирования;

- поддерживать целостность и доступность информации и средств, обрабатывающих информацию;

- разрабатывать процедуры защиты носителей информации, коммуникаций и восстановления информационно-управляющих систем после сбоя или отказа;

- гарантировать защиту информации в сетях и защиту вспомогательной инфраструктуры;

- осуществлять:

контроль деятельности по обеспечению безопасности информации на предприятии;

информационное, материально-техническое и научно-техническое обеспечение безопасности информации;

контроль состояния работ по обеспечению безопасности информации на предприятии и их соответствие нормативно-правовым актам;

- предотвращать неразрешенное разглашение, изменение, удаление или уничтожение активов, а также прерывание деловых операций;

- давать отзывы и заключения на проекты вновь создаваемых и модернизируемых объектов и других разработок по вопросам обеспечения безопасности информации на предприятии;

- участвовать в рассмотрении технических заданий на научно-исследовательские и опытно-конструкторские работы по обеспечению безопасности информации на предприятии, оценивать их соответствие действующим нормативным и методическим документам;

- участвовать в работах по внедрению новых средств технической защиты информации;

- гарантировать защиту услуг электронной торговли, а также их безопасное использование;

- обнаруживать неразрешенную деятельность по обработке информации;

- гарантировать защиту информации при использовании средств мобильной обработки и телеобработки;

- предотвращать ошибки, потерю, неразрешенное изменение или неправильное использование информации в приложениях;

- защищать конфиденциальность, аутентичность или целостность информации криптографическими средствами;

- контролировать информацию о технически уязвимых местах используемых информационных систем, оценивать подверженность предприятия влиянию через такие уязвимые места, и предпринимать подходящие меры для решения проблемы связанного с этим риска;

- сообщать о событиях и слабостях в системе защиты информации руководящему составу предприятия;

- содействовать распространению на предприятии передового опыта и внедрению современных организационно-технических мер, средств и способов обеспечения информационной безопасности;

- проводить оценку технико-экономического уровня и эффективности предлагаемых и реализуемых организационно-технических решений по обеспечению информационной безопасности на предприятии.

- управлять доступом персонала к информации;

- разрабатывать списки доступа персонала на объекты защиты, порядок и правила поведения работников, в том числе при их перемещении, увольнении и взаимодействии с персоналом сторонних организаций;

- гарантировать доступ зарегистрированного пользователя и предотвращать неразрешенный доступ к информационным системам;

- предотвращать неразрешенный доступ пользователей, а также компрометацию или кражу информации и средств, обрабатывающих информацию;

- предотвращать неразрешенный доступ персонала к сетевым услугам, не имеющих соответствующих допусков;

- предотвращать неразрешенный доступ персонала к операционным системам, не имеющих соответствующих допусков;

- предотвращать неразрешенный доступ персонала к информации, содержащейся в прикладных системах, не имеющих соответствующих допусков;

- проводить оценку и разрабатывать списки доступа на объекты предприятия при работе с клиентами;

- проводить занятия с сотрудниками подразделений предприятия по правилам работы на компьютере и по изучению руководящих документов по вопросам обеспечения безопасности информации;

- осуществлять руководство и обучение персонала действиям в кризисных ситуациях, включая порядок действий руководящих и других ответственных лиц на предприятии;

- координировать свою деятельность по защите информации с представителями различных частей организации с соответствующими ролями и их рабочими функциями;

- контролировать выполнение обязанностей администраторами безопасности, ответственными за информационную безопасность в подразделениях, ответственными за эксплуатацию конкретных АРМ, за обслуживание определенных технических и программных средств;

- контролировать исполнение порядка учета, хранения, использования и уничтожения отчуждаемых магнитных носителей конфиденциальной информации;

- контролировать выполнение установленных правил создания, хранения и использования эталонных копий программных средств, соблюдение порядка формирования и использования информационных массивов и баз данных, резервного и архивного копирования данных;

- участвовать в расследовании причин возникновения серьезных кризисных ситуаций;

- постоянно проводить работу по выявлению возможных каналов утечки конфиденциальных сведений при эксплуатации информационной системы предприятия и несанкционированного вмешательства в процесс ее функционирования, готовить предложения по совершенствованию системы защиты и пересмотру Плана защиты;

- участвовать в работе комиссий по пересмотру Плана защиты.

- гарантировать соответствие систем организационной политики предприятия стандартам защиты.

**Менеджер по информационной безопасности несет ответственность за:**

- ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей должностной инструкцией - в пределах, определенных действующим трудовым законодательством;

- правонарушения, совершенные в процессе осуществления своей деятельности - в пределах, определенных действующим административным, уголовным и гражданским законодательством;

- причинение материального ущерба - в пределах, определенных действующим трудовым и гражданским законодательством.

## 3. Требования к менеджеру по информационной безопасности исходя из того, какие задачи нужно будет ему выполнять, предъявляемые ему при приеме его на работу.

Менеджер по информационной безопасности, должен хорошо представлять себе техническую сторону защиты информации. Он должен иметь полное/неполное высшее или высшее техническое образование, знание английского языка на уровне чтения технической литературы, понимание основ информационной безопасности.

На должность менеджера по информационной безопасности назначается лицо, имеющее стаж работы по защите информации не менее 3 лет.

Назначение на должность менеджера по информационной безопасности и освобождение от нее производится приказом Генерального директора (Директора) предприятия по представлению руководителя службы информационной защиты (если такой предусмотрен штатом предприятия) или заместителем Генерального директора.

Кандидат на должность менеджера по информационной безопасности должен ориентироваться в:

- законодательных актах, нормативных и методических материалах по вопросам, связанным с обеспечением информационной безопасности предприятия;

- особенностях деятельности предприятий его управления, типов организационно-штатных структур;

- методах планирования и организации проведения работ по защите информации и обеспечению коммерческой тайны и обеспечению экономической и кадровой безопасности предприятия;

- основах экономики, организации производства, труда и управления;

- основах трудового законодательства;

- правилах и нормах охраны труда, техники безопасности, производственной санитарии и противопожарной защиты.

Менеджер по информационной безопасности подчиняется непосредственно руководителю службы информационной безопасности предприятия или в случае его отсутствия на предприятии – генеральному директору.

4. **Какие компетентности (компетенции) необходимы человеку, который придет на позицию менеджера по информационной безопасности?**
   **Сформировать список и описать каждую компетенцию.**

**А. Общие компетенции:**
*Управленческие компетенции – это компетенции, необходимые* для выполнения руководящих обязанностей.

*Личностно-деловые качества:*
- способности к саморазвитию;
- устойчивость к стрессам;
- способность мобилизовать свои силы в короткий отведенный промежуток времени;
- умение убеждать;
- умение слушать;
- умение подчинять себе толпу;
- нацеленность на результат;
- высокий уровень самомотивации.

*Работа в команде:*
- Вести за собой других;
- Владеть культурой межличностного общения;
- Уточнять постановку задач;
- Работать в команде;
- Отстаивать и аргументировать свою позицию;

*Самоконтроль и ответственность*
- Принимать решения в рамках профессиональной компетентности;
- Брать ответственность за принимаемые решения в рамках профессиональной компетентности;
- Рационально организовывать свой труд на рабочем месте;
- Планировать и организовывать собственную работу;
- Планировать свою деятельность;
- Оценивать границы собственной компетентности;
- Ответственно подходить к выполнению рабочих заданий;
- Поддерживать и повышать профессиональный и личный имидж;
- Соблюдать нормы времени;
- Проявлять новаторство и творческий подход в профессиональной деятельности;
- Производить самоконтроль качества выполненных работ;
- Формировать в себе аккуратность, дисциплинированность, ответственность, исполнительность;
- Соблюдать нормы затрат материальных ресурсов;
- Проявлять творческий подход и инициативу в профессиональной деятельности;
- Качественно выполнять поставленную задачу;
- Проявлять творческий подход в профессиональной деятельности.

*Умение правильно читать*
- Читать техническую документацию на английском языке;
- Читать проектную документацию на разработку информационной системы;
- Следить за новинками в области сетевого программного обеспечения;
- Читать профессиональную литературу;
- Работать с документацией и технической литературой;
- Работать с различными источниками информации;
- Следить за новинками отечественной и зарубежной профессиональной литературы.

*Саморазвитие*

- Оценивать перспективы развития информационных и коммуникационных технологий;
- Владеть инструментами экспресс обследования предприятия;
- Быть ответственным, дисциплинированным, аккуратным, исполнительным, инициативным, внимательным, способным к обучению, развивать аналитические способности;
- Анализировать собственный профессиональный опыт и совершенствовать свою деятельность;
- Владеть офисными и общесистемными программными средствами;
- Развивать в себе стрессоустойчивость, системное мышление, толерантность, логическое мышление дисциплинированность, аккуратность, ответственность, требовательность, коммуникабельность, умение убеждать;
- Осваивать новые технологии;
- Развивать в себе гибкость мышления, системность мышления, инициативность, уверенность в себе;
- Развивать аналитическое мышление, ответственность, коммуникабельность, креативность, инициативность, эмоциональную сдержанность, лидерские и организаторские качества;
- Совершенствовать объективность восприятия, гибкость мышления, системность мышления, нацеленность на результат, инициативность, обучаемость, умение принимать других, уверенность в себе, ответственность, адаптивность, аккуратность, дисциплинированность, доброжелательность, коммуникабельность, стрессоустойчивость;
- Непрерывно повышать свою квалификацию.

*Навыки публичных выступлений*

- Участвовать в научно-практических конференциях и семинарах;
- Проводить презентации;
- Письменно и устно излагать свои предложения и полученные результаты для различных аудиторий;
- Участвовать в конференциях, семинарах.

**Б. Профессиональные компетенции:**

**Основы программирования** (языки программирование, процесс создания ПО, методы обеспечения качества программных продуктов, инспекции и т.д. и т.п.);

*Языки программирования*

- Владеть основами современных языков программирования;
- Использовать языки программирования и инструментарий для разработки программного обеспечения;
- Находить ошибки кодирования в разрабатываемой информационной системе;

*Понимание процесса и методов создания ПО*

- Владеть системами контроля версий
- Выбор программно-технических средств сбора и хранения информации;
- Владеть основными методами разработки программного обеспечения;
- Осуществлять построение моделей процессов, данных, объектов
- Описывать сценарии использования системы безопасности;
- Проводить сбор сведений для описания моделей процессов, данных, объектов предметной области;
- Применять эффективные методы проектирования;
- Вырабатывать требования к программному обеспечению;
- Разрабатывать технические задания на выполнение работ;

- Производить оптимизацию разрабатываемых алгоритмов решений;
- Владеть методами анализа архитектуры программного обеспечения.

*Обеспечение качества и безопасности создаваемого ПО*

- Анализировать результаты экспертного тестирования информационных систем на этапе опытной эксплуатации;
- Оценивать качество программного обеспечения;
- Организовывать и проводить экспертное тестирование информационных систем на этапе опытной эксплуатации;
- Оценивать функциональность программного обеспечения.

**Операционные системы, компьютеры и сети** (идеология, архитектура, проектирование, внедрение и сопровождение);

*Контроль текущего состояния ПО*

- Устанавливать ограничения по степени использования ресурсов;
- Сравнивать характеристики программно-технических средств;
- Осуществлять презентации новых программно-технических средств;
- Определять соответствие технических средств и программного обеспечения;
- Проводить инвентаризацию программно-технических средств системы;
- Выбирать программно-технические средства обеспечения мониторинга;
- Инсталлировать, конфигурировать и настраивать программное обеспечение мониторинга;
- Устанавливать и настраивать программное обеспечение системы резервного копирования;
- Настраивать специализированное программное обеспечение.

*Модернизация ПО*

- Обосновывать необходимость закупки программно-технических средств;
- Составлять график модернизации программно-технических средств;
- Проводить технико-экономическое обоснование внедрения новых программно-технических средств;
- Формулировать рекомендации по обновлению или замене программного обеспечения;
- Разрабатывать предложения по модернизации программно-технических средств.

*Фиксация событий и документирование различных процедур, связанных с работой оборудования*

- Фиксировать и анализировать сбои в работе серверного и сетевого оборудования;
- Проверять маркировку оборудования;
- Сопоставлять инвентарные номера
- Фиксировать результаты приемки, монтажа и испытаний;
- Визировать заявки на закупку оборудования и материалов;
- Маркировать компьютеры и периферийные устройства;
- Контролировать выполнение графика проведения инвентаризации;
- Фиксировать в журнале вызовы для устранения неисправности оргтехники;
- Разрабатывать правила приемки, монтажа и испытания вводимых в эксплуатацию новых аппаратных, программных и коммуникационных средств.

*Эксплуатация оборудования*

- Обеспечивать своевременное выполнение профилактических работ;
- Выявлять устаревшее оборудование и программные средства;
- Контролировать эксплуатацию программно-технических средств на соответствие техническим условиям и нормативам обслуживания;

- Обеспечивать контроль соблюдения правил приемки, монтажа и испытаний программных средств и оборудования;
- Контролировать техническое состояние оборудования;
- Контролировать эксплуатацию серверного и сетевого оборудования в соответствии с техническими условиями и нормативами обслуживания;
- Анализировать результаты мониторинга функционирования программно-технических средств;
- Анализировать состояние параметров программно-технических средств.

*Контроль и мониторинг состояния Информационных систем и сетей (ИСиС)*
- Осуществлять мониторинг состояния информационной системы
- Обеспечивать контроль технического состояния коммуникационных объектов сетевой инфраструктуры
- Оценивать состояние информационных ресурсов;
- Анализировать  показатели использование компьютерной сети.

*Эксплуатация и сопровождение ИСиС*
- Анализировать состояние почтовой системы;
- Принимать участие в тестировании вводимых в сетевую конфигурацию системы новых аппаратных, программных и коммуникационных компонент;
- Развивать и внедрять передовые технологии системного администрирования;
- Поддерживать и актуализировать знания в области системного администрирования.

*Выявление и устранение причин неисправности ИСиС*
- Выявлять и анализировать причины проблем в работе информационных систем;
- Давать точную техническую формулировку проблем;
- Выявлять и анализировать причины проблем в работе компьютерных систем;
- Идентифицировать технические проблемы, возникающие в процессе эксплуатации системы;
- Проводить осмотр объектов сетевой инфраструктуры и рабочих станций согласно утвержденному графику;
- Информировать администратора баз данных при обнаружении неполадок в работе.

*Разработка документов и регламентов по работе с ИСиС*
- Разрабатывать методики экспертного тестирования информационных систем на этапе опытной эксплуатации;
- Разрабатывать схемы и процедуры послеаварийного восстановления работоспособности вычислительной сети;
- Вести учет и анализ показателей использования сетевых ресурсов
- Вести учет и анализ показателей условий эксплуатации системы.

**Базы данных** (создание, администрирование, защита);
- Использовать программные и технические средства сбора и обработки данных;
- Анализировать рынок современных систем управления базами данных и баз данных;
- Поддерживать и актуализировать знания в области администрирования баз данных;
- Выбирать базы данных и поставщика баз данных.

*Обработка информации*
- Осуществлять сбор информации;
- Обрабатывать информацию;
- Анализировать информацию;
- Структурировать информацию;
- Сохранять данные на сменных носителях;

- Владеть инструментарием обработки данных на персональном компьютере.

*Резервное копирование*
- Составлять план архивации данных;
- Разработка регламента сбора и хранения информации;

*Осуществление контроля и документирования работы с базами данных*
- Вести журнал архивации данных и степени использования носителей;
- Контролировать структурные изменения баз данных;
- Осуществлять мониторинг использования баз данных;
- Проводить технико-экономическое обоснование внедрения новых систем управления базами данных и баз данных;
- Применять нормативно-техническую документацию при использовании систем управления базами данных и баз данных;
- Подготавливать отчеты о функционировании систем управления базами данных.

**Системный анализ и управление** (анализ любых информационных систем, бизнес процессов, управление инфраструктурой);

*Управление проектной деятельностью*
- Анализировать риски проекта;
- Проверять соответствие выполняемых работ требованиям проектной документации;
- Оценивать необходимые ресурсы для выполнения работ;
- Формировать рекомендации по корректировке результатов работ;
- Проверять соответствие выполненных работ требованиям проектной документации.

*Понимание стратегии организации*
- Обосновывать предложения по реализации стратегии в области информационных технологий;
- Оценивать потребности организации в информационных ресурсах;
- Контролировать заполнение соответствующей документации;
- Формировать функциональные требования к информационной системе для решения бизнес-задач предприятия.

*Управление администрированием информационных систем*
- Прогнозировать сроки модернизации информационной инфраструктуры;
- Анализировать причины проблем, инцидентов;
- Анализировать результаты мониторинга по использованию вычислительной сети;
- Анализировать технологические и архитектурные решения в области информатизации;
- Анализировать качество выполнения работ на соответствие инструкций по эксплуатации программно-технических средств;
- Определять узкие места в функционировании информационных систем;
- Анализировать протоколы системных и сетевых событий;
- Анализировать статистику отказов;
- Контролировать выполнение процедуры списания технических средств;
- Регулярно осуществлять проверку отчетов по результатам инвентаризации и списанию программно-технических средств;
- Контролировать наличие и движение программно-технических средств;
- Оценивать состояние программно-технических ресурсов;
- Формировать необходимые для работы информационной системы требования к конфигурации локальных компьютерных сетей.

*Управление планово-отчётной деятельностью*

- Контролировать качество и объемы выполненных технических работ;
- Контролировать графики проверок технической документации, регламентов, инструкций;
- Отслеживать утвержденный график выполнения профилактических работ;
- Определять и формулировать первоочередные задачи;
- Составлять аналитические отчёты;
- Контролировать графики поставок оборудования и выполнения работ;
- Составлять и обосновывать заключения и давать рекомендации.

**Работа с людьми** (взаимодействие с заказчиками, управление персоналом, взаимодействие с пользователями, работа с разрешающими и уполномоченными органами, работа с представителями власти)

*Управлять персоналом*

- Осуществлять руководство рабочей группой;
- Работать с персоналом;
- Ставить задачи системным аналитикам, программистам и другим специалистам.

*Обеспечение взаимодействия между людьми*

- Организовывать и подготавливать совместно с другими подразделениями технические совещания;
- Сотрудничать с другими работниками в составе рабочей группы;
- Распределять работы по направлениям между смежными подразделениями;
- Анализировать проблемы взаимодействия системных аналитиков, программистов и других специалистов;
- Оценивать работу персонала;
- Обеспечивать рациональную расстановку и загрузку персонала;
- Определять квалификационные требования к исполнителям работ;
- Организовывать и подготавливать технические совещания.

*Поддержание позитивной рабочей атмосферы*

- Создавать и поддерживать микроклимат в коллективе;
- Внедрять корпоративную культуру и социальную этику;
- Аргументировать и убеждать собеседников;
- Управлять межличностными отношениями;
- Управлять конфликтными ситуациями;
- Мотивировать партнеров по взаимодействию;
- Разрешать конфликтные ситуации;
- Создавать и поддерживать авторитет в среде коллег и заказчиков;
- Управление отношениями участников проекта.

*Работа с заказчиком*

- Анализировать требования заказчика по использованию информационных систем;
- Владеть терминологией заказчика в одной или нескольких предметных областях;
- Проводить интервью с ключевыми сотрудниками заказчика;
- Документировать результаты взаимодействия с заинтересованными лицами в процессе разработки, тестирования и внедрения компьютерных систем.

*Обеспечение норм охраны труда*

- Контролировать соблюдение персоналом технологической, производственной и трудовой дисциплины;
- Соблюдать правила поведения в чрезвычайных ситуациях;
- Соблюдать требования охраны труда;
- Обеспечивать условия труда в соответствии с выполняемыми задачами;

- Контролировать соблюдение требования пожарной безопасности;
- Анализировать эффективность использования рабочего времени;

*Работа с пользователями информационных систем*
- Обрабатывать результаты анкетирования;
- Структурировать и анализировать запросы структурных подразделений;
- Анализировать отзывы пользователей;
- Осуществлять проверку знаний и умений пользователей;
- Анализировать требования пользователей;
- Выявлять  проблемы пользователя;
- Консультировать пользователей информационной системы;
- Отвечать на вопросы пользователей информационной системы;
- Обучать пользователей.

*Люди и проекты*
- Подбирать исполнителей работ и оценивать их соответствие квалификационным требованиям;
- Проводить обучение исполнителей проекта;
- Оценивать результаты работы исполнителей проекта и корректировать их деятельность;
- Разрабатывать квалификационные требования к исполнителям проекта в соответствии с задачами проекта;

*Анкетирование и интервью*
- Разрабатывать вопросники для интервьюирования;
- Обрабатывать результаты интервьюирования;
- Проводить письменное анкетирование;
- Принимать участие в разработке анкет;
- Подготавливать и проводить устные интервью;
- Проверять знания персонала по заполнению необходимой документации;
- Участвовать в разработке учебных материалов;
- Передавать знания и опыт работы;
- Осуществлять обучение персонала.

**Информационная безопасность** (шифрование, VPN, FireWall, Antivirus, IDS, СКУД, пароли, восстановление данных, политики безопасности)

*Следование инструкциям по обеспечению информационной безопасности*
- Выполнять требования инструкции по обеспечению информационной безопасности отдела;
- Участвовать в составлении проектной документации на разработку информационной системы;

*Применять технические средства защиты информации*
- Применять технические средства обеспечения информационной безопасности;
- Разрабатывать стандарты настройки системы безопасности;
- Настраивать системы безопасности;
- Обеспечивать информационную безопасность периметра;
- Контролировать настройки системы безопасности;
- Устанавливать средства дополнительной защиты, обслуживать и эксплуатировать эти средства.

*Анализ и аудит информационных систем и систем безопасности*

- Выполнять анализ основных показателей деятельности ИТ-подразделения в соответствии с корпоративной бизнес-стратегией предприятия;
- Анализировать бизнес процессы организации в области информационной безопасности;

*Работа с системами антивирусной защиты*
- Настраивать системы антивирусной защиты;
- Заполнять журналы вирусных атак;
- Контролировать регулярное обновление программного обеспечения антивирусной защиты;
- Разрабатывать регламент обновления программного обеспечения антивирусной защиты.

*Создавать ограничивающие политики и процедуры*
- Устанавливать ограничения по использованию времени;
- Разрабатывать политику ограничения пользователей по правам доступа и степени использования ресурсов;
- Устанавливать ограничения по использованию рабочей станции или серверов.

*Контролирование использования вычислительных ресурсов*
- Контролировать использование сети Интернет и электронной почты;
- Организовывать доступ к локальным и глобальным сетям, в том числе, в сети Интернет;
- Контролировать работоспособность серверов вычислительной сети во время отсутствия системного администратора.

*Формирование политик безопасности*
- Соблюдать политику информационной безопасности;
- Участвовать в разработке политики информационной безопасности.

*Анализ рынка программно-технических средств*
- Анализировать рынок программно-технических средств;
- Следить за рынком программного обеспечения и технических средств.

*Работа с учётными записями информационных систем и пользователей*
- Назначать идентификаторы и пароли при регистрации пользователей;
- Создавать и поддерживать в актуальном состоянии пользовательские учетные записи;
- Разграничивать права доступа и вести реестр пользователей;
- Протоколировать события доступа к ресурсам.

*Реагирование на критические события и устранение аварийных ситуаций*
- Выявлять причины возникновения аварийных ситуаций;
- Утверждать систему мер реагирования на критические события;
- Обеспечивать противодействие атакам;
- Контролировать настройки оповещения о критических событиях;
- Разрабатывать систему мер реагирования на критические события, на атаки хакеров.

**Инструментальный контроль** (предотвращение утечки информации по физическим полям, обнаружение закладок и жучков, проверка оборудования на предмет наличия в нём посторонних закладных устройств)

*Физическая охрана объектов и устройства охранной сигнализации*

- Демонстрирует системное и полное владение методологией охранной деятельности и инженерно-техническими аспектами организации защиты и охраны объектов, владеет информацией о том, как организованы эксплуатируемые технические системы охраны и как организована физическая охрана на конкретном объекте компании;
- Умеет формировать ТЗ или привлекать специалистов подрядных организаций для формирования технических заданий по организации инженерно-технической системы охраны объектов. Умеет последовательно спланировать и организовать внедрение системы;
- Знает различные типы оборудования, их сравнительные рабочие характеристики, новейшие тенденции и современные разработки в области средств инженерно-технической охраны объектов. Регулярно отслеживает изменения и нововведения посредством выставок, получая информацию с помощью налаженных профессиональных контактов с экспертами в данных областях.

*Средства и методы обеспечения специальной связи*

- Знает технологию и инженерно-технически средства осуществления и обеспечения специальной связи;
- Знает механизм взаимодействия и обращения к контролирующим органам.

*Специсследования, спецпроверки, спецобследования*

- Понимание физических основ перехвата информации по физическим полям побочных электромагнитных излучений;
- Обнаружение побочных электромагнитных излучений;
- Обнаружение закладных устройств (жучков, микрофонов, диктофонов);
- Проверка печатных плат устройств на предмет обнаружения посторонних логических элементов, не являющихся частью изначального дизайна устройства;
- Знает технологии защиты информации от утечки по техническим каналам (стекла, двери и др.), способы их ликвидации, технологии противодействия средствам технической разведки.