УТВЕРЖДАЮ

Генеральный директор
ООО «Сатурн»

Соколов А.А.

«___» _____ 2018 г.

Должностная инструкция

начальника отдела информационной безопасности

1 Общие положения

1.1 Настоящая должностная инструкция устанавливает общие положения, должностные обязанности, права и ответственность начальника отдела информационной безопасности (далее – ОИБ) ООО «Сатурн» (далее – Компания).

1.2 Назначение на должность начальника отдела и освобождение от занимаемой должности производится приказом Генерального директора по представлению начальника управления по безопасности.

1.3 Начальник отдела непосредственно подчиняется начальнику управления по безопасности.

1.4 В период отсутствия начальника отдела (командировка, отпуск, больничный) его обязанности исполняет иное лицо, если принято решение о назначении исполняющего обязанности. Решение о назначении исполняющего обязанности утверждается приказом Генерального директора по представлению начальника управления по безопасности. Вышеуказанное лицо приобретает соответствующие права, обязанности и несет ответственность за их ненадлежащее исполнение.

1.5 На должность начальника отдела назначается лицо, имеющее высшее профессиональное (техническое) образование по направлению подготовки «Информационная безопасность» и стаж работы в области защиты информации не менее 5 лет, или лицо, имеющее высшее профессиональное (техническое) образование и (или) прошедший переподготовку по одной из специальностей направления «Информационная безопасность» (нормативный срок - свыше 500

аудиторных часов), а также имеющее стаж работы в области защиты информации не менее 5 лет.

1.6 Начальник отдела должен знать:

– законы и иные нормативно–правовые акты Российской Федерации (РФ), регулирующие отношения, связанные с защитой государственной тайны и иной информации ограниченного доступа;

– нормативные и методические документы по вопросам, связанным с обеспечением защиты информации и противодействия техническим разведкам, а также планированием мероприятий и контролем выполнения работ по защите информации и противодействию техническим разведкам;

– достижения науки и техники в стране и за рубежом в области технической разведки, противодействия техническим разведкам и защиты информации;

– порядок пользования реферативными и справочно-информационными изданиями, а также другими источниками научно-технической информации;

– перспективы и направления развития методов и средств защиты информации;

– правила лицензирования и сертификации в области защиты информации;

– виды угроз безопасности информации и способы их выявления;

– методы планирования и организации выполнения работ по защите информации и противодействию техническим разведкам;

– правила разработки и подготовки к утверждению проектов нормативных и методических документов, регламентирующих работу по технической защите информации и противодействию техническим разведкам;

– порядок составления перспективных планов и программ проведения исследований, разработок, испытаний, внедрения новых технических и программно-аппаратных средств защиты информации и средств по противодействию техническим разведкам;

– основные требования и мероприятия по обеспечению режима секретности;

– организацию секретного, конфиденциального и несекретного делопроизводства;

– порядок контроля за прохождением служебных документов и материалов;

– стандарты системы организационно-распорядительной документации;

– мероприятия по технической защите информации;

– методы и средства контроля эффективности защиты;

– способы выявления технических каналов утечки информации;

– методики оценки возможностей технических разведок;

– показатели оценки эффективности мер по обеспечению безопасности информации и противодействию техническим разведкам, методы их расчета и анализа, отыскания оптимальных решений по повышению эффективности технической защиты информации и противодействия техническим разведкам;

– принципы построения локальных и распределенных автоматизированных систем;

– объекты информатизации, подлежащие защите;

– порядок проведения категорирования и классификации объектов;

– порядок проектирования объектов информатизации;

– организационную структуру объектов защиты;

– организацию деятельности объектов защиты и функционирования на них систем управления, связи и автоматизации;

– структуру управления, связи и автоматизации и основные элементы ключевой системы информационной инфраструктуры филиала;

– порядок обследования ключевых систем информационной инфраструктуры;

– технико-эксплуатационные характеристики, конструктивные особенности, назначение и режимы работы современных электронно-вычислительных машин (ЭВМ), правила их технической эксплуатации в комплексах технической защиты информации;

– спецификацию изделий технической защиты информации, комплектующих, запасного имущества и ремонтных материалов;

– правила эксплуатации средств защиты информации и шифровальных (криптографических) средств, организации их обслуживания и ремонта;

– 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;

– порядок заключения договоров на проведение специальных исследований и специальных проверок, работ по защите основных и вспомогательных технических средств и систем;

– порядок проведения специальных проверок и специальных исследований;

– порядок и содержание контрольных проверок;

– порядок аттестации объектов информатизации;

– требования по оформлению актов проверок, протоколов испытаний, предписаний на право эксплуатации основных и вспомогательных технических средств и систем;

– профиль, специализацию, особенности структуры филиала;

– перспективы развития и направления деятельности предприятия и его подразделений;

– документы, определяющие основные направления экономического и социального развития предприятия;

– системы сертификации, лицензирования и организацию технической защиты информации, действующую на предприятии;

– оснащенность организации основными и вспомогательными техническими средствами и системами, перспективы их развития и модернизации;

– систему материально-технического обеспечения предприятия;

– порядок финансирования;

– структуру, назначение, задачи, полномочия и техническую оснащенность подразделения;

– организацию взаимодействия подразделений филиала при решении вопросов обеспечения информационной безопасности и противодействия техническим разведкам;

– методы оценки профессионального уровня специалистов по технической защите информации, аттестации специалистов;

– принципы подбора и расстановки кадров, методику и порядок проведения служебных расследований, воспитательной и профилактической работы;

– правила внутреннего трудового распорядка;

– основы трудового законодательства;

– правила и нормы охраны труда, производственной санитарии и противопожарной безопасности;

– опасности и риски на своих рабочих местах и при перемещении по территории филиала;

1.7 Начальник отдела в своей работе руководствуется Конституцией РФ, Федеральными законами, Указами и распоряжениями Президента РФ, Постановлениями Правительства РФ, руководящими и методическими документами по информационной безопасности Федеральной службы безопасности РФ (далее - ФСБ РФ), руководящими и методическими документами по информационной безопасности Федеральной службы по техническому и экспортному контролю РФ (далее - ФСТЭК РФ), предписаниями на эксплуатацию основных и вспомогательных технических средств и систем, предписаниями на эксплуатацию шифровальных (криптографических) средств, приказами и инструкциями Министерства обороны РФ, Перечнем сведений, подлежащих засекречиванию по МО РФ, Перечнем сведений, составляющих служебную тайну,

Перечнем сведений, составляющих коммерческую тайну, Уставом Компании, приказами, регламентами и инструкциями, инструкциями по охране труда, пожарной безопасности, требованиями природоохранного законодательства РФ, правилами внутреннего трудового распорядка, распоряжениями по отделу, настоящим Положением и другими нормативными правовыми актами. Положением об ОИБ, настоящей должностной инструкцией и другими нормативными документами.

1.8 Начальник отдела осуществляет руководство подчиненными работниками, согласно утвержденному штатному расписанию, координирует и направляет их деятельность.

2 Должностные обязанности

Начальник отдела:

2.1 В части планирования:

2.1.1 Изучает, анализирует и оценивает состояние информационной безопасности:

2.1.1.1 Изучает и обобщает научно-техническую литературу, нормативные и методические материалы по техническим средствам и способам защиты информации. Изучает периодику (журналы, газеты).

2.1.1.2 Изучает и обобщает опыт работы других организаций и предприятий по использованию технических средств и способов защиты информации с целью повышения эффективности и совершенствования работ по её защите.

2.1.1.3 Исследует функциональные возможности, технические характеристики, принципы работы технических средств и программного обеспечения, применяемых для защиты информации.

2.1.1.4 Исследует технологии обработки информации для определения необходимости и достаточности защиты на объектах информатизации.

2.1.1.5 Исследует производственные технологические процессы для определения возможности утечки защищаемой информации, а также необходимости и достаточности её защиты.

2.1.1.6 Исследует, обобщает и анализирует состояние информационной безопасности на филиале в целом.

2.1.2 Определяет информационные и технические ресурсы, подлежащие защите:

2.1.2.1 Организует и участвует в категорировании объектов вычислительной техники.

2.1.2.2 Организует и участвует в категорировании выделенных и защищаемых помещений.

2.1.2.3 Организует и участвует в классификации автоматизированных систем.

2.1.3 Формулирует требования по защите информации при создании и развитии объектов информатизации:

2.1.3.1 Принимает участие в рассмотрении, согласовании и внесении изменений в проекты договоров (контрактов), технических требований, технических заданий, планов, графиков на проведение работ на объекты информатизации, предназначенные для обработки или обсуждения информации, составляющей служебную или коммерческую тайну, а также персональные данные.

2.1.3.2 Предлагает рекомендации по внедрению средств защиты, их модернизации или замене.

2.1.3.3 Принимает участие в рассмотрении, согласовании и внесении изменений в проекты договоров (контрактов), технических требований, технических заданий, планов, графиков проведения работ на объектах информатизации.

2.1.4 Выявляет угрозы и уязвимости информационной безопасности, каналы утечки информации, оценивает риски и уровни сложности автоматизированных систем:

2.1.4.1 Выявляет возможные технические каналы утечки информации при эксплуатации шифровальных средств, объектов вычислительной техники, выделенных и защищаемых помещений.

2.1.4.2 Организует и участвует в создании моделей угроз.

2.1.4.3 Организует и участвует в проведении оценки рисков и уровней сложности автоматизированных систем.

2.1.5 Планирует текущую деятельность отдела и составляет:

- еженедельные отчеты;
- ежемесячные отчеты;
- ежеквартальные планы работы отдела;
- ежегодные планы работы отдела;
- ежегодные планы бюджета отдела;
- ежеквартальные планы (заявки) на материалы;
- ежегодные планы по проведению обучения работников отдела.

2.1.6 Участвует в планировании деятельности предприятия в случае пожара, аварии, стихийного бедствия и при возникновении других чрезвычайных ситуаций:

2.1.6.1 Участвует в планировании деятельности предприятия по обработке, обсуждению, хранению, передаче информации, составляющей служебную или коммерческую тайну, а также персональных данных, в случае пожара, аварии, стихийного бедствия и при возникновении других чрезвычайных ситуаций.

2.1.6.2 Планирует эвакуацию электронных носителей информации, составляющих служебную или коммерческую тайну, а также персональных

данных, при чрезвычайных ситуациях в случае пожара, аварии, стихийного бедствия и при возникновении других чрезвычайных ситуаций.

2.1.6.3 Участвует в планировании деятельности предприятия по обработке, обсуждению, хранению, передаче информации, составляющей служебную или коммерческую тайну, а также персональных данных, в военное время.

2.2 В части реализации:

2.2.1 Выполняет запланированные мероприятия:

2.2.1.1 Осуществляет задачи и функции, возложенные утвержденными планами мероприятий, в части информационной безопасности.

2.2.1.2 Обеспечивает выполнение указаний органов государственного надзора и контроля в части информационной безопасности в соответствии с поручением руководства в установленные сроки.

2.2.2 Организует и участвует в работах по внедрению, модернизации или замене средств информационной безопасности:

2.2.2.1 Организует приобретение программных и программно-аппаратных средств (комплексов) защиты информации и шифровальных (криптографических) средств, лицензий к ним, запасных частей, материалов и принадлежностей.

2.2.2.2 Организует и проводит установку, модернизацию или замену средств защиты информации.

2.2.2.3 Организует и проводит первичную настройку средств защиты информации.

2.2.3 Организует и участвует в испытаниях и приемке в эксплуатацию объектов информатизации.

2.2.3.1 Организует и участвует в испытаниях и приемке автоматизированных систем в защищенном исполнении, предназначенных для обработки информации, составляющей служебную или коммерческую тайну, а также персональных данных.

2.2.3.2 Организует и участвует в аттестационных испытаниях автоматизированных систем и выделенных (защищаемых) помещений, предназначенных для обработки или обсуждения информации, составляющей служебную или коммерческую тайну, а также персональных данных.

2.2.3.3 Организует и участвует в ежегодном инструментальном контроле защищенности автоматизированных систем и выделенных (защищаемых) помещений, предназначенных для обработки или обсуждения информации, составляющей служебную или коммерческую тайну, а также персональных данных.

2.2.4 Организует и осуществляет разработку и внедрение нормативных и распорядительных документов:

2.2.4.1 Организует и осуществляет разработку должностных инструкций и положения об отделе в рамках компетенции отдела.

2.2.4.2 Организует и разрабатывает инструкции по информационной безопасности в рамках компетенции отдела.

2.2.4.3 Организует и разрабатывает (вносит изменения) технические паспорта автоматизированных систем и выделенных (защищаемых) помещений.

2.2.4.4 Организует и принимает участие в разработке технологических процессов обработки информации в автоматизированных системах, а также в процессе внесения изменений в них.

2.2.4.5 Организует и разрабатывает разрешительную систему доступа пользователей к техническим, программным средствам и информационным ресурсам автоматизированных систем, а также вносит изменения в разрешительную систему.

2.2.4.6 Организует и разрабатывает перечни средств защиты информации на объектах информатизации.

2.2.4.7 Организует и разрабатывает (перерабатывает) перечни средств вычислительной техники и их компонентов, прошедших специальные проверки.

2.2.4.8 Организует, разрабатывает и внедряет иные нормативные и распорядительные документы по информационной безопасности.

2.2.4.9 Организует, разрабатывает и внедряет нормативные и распорядительные документы по организации работы шифровальных средств, сетей шифрованной связи.

2.2.4.10 Организует и участвует в подготовке актов ввода в эксплуатацию средств защиты информации автоматизированных систем и выделенных (защищаемых) помещений.

2.2.4.11 Организует и участвует в подготовке актов обследования пригодности помещений к проведению работ со сведениями, составляющими служебную или коммерческую тайну.

2.2.4.12 Организует и участвует в подготовке схем электроснабжения, освещения и заземления, схем прокладки линий телефонной связи, схем локальной вычислительной сети, схем охранной и пожарной сигнализации, схем прокладки линий радиотрансляции и оповещения, схем прокладки систем отопления и кондиционирования объектов информатизации.

2.2.4.13 Организует и участвует в определении перечня лиц, имеющих право доступа на объекты информатизации.

2.2.4.14 Организует и участвует в разработке приказов об обеспечении режима секретности, о назначении ответственных за эксплуатацию автоматизированных систем и выделенных (защищаемых) помещений, администраторов безопасности автоматизированных систем, о проведении аттестации автоматизированных систем и выделенных (защищаемых) помещений, о вводе в действие автоматизированных систем и выделенных (защищаемых) помещений.

2.2.4.15 Участвует в разработке приказов о наложении взысканий по результатам служебных расследований по фактам нарушения информационной безопасности.

2.2.4.16 Организует и участвует в разработке иных приказов в компетенции отдела.

2.2.4.17 Участвует в разработке стандартов организации.

2.2.5 Эксплуатирует объекты информатизации:

2.2.5.1 Организует работы по проведению изменений в настройках средств защиты информации автоматизированных систем при изменении состава или полномочий пользователей для обеспечения доступа лиц к информации, составляющей служебную или коммерческую тайну, а также персональные данные и несекретные сведения.

2.2.5.2 Организует работы по проведению изменений в настройках средств защиты информации автоматизированных систем при изменении состава технических и (или) программных средств.

2.2.5.3 Организует работы по проведению оперативных изменений в настройках средств защиты информации автоматизированных систем при выявлении фактов несовместимости (неработоспособности) системного или прикладного программного обеспечения и программного обеспечения средств защиты информации.

2.2.5.4 Организует работы по проведению оперативных действий по предоставлению пользователям сообщений электронной почты и их вложений, помещенных в карантин средствами контроля почтового трафика локальных вычислительных сетей.

2.2.5.5 Организует работы по проведению оперативных действий по дополнительной настройке средств контроля сетевого и почтового трафика локальных вычислительных сетей, в том числе при использовании сети интернет, для обеспечения доступа лиц к информации, ошибочно блокируемой такими средствами контроля.

2.2.5.6 Организует работы администратора(ов) безопасности на объектах вычислительной техники, предназначенных для обработки сведений, составляющих служебную или коммерческую тайну, а также персональные данные.

2.2.5.7 Обеспечивает выполнение требований по организации и функционированию шифровальных (криптографических) средств.

2.2.5.8 Обеспечивает бесперебойную защищенную криптографическими методами связь.

2.2.5.9 Выполняет требования по безопасности информации при организации технического обслуживания шифровальных средств, объектов вычислительной техники и при отправке их в ремонт.

2.2.5.10 Организует и осуществляет маркирование и опечатывание шифровальных средств, объектов вычислительной техники, технических средств защиты.

2.2.5.11 Организует и обеспечивает создание, хранение и использование эталонных копий программных средств.

2.2.5.12 Организует и обеспечивает выполнение требований по организации учёта, хранения, выдачи и использования устройств и носителей информации.

2.2.5.13 Организует и обеспечивает выдачу идентификаторов для автоматизированных систем.

2.2.5.14 Организует и обеспечивает выдачу защищенных ключевых носителей (eToken, ruToken и т.п.) для систем электронной подписи.

2.2.5.15 Организует и обеспечивает выполнение требований по организации и обеспечению функционирования систем дистанционного банковского обслуживания.

2.2.6 Организует и обеспечивает регистрацию и хранение данных о событиях информационной безопасности:

2.2.6.1 Организует и обеспечивает регистрацию событий и их хранение в системных журналах и журналах средств защиты информации средств вычислительной техники.

2.2.6.2 Организует и обеспечивает регистрацию событий и их хранение в средствах контроля сетевого и почтового трафика локальных вычислительных сетей, в том числе при использовании сети интернет.

2.2.6.3 Организует и обеспечивает регистрацию событий и их хранение в средствах контроля доступа к информационным ресурсам локальных вычислительных сетей, контроля использования носителей информации и принтеров локальных вычислительных сетей.

2.2.7 Организует и осуществляет повседневную, периодическую и дополнительную деятельность отдела:

2.2.7.1 Организует и осуществляет хранение несекретных документов в пределах компетенции отдела.

2.2.7.2 2Организует и осуществляет хранение и учёт конфиденциальных документов в отделе.

2.2.7.3 Осуществляет исполнение несекретных, конфиденциальных и секретных документов в пределах компетенции отдела.

2.2.7.4 Организует и осуществляет учёт несекретных и конфиденциальных устройств (носителей) в пределах компетенции отдела. Ведет журналы учета несекретных и конфиденциальных устройств (носителей), журналы выдачи несекретных и конфиденциальных устройств (носителей).

2.2.7.5 Проводит отбор несекретных, конфиденциальных и секретных документов и носителей для уничтожения.

2.2.7.6 Организует и участвует в уничтожении несекретных, конфиденциальных и секретных документов и носителей.

2.2.7.7 Участвует в инвентаризации основных средств, закрепленных за отделом.

2.2.7.8 Организует и осуществляет хранение и учёт стандартов организации и документов к ним (приказы в области стандартизации, изменения, служебные записки и др.).

2.2.7.9 Составляет отчеты по нерациональному использованию интернет-ресурсов (не в рабочих целях).

2.2.7.10 Составляет отчеты о проведенном обучении работников отдела.

2.2.7.11 Составляет иные отчеты и справки.

2.2.7.12 Осуществляет постановку ежедневных задач отделу.

2.2.7.13 Осуществляет подбор и расстановку кадров в подразделении.

2.2.7.14 Осуществляет мероприятия по повышению деловой активности кадров в подразделении.

2.2.7.15 Обеспечивает необходимые условия труда в подразделении.

2.2.7.16 Представляет интересы Компании в министерствах, ведомствах, учреждениях и организациях по вопросам, входящим в компетенцию отдела.

2.2.7.17 Участвует в мероприятиях при посещении предприятия иностранными представителями.

2.2.7.18 Соблюдает и обеспечивает соблюдение работниками отдела требования правил и норм трудового законодательства, режимных требований, приказов, распоряжений по отделу, трудовой дисциплины, правил внутреннего трудового распорядка.

2.2.7.19 Выполняет другие работы по указанию директора предприятия, начальника управления по безопасности и руководства.

2.3 В части контроля:

2.3.1 Контролирует исполнительскую дисциплину:

2.3.1.1 Осуществляет контроль выполнения работниками отдела их должностных обязанностей.

2.3.1.2 Осуществляет контроль разработки (переработки) перечней программных средств автоматизированных систем, подготавливаемых специалистами подразделений.

2.3.1.3 Осуществляет контроль выполнения подрядчиками хода работ по договорным отношениям.

2.3.1.4 Осуществляет контроль правильности и полноты предоставленных подрядчиками заключений о специальной проверке технических средств, протоколов специальных исследований и предписаний на эксплуатацию средств вычислительной техники, протоколов оценки и (или) контроля эффективности защиты информации на объектах вычислительной техники, заключений по

результатам аттестационных испытаний и аттестатов соответствия автоматизированных систем и выделенных (защищаемых) помещений.

2.3.1.5 Осуществляет контроль правильности и полноты предоставленных подрядчиками финансовых документов по договорным отношениям.

2.3.2 Контролирует меры и средства защиты:

2.3.2.1 Осуществляет контроль срока действия лицензий на право осуществления лицензируемых видов деятельности.

2.3.2.2 Осуществляет контроль срока действия аттестатов соответствия аттестованных объектов информатизации.

2.3.2.3 Осуществляет контроль срока действия сертификатов соответствия на средства защиты информации.

2.3.2.4 Осуществляет контроль действия редакций законов и нормативных документов по вопросам информационной безопасности.

2.3.2.5 Осуществляет контрольные проверки работоспособности и эффективности средств защиты информации.

2.3.2.6 Выявляет и предупреждает применение в сетях шифрованной связи несанкционированных шифров.

2.3.2.7 Организует и осуществляет визуальный осмотр помещений, где обрабатывается и/или обсуждается информация ограниченного доступа, установлены программные или программно-аппаратные средства защиты информации, шифровальное оборудование (средства криптографической защиты) с целью выявления нарушений.

2.3.2.8 Организует и осуществляет инструментальный контроль помещений, где обрабатывается и/или обсуждается информация ограниченного доступа, установлены программные или программно-аппаратные средства защиты информации, шифровальное оборудование (средства криптографической защиты) с целью выявления нарушений.

2.3.2.9 Организует и осуществляет контроль обеспечения информационной безопасности на каналах связи с контрагентами, в том числе с использованием средств шифрования (криптографической защиты).

2.3.3 Организует и контролирует соблюдение установленных правил эксплуатации:

2.3.3.1 Организует и осуществляет контроль деятельности всех подразделений в части выполнения лицензионных требований по информационной безопасности.

2.3.3.2 Организует и осуществляет контроль деятельности всех подразделений в части выполнения руководящих документов по информационной безопасности.

2.3.3.3 Организует и осуществляет контроль выполнения организационно-технических мер в выделенных и защищаемых помещениях и автоматизированных системах.

2.3.3.4 Организует и осуществляет контроль эксплуатации средств защиты информации и антивирусных средств.

2.3.3.5 Организует и осуществляет контроль эксплуатации шифровальных средств.

2.3.3.6 Организует и осуществляет контроль учета, передачи, хранения, использования и уничтожения носителей информации.

2.3.3.7 Организует и осуществляет контроль знаний правил и принципов работы в автоматизированных системах.

2.3.3.8 Организует и осуществляет контроль содержимого системных журналов и журналов средств защиты информации средств вычислительной техники на предмет выявления фактов нарушения установленного порядка работ и попыток несанкционированного доступа на объекты информатизации.

2.3.3.9 Организует и осуществляет контроль содержимого журналов в средствах контроля сетевого и почтового трафика локальных вычислительных сетей, в том числе при использовании сети интернет, на предмет выявления фактов нарушения установленного порядка работ и попыток несанкционированного доступа на объекты информатизации.

2.3.3.10 Организует и осуществляет контроль содержимого журналов в средствах контроля доступа к информационным ресурсам локальных вычислительных сетей, контроля использования носителей информации и принтеров локальных вычислительных сетей на предмет выявления фактов нарушения установленного порядка работ и попыток несанкционированного доступа на объекты информатизации.

2.3.4 Расследует инциденты:

2.3.4.1 Информирует непосредственного руководителя о фактах разглашения сведений, составляющих служебную или коммерческую тайну, а также персональные данные, утрате носителей информации и иных нарушениях или негативных событиях.

2.3.4.2 Участвует в служебных расследованиях по фактам разглашения сведений, составляющих служебную или коммерческую тайну, а также персональные данные, утрате носителей информации.

2.3.4.3 Участвует в проверках и в служебных расследованиях по фактам нарушений режимных требований и требований по защите информации.

2.3.4.4 Организует и осуществляет проверку информации, записанной на носителях и выносимых с территории предприятия (видеокамеры, фотоаппараты, USB-носители), в том числе изъятых у задержанных лиц.

2.3.5 Участвует во внутреннем и внешнем аудите:

2.3.5.1 Участвует в проведении внутренних и внешних проверок состояния информационной безопасности.

2.3.5.2 Участвует в проведении проверок учета, хранения, выдачи и использования документов и носителей информации.

2.4 В части корректирующих действий:

2.4.1 Организует и реагирует на попытки несанкционированных действий и нарушения правил функционирования системы защиты, действует в чрезвычайных ситуациях:

2.4.1.1 Организует и принимает неотложные меры по предотвращению утечки сведений, составляющих служебную и коммерческую тайну, а также персональные данные.

2.4.1.2 Организует и осуществляет эвакуацию электронных носителей информации.

2.4.1.3 Организует и осуществляет планы по устранению замечаний и возможных несоответствий, выявленных при проведении внутреннего и внешних аудитов информационной безопасности.

2.4.2 Выполняет восстановительные процедуры после фактов нарушения информационной безопасности:

2.4.2.1 Обеспечивает своевременное устранение неисправностей, выявленных в ходе технического обслуживания или эксплуатации средств защиты информации и шифровальных (криптографических) средств.

2.4.2.2 Приводит в соответствие и поддерживает в актуальном состоянии организационно-распорядительные и нормативные документы по обеспечению информационной безопасности.

2.4.3 Разрабатывает предложения по совершенствованию информационной безопасности и планы мероприятий:

2.4.3.1 Разрабатывает перспективные и текущие планы мероприятий по вопросам защиты служебной и коммерческой тайны, а также персональных данных, инженерно-техническому обеспечению функционирования системы информационной безопасности.

2.4.3.2 Вносит предложения по изменению перечней сведений, составляющих служебную и коммерческую тайну, конфиденциальную информацию.

2.4.3.3 Вносит предложения к годовой смете расходов, связанных с обеспечением информационной безопасности и защиты служебной и коммерческой тайны, а также персональных данных.

2.4.3.4 Разрабатывает меры по защите информации при возможном использовании технических средств разведки при посещении предприятия иностранными представителями.

2.4.4 Организует и проводит мероприятия с работниками предприятия в сфере информационной безопасности:

2.4.4.1 Разрабатывает профилактические мероприятия по предупреждению нарушений в области защиты информации.

2.4.5 Организует обучение работников предприятия:

2.4.5.1 Определяет потребность и организует обучение работников ОИБ, их профессиональную подготовку и переподготовку по вопросам информационной безопасности.

2.4.5.2 Организует и проводит занятия и консультации с работниками структурных подразделений предприятия по вопросам обеспечения информационной безопасности, шифровальной работе, защите информации при использовании шифровальных средств и технических средств защиты информации.

2.5 В части взаимодействия:

2.5.1 Координирует деятельность обслуживающего персонала и администраторов автоматизированных систем в части обеспечения информационной безопасности:

2.5.1.1 Осуществляет методологическое управление обслуживающим персоналом и администраторами автоматизированных систем в части обеспечения информационной безопасности.

2.5.1.2 Даёт рекомендации и указания обслуживающему персоналу и администраторам автоматизированных систем по их настройке и эксплуатации в части обеспечения информационной безопасности.

2.5.1.3 Осуществляет согласованное взаимодействие с обслуживающим персоналом и администраторами автоматизированных систем в части обеспечения работоспособности таких систем.

2.5.2 Координирует деятельность подразделений в целях защиты служебной и коммерческой тайны, а также персональных данных:

2.5.2.1 Ведет служебную переписку с подразделениями по вопросам, относящимся к компетенции отдела.

2.5.2.2 Составляет заявки на необходимые программные и программно-аппаратные средства (комплексы), запасные части, материалы и принадлежности.

2.5.2.3 Согласовывает служебные записки в пределах компетенции отдела.

2.5.2.4 Согласовывает заявки на доступ к автоматизированным системам.

2.5.2.5 Согласовывает заявки на доступ к сети интернет.

2.5.2.6 Согласовывает заявки на доступ в режимные и защищаемые помещения, в которых расположены автоматизированные системы.

2.5.2.7 Согласовывает положения о структурных подразделениях и должностные инструкции работников предприятия в пределах компетенции отдела.

2.5.2.8 Согласовывает иные документы и вопросы в пределах компетенции отдела.

2.5.2.9 Участвует в оперативных совещаниях у руководства предприятия.

2.5.2.10 Организует и (или) участвует в различных производственных совещаниях.

2.5.2.11 Предоставляет отчетные финансовые документы по договорным отношениям с подрядчиками.

2.5.3 Взаимодействует с компаниями – поставщиками решений и услуг в сфере информационной безопасности:

2.5.3.1 Организует и осуществляет подготовку проектов соглашений и договоров с организациями, предоставляющими услуги в области защиты информации и имеющими лицензию на соответствующий вид деятельности.

2.5.3.2 Организует и осуществляет подготовку проектов соглашений и договоров с организациями на приобретение программных и программно-аппаратных средств (комплексов), лицензий к ним, запасных частей, материалов и принадлежностей.

2.5.3.3 Организует и осуществляет подготовку средств вычислительной техники, предназначенной для проведения специальных проверок и специальных исследований, к вывозу за пределы предприятия, её вывоз, доставку до компании, передачу по акту и последующий возврат техники на филиал.

2.5.3.4 Взаимодействует с компаниями по вопросам, относящимся к компетенции отдела.

2.5.4 Взаимодействует с регуляторами в сфере информационной безопасности:

2.5.4.1 Взаимодействует с ФСБ РФ и ФСТЭК РФ при оформлении и переоформлении лицензий.

2.5.4.2 Взаимодействует с Роскомнадзором по вопросам, связанным с обработкой персональных данных.

2.5.4.3 Готовит документацию и объекты информатизации для получения лицензии ФСБ РФ на осуществление работ, связанных с использованием сведений, составляющих государственную тайну.

2.5.4.4 Готовит документацию и объекты информатизации для получения лицензии ФСБ РФ на осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны в части эксплуатации шифровальных средств, предназначенных для защиты информации, содержащей сведения, составляющие государственную тайну.

2.5.4.5 Готовит документацию и объекты информатизации для получения лицензии ФСТЭК РФ на деятельность по технической защите конфиденциальной информации.

2.5.4.6 Готовит документацию и объекты информатизации для получения лицензии ФСБ РФ на работы, связанные с распространением шифровальных (криптографических) средств, предоставлением услуг в области шифрования информации, не содержащей сведений, составляющих государственную тайну и техническое обслуживание шифровальных (криптографических) средств.

2.6 Организовывает работу по обеспечению сохранности государственной, служебной и коммерческой тайны, контролирует соблюдение всеми работниками отдела требований режима секретности, информационной и общей безопасности.

3 Права

Начальник отдела вправе:

3.1 Знакомиться с проектами решений директора предприятия и начальника управления по безопасности, касающихся деятельности отдела информационной безопасности и спецпроектов.

3.2 Знакомиться с проектами решений руководства, касающихся деятельности отдела информационной безопасности.

3.3 Участвовать в обсуждении вопросов относительно исполняемых им обязанностей.

3.4 Вносить предложения начальнику управления по безопасности о совершенствовании своей деятельности, связанной с выполнением должностных обязанностей, определенных настоящей должностной инструкцией, деятельности отдела в целом и деятельности отдельных сотрудников отдела.

3.5 Выходить с предложением к начальнику управления по безопасности об оказании содействия в исполнении обязанностей и прав, представленных в настоящей должностной инструкции.

3.6 Получать доступ к автоматизированным системам, объектам вычислительной техники, информационным ресурсам и сервисам, работам и документам структурных подразделений предприятия, необходимых для оценки эффективности принимаемых мер по обеспечению информационной безопасности, рисков информационной безопасности, выявления угроз безопасности и возможных нарушений.

3.7 Осуществлять взаимодействие с работниками всех структурных подразделений предприятия при выполнении должностных обязанностей, определенных настоящей должностной инструкцией.

3.8 Требовать от всех работников предприятия соблюдения требований нормативных документов по вопросам информационной безопасности.

3.9 Требовать от работников, допущенных к обработке (обсуждению) защищаемой информации, в том числе передаваемой по каналам шифрованной связи, точного выполнения установленного порядка обращения с информацией.

3.10 Вносить предложения начальнику управления по безопасности о приостановке работ и принятия необходимых мер в случае обнаружения нарушений требований по защите информации, утечки информации или предпосылок к ее утечке.

3.11 Изменять режим работы (или осуществлять отключение) шифровальных средств или отдельных устройств защиты информации на время проведения профилактических работ и производства ремонтных работ по

согласованию с начальником управления по безопасности и руководителем соответствующего структурного подразделения.

3.12 Требовать от работников предприятия представления объяснений, в том числе в письменной форме, по фактам нарушения требований нормативных документов по информационной безопасности.

3.13 Запрашивать лично или по указанию начальника управления по безопасности и получать от руководителей структурных подразделений и их работников справки и сведения, в том числе в устной и письменной форме, а также документы и другие материалы по вопросам, входящих в компетенцию отдела информационной безопасности и необходимых для выполнения своих должностных обязанностей.

3.14 Принимать участие в совещаниях по вопросам обеспечения информационной безопасности и совершенствования систем защиты информации, состава и организации эксплуатации шифровальных средств и технических средств защиты информации на объектах информатизации.

3.15 Готовить предложения о привлечении к проведению работ по защите информации специализированных организаций, имеющих лицензию на соответствующий вид деятельности.

3.16 Подписывать и визировать документы в пределах своей компетенции.

3.17 Издавать распоряжения по отделу и контролировать их исполнение.

3.18 Направлять начальнику управления по безопасности предложения о привлечении подчиненных ему работников к дисциплинарной ответственности, мерам материального воздействия за совершение дисциплинарного проступка, т.е. неисполнение или ненадлежащее исполнение работником по его вине возложенных трудовых обязанностей, правил внутреннего трудового распорядка, за нарушение информационной безопасности, а также представлять предложения о поощрении отличившихся работников.

3.19 Вносить на рассмотрение руководства предприятия предложения о лишении формы допуска к государственной тайне работников предприятия, допустивших нарушения режима секретности.

3.20 Действовать от имени структурного подразделения и представлять его интересы во взаимоотношениях с иными структурными подразделениями предприятия и другими организациями в пределах своей компетенции.

4 Ответственность

Начальник отдела несет ответственность за:

– ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей должностной инструкцией и трудовым договором;

– правонарушения, совершенные в процессе осуществления своей деятельности, в пределах, определенных действующим законодательством РФ;

– причинение материального ущерба, в пределах, определенных действующим законодательством РФ;

– разглашение сведений, составляющих служебную и коммерческую тайну, а также персональные данные, ставшие известными ему в связи с исполнением должностных обязанностей, в пределах, определенных действующим законодательством и нормативными документами;

– нарушение требований нормативных документов по вопросам режима и информационной безопасности, установленного порядка обработки (обсуждения) информации, составляющей служебную и коммерческую тайну, а также персональные данные, передаваемыми, в том числе по каналам шифрованной связи.

Директор по ИБ _____ Волков Д.Д.