Приложение № 1 к приказу
директора ООО «Анапское взморье»
№ _____от «____» _____ 2025г.

ПОЛИТИКА
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ОБЩЕСТВА С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ
«АНАПСКОЕ ВЗМОРЬЕ»

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 0604F3A400C1B2948643864FC331C6210A
Владелец: Шабалина Юлия Александровна
Действителен: с 16.04.2025 по 16.04.2026

г. Анапа, 2025 год

Содержание

1. Общие положения

Настоящая Политика информационной безопасности (далее – Политика) определяет собой официально принятую систему взглядов на проблему обеспечения безопасности информации в автоматизированных системах и представляет собой систематизированное изложение целей и задач, а также организационных, технологических и процедурных аспектов обеспечения безопасности информации объектов информационной инфраструктуры общества с ограниченной ответственностью «Анапское взморье» (далее – Организация).

Настоящая Политика разработана с учетом требований действующего законодательства Российской Федерации и ближайших перспектив развития объектов информационной инфраструктуры, с учетом характеристик и возможностей применения современных организационно-технических методов и средств защиты информации на основе анализа угроз безопасности для информационной инфраструктуры Организации.

Правовой основой для формирования настоящей Политики являются:

− Конституция Российской Федерации;

− Гражданский и Уголовный кодексы;

− Кодекс об административных правонарушениях;

− законы, указы, постановления и другие нормативные документы действующего законодательства Российской Федерации в области информации, информатизации и информационных технологий;

− нормативные и регламентирующие документы государственных органов Российской Федерации (ФСТЭК, ФСБ, Роскомнадзор и др.) в области защиты информации;

− внутренние организационно-распорядительные и нормативно-методические документы Организации.

Основной целью, на которую направлены положения настоящей Политики, является защита информационных активов Организации от возможного нанесения материального ущерба, возникновения при этом репутационных рисков и потерь, посредством случайного или преднамеренного воздействия на информацию, её носители, процессы обработки и передачи, а также минимизация рисков информационной безопасности.

Положения и требования Политики распространяются на все структурные подразделения, в которых осуществляется автоматизированная и смешанная обработка информации, содержащей сведения, составляющие конфиденциальную информацию или персональные данные, а также на подразделения, осуществляющие сопровождение, обслуживание и обеспечение нормального функционирования автоматизированных систем. Основные положения Политики могут быть распространены также на подразделения других организаций и учреждений, осуществляющие взаимодействие в качестве поставщиков и (или) потребителей информации автоматизированных систем Организации.

Политика является методологической основой для формирования и проведения мероприятий в области обеспечения безопасности информации объектов информационной инфраструктуры, принятия согласованных управленческих решений и разработки практических мер, направленных на обеспечение информационной безопасности, координации деятельности структурных подразделений Организации при проведении работ по созданию, развитию и эксплуатации объектов информационной инфраструктуры.

Политика не регламентирует вопросы организации охраны помещений и обеспечения сохранности и физической целостности компонентов информационной инфраструктуры, защиты от стихийных бедствий, и сбоев в системе энергоснабжения, однако предполагает построение системы информационной безопасности на тех же концептуальных основах, что и система безопасности Организации в целом.

Реализация политики обеспечивается соответствующими положениями, порядками, инструкциями, методическими указаниями и системой оценки информационной безопасности, разработанными и введенными в действие в Организации.

Настоящая Политика является локальным нормативным документом постоянного действия.

Настоящая Политика утверждается и вводится в действие, изменяется или признается утратившей силу решением Директора ООО «Анапское взморье», оформленным приказом.

1.1. Обозначения и сокращения.

АРМ	Автоматизированное рабочее место
АС	Автоматизированная система
ГИС	Глобальная информационная сеть
ИБ	Информационная безопасность
ИР	Информационный ресурс
ИС	Информационная система
ИСПДн	Информационная система персональных данных
ИТ	Информационные технологии
ИТКС	Информационно-телекоммуникационная сеть
ЛВС	Локальная вычислительная сеть
НСД	Несанкционированный доступ
ПДн	Персональные данные
ПО	Программное обеспечение
САВЗ	Средство антивирусной защиты
СИБ	Система информационной безопасности
СКЗИ	Средство криптографической защиты информации
СУБД	Система управления базами данных

1.2. Термины и определения.

Автоматизированная система - система, состоящая комплекса средств автоматизации ее деятельности и персонала, реализующая информационную технологию выполнения установленных функций.

Администратор информационной безопасности – работник отдела автоматизации и информационных технологий, осуществляющий контроль за обеспечением защиты информации в информационных системах, а также осуществляющий организацию работ по выявлению и предупреждению возможных каналов утечки информации, потенциальных возможностей осуществления НСД к защищаемой информации.

Автоматизированное рабочее место - это рабочее место специалиста, оснащенное персональным компьютером, программным обеспечением и совокупностью информационных ресурсов индивидуального или коллективного пользования, которые позволяют ему вести обработку данных с целью получения информации, обеспечивающей поддержку принимаемых им решений при выполнении профессиональных функций.

Глобальная информационная сеть – телекоммуникационная сеть, которая распространяется на большую географическую территорию.

Доступность информационных активов - свойство информационной безопасности, состоящее в том, что информационные активы предоставляются авторизованному пользователю, в том виде и в том месте, которые необходимы пользователю, и в то время, когда они ему необходимы.

Защищаемая информация – конфиденциальная информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиям, установленным собственником информации.

Информационные активы – различные виды информации, циркулирующей в информационной системе Организации на всех этапах жизненного цикла (создание, хранение, обработка, передача, уничтожение), находящиеся в распоряжении Организации и представляющие ценность для Организации в интересах достижения целей деятельности.

Информационная безопасность - состояние защищенности интересов (целей) Общества в условиях угроз в информационной сфере. Защищенность достигается обеспечением совокупности свойств ИБ - доступности, целостности, конфиденциальности информационных активов Общества. Приоритетность свойств ИБ определяется ценностью указанных активов для интересов (целей) Общества.

Информационная инфраструктура - система структурных подразделений Общества, обеспечивающих функционирование и развитие информационного пространства и средств информационного взаимодействия. Информационная инфраструктура Общества включает в себя совокупность информационных подсистем, баз данных, систем связи, аппаратно-программных средств и технологий обеспечения сбора, хранения, обработки и передачи информации.

Информационные ресурсы – это отдельные документы или отдельные массивы документов (электронных документов) , документы или массивы документов в информационных системах (библиотеках, базах данных).

Информационная система — система обработки информации и соответствующие ей организационные ресурсы (человеческие, технические, финансовые и т. д.).

Информационная система персональных данных – это совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств, т.е. любая АС Организации в которой хранится и (или) обрабатывается персональная информация как собственных сотрудников, так и сторонних лиц (контрагентов, получателей услуг размещения и проживания и т.п.).

Инцидент информационной безопасности – одно или несколько нежелательных событий информационной безопасности, которые имеют значительную вероятность компрометации бизнес-процессов и угрожают информационной безопасности (например, несанкционированный доступ к информации, нарушение работы информационной системы, угроза внедрения или неудачная попытка получения доступа к ресурсам).

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Конфиденциальная информация – информация ограниченного доступа, не содержащая сведения, составляющие государственную тайну, доступ к которой ограничен федеральными законами (персональные данные) или решением руководителя Организации (коммерческая тайна).

Локальная вычислительная сеть – сеть, которая соединяет компьютерное и периферийное оборудование для обмена данными между сопряженными устройствами.

Несанкционированный доступ – доступ к информации в нарушение должностных полномочий работника, доступ к закрытой для публичного доступа информации со стороны лиц, не имеющих разрешения на доступ к этой информации или получение доступа к информации лицом, имеющим право на доступ к этой информации в объёме, превышающем необходимый для выполнения служебных обязанностей.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Сетевые ресурсы – объекты сети, которые являются источниками информации или источниками сервисов (файлы, каталоги, базы данных, веб-сайты, сетевые диски, файловые сервера и системы хранения данных, принтеры и т.п.).

Системный администратор – работник отдела автоматизации и информационных технологий, в обязанности которого входит настройка, поддержка и совершенствование ИТ-инфраструктуры Организации, включая оборудование, периферию, программное обеспечение и сетевые подключения.

Система информационной безопасности - совокупность защитных мер, защитных средств и процессов их эксплуатации, включая ресурсное и административное (организационное) обеспечение.

Целостность информационных активов - свойство ИБ сохранять неизменность или исправлять обнаруженные изменения в своих информационных активах без ущерба интересам общества.

2. Заявление о политике в области информационной безопасности

Настоящая Политика выражает позицию Организации в области информационной безопасности. Принятием настоящей Политики Организация заявляет и обязуется осуществлять все возможные меры для защиты информации, деловой репутации и бизнес-процессов Организации от риска причинения вреда, убытков и ущерба, возникающих в результате реализации угроз информационной безопасности.

Руководство Организации осознает важность и необходимость продвижения и совершенствования мер и средств обеспечения информационной безопасности в контексте развития законодательства Российской Федерации и регулирования норм информационной безопасности, а также развития используемых информационных технологий при автоматизации бизнес-процессов. Соблюдение принципов информационной безопасности дополнительно позволит упрочить конкурентные преимущества Организации, обеспечить соответствие правовым, регуляторным и договорным требованиям, снизить репутационные риски.

Руководство Организации придерживается взглядов, что соблюдение принципов, правил и требований информационной безопасности является, в том числе, элементом корпоративной культуры. Следование требованиям информационной безопасности является важным условием при осуществлении повседневной деятельности, включая совместную работу с деловыми партнерами. Каждый работник Организации несёт ответственность за безопасную работу с вверенными ему информационными активами, компьютерным оборудованием, мобильными техническими средствами, носителями информации, предоставленной и обрабатываемой информацией Организации.

Руководители структурных подразделений и специалисты по информационной безопасности Организации должны ответственно выполнять свои обязанности, осознавая, что качество их работы непосредственно влияет на состояние защищённости информации, информационных активов и бизнес-процессов Организации.

Работники Организации должны руководствоваться настоящей Политикой в профессиональной деятельности, при взаимодействии между подразделениями, личном развитии и повышении культуры информационной безопасности.

3. Основные принципы обеспечения информационной безопасности

Основными принципами информационной безопасности в общем понимании являются конфиденциальность, целостность и доступность.

Меры по обеспечению конфиденциальности призваны предотвратить несанкционированное разглашение информации. Цель принципа конфиденциальности - сохранить информацию в тайне и обеспечить ее видимость и доступ к ней только тем лицам, которые владеют ею или нуждаются в ней для выполнения своих функций.

Целостность включает в себя защиту несанкционированных изменений данных. Принцип целостности обеспечивает точность и надежность данных и исключает их некорректное изменение, как случайное, так и злонамеренное.

Доступность – это способность делать информационные системы и данные полностью доступными, когда они нужны пользователю, либо когда они необходимы для организационного процесса или для клиентов Организации.

Из основных принципов информационной безопасности следуют общие и специальные принципы безопасного функционирования информационных систем.

Общие принципы.

Своевременность обнаружения проблем, потенциально способных повлиять на бизнес-цели Организации.

Прогнозируемость развития проблем, заключающаяся в выявлении причинно-следственной связи возможных проблем и построении на этой основе точного прогноза их развития.

Оценка степени влияния проблем на бизнес-цели Организации.

Адекватность защитных мер, выбор защитных мер в соответствии с моделями угроз и нарушителей, с учетом соотношения объема возможных потерь от реализации угроз и затрат на реализацию таких мер.

Эффективность реализации принятых защитных мер.

Использование (накопление, обобщение) опыта при принятии и реализации решений.

Непрерывность реализации принципов безопасного функционирования.

Специальные принципы.

Специальные принципы обеспечения информационной безопасности реализуются выполнением перечисленных далее мер.

Определенность целей. Функциональные цели и цели информационной безопасности Организации явно определяются во внутренних документах, чтобы исключить неопределенность, которая приводит к «расплывчатости» организационной структуры, ролей персонала, политик ИБ и невозможности оценки адекватности принятых защитных мер.

Персонификация и адекватное разделение ролей и ответственности. Ответственность должностных лиц структурных подразделений на всех уровнях за решения, связанные с ее активами, персонифицируется и осуществляется преимущественно в форме поручительства. Ответственность определяется адекватно степени влияния на цели организации, фиксируется в политиках, контролируется и совершенствуется.

Адекватность ролей функциям и процедурам и их сопоставимость с критериями и системой оценки. Роли должны адекватно отражать исполняемые функции и процедуры их реализации, принятые в информационных процессах Организации. При назначении взаимосвязанных ролей должна учитываться необходимая последовательность их выполнения. Роль должна быть согласована с критериями оценки эффективности её выполнения. Основное содержание и качество исполняемой роли реально определяются применяемой к ней системой оценки.

Доступность услуг и сервисов. Работники структурных подразделений Организации должны обеспечить для своих клиентов и контрагентов доступность услуг и сервисов в установленные сроки, определенные соответствующими договорами (соглашениями) и/или иными документами.

Знание своих работников и контрагентов. Управляющие органы должны обладать информацией о своих контрагентах, тщательно подбирать работников, вырабатывать и поддерживать корпоративную этику, для создания благоприятной доверительной среды деятельности Организации по управлению активами.

Наблюдаемость и оцениваемость обеспечения ИБ. Любые предлагаемые защитные меры должны быть устроены так, чтобы результат их применения был явно наблюдаем (прозрачен) и мог быть оценен структурным подразделением Организации, имеющим соответствующие полномочия.

4. Цели и задачи обеспечения информации безопасности

Субъектами правоотношений в Организации при использовании АС и в обеспечении безопасности информации являются:

ООО «Анапское взморье», как собственник информационных ресурсов;

структурные подразделения ООО «Анапское взморье», обеспечивающие эксплуатацию автоматизированных систем;

работники структурных подразделений ООО «Анапское взморье», как пользователи и поставщики информации, в соответствии с возложенными на них функциями;

физические и юридические лица, сведения о которых накапливаются, хранятся и обрабатываются в АС;

другие физические и юридические лица, задействованные в процессе создания и функционирования АС (разработчики компонентов системы, организации, привлекаемые для оказания различных услуг в области информационных технологий и др.).

Исходя из сформулированных принципов информационной безопасности основной целью обеспечения безопасности информации для Организации является защита субъектов информационных отношений от возможного нанесения им ущерба посредством случайного или преднамеренного несанкционированного вмешательства в процесс функционирования автоматизированной системы или несанкционированного доступа к циркулирующей в ней информации и незаконного ее использования.

Указанная цель достигается посредством обеспечения и постоянного поддержания следующих свойств информации и автоматизированной системы ее обработки:

доступности обрабатываемой информации для зарегистрированных пользователей;

конфиденциальности определенной части информации, хранимой, обрабатываемой и передаваемой по каналам связи;

целостности и аутентичности информации, хранимой, обрабатываемой и передаваемой по каналам связи.

Для достижения основной цели обеспечения безопасности информации система информационной безопасности автоматизированной системы должна обеспечивать эффективное решение задач защиты он несанкционированного доступа к информационным ресурсам, своевременного выявления источников угроз, создания условий для локализации и минимизации возможного ущерба.

Решение задач обеспечения безопасности информации достигается определением и реализацией комплекса организационных и технических мер, выработанных на основе анализа актуальных угроз информационной безопасности.

5. Объекты, подлежащие защите

Основными объектами Организации, подлежащими защите, являются:

информационные ресурсы, представленные в виде документов и массивов информации, вне зависимости от формы и вида их представления, включающие, в том числе конфиденциальную и открытую информацию;

система формирования, распространения и использования информационных ресурсов, библиотеки, архивы, базы данных, информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации, технический и обслуживающий персонал;

информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены компоненты информационной инфраструктуры.

5.1. Особенности автоматизированной системы.

В автоматизированных системах структурных подразделений Организации циркулирует информация разных категорий. Защищаемая информация может быть совместно использована различными пользователями из различных подсетей единой корпоративной сети.

В ряде подсистем автоматизированных систем предусмотрено взаимодействие с внешними (государственными и коммерческими) российскими организациями, по каналам связи с использованием средств передачи информации.

Комплекс технических средств АС включает средства обработки данных (рабочие станции, серверы БД и т.п.), средства обмена данными в локальной вычислительной сети с возможностью выхода в глобальные сети (кабельная система, мосты, шлюзы, маршрутизаторы и т.п.), а также средства хранения (в т.ч. архивирования) данных.

5.2. Типы информационных активов, подлежащих защите.

В подсистемах АС Организации циркулирует информация различных уровней конфиденциальности, содержащая сведения ограниченного распространения и открытые сведения.

В обращении информации АС присутствуют:

персональные данные;

финансовые документы;

сведения о лицевых счетах гостей в отелях и оказанных им услугах;

отчеты (финансовые, аналитические и др.);

другая информация ограниченного распространения.

Защите подлежит вся информация, циркулирующая в АС и содержащаяся в информационных активах.

5.3. Категории пользователей автоматизированной системы.

В структурных подразделениях Организации есть категории пользователей и обслуживающего персонала, которые должны иметь различные полномочия по доступу к информационным ресурсам АС:

рядовые пользователи (конечные пользователи, работники структурных подразделений);

должностные лица из числа управляющего персонала (руководители структурных подразделений, старшие менеджеры);

администраторы информационной безопасности;

системные администраторы;

работники, осуществляющие обслуживание и техническую поддержку информационной инфраструктуры.

5.4. Уязвимость основных компонентов автоматизированной системы.

Наиболее уязвимыми компонентами АС являются сетевые рабочие станции – АРМ работников структурных подразделений, по причине того, что с АРМ работников могут быть предприняты попытки несанкционированного доступа к информации или попытки несанкционированных действий (непреднамеренных или умышленных) в компьютерной сети. Нарушения конфигурации аппаратно-программных средств рабочих станций и неправомерное вмешательство в процессы их функционирования могут приводить к блокированию информации, невозможности своевременного решения важных задач и выходу из строя отдельных АРМ и подсистем.

В особой защите нуждаются такие элементы сетей как выделенные файловые серверы, серверы баз данных и серверы приложений. Недостатки протоколов обмена и средств разграничения доступа к ресурсам серверов могут дать возможность несанкционированного доступа к защищаемой информации и оказания влияния на работу различных подсистем. При этом могут предприниматься попытки как удаленного (со станций сети), так и непосредственного (с консоли сервера) воздействия на работу серверов и их средств защиты.

6. Угрозы безопасности информации и их источники

Наиболее опасными угрозами безопасности информации, обрабатываемой в автоматизированных системах Организации, являются:

нарушение конфиденциальности (разглашение, утечка) сведений, составляющих служебную тайну или персональные данные;

нарушение работоспособности (дезорганизация работы) АС, блокирование информации, нарушение технологических процессов, срыв своевременного решения задач;

нарушение целостности (искажение, подмена, уничтожение) информационных, программных и других ресурсов АС.

Основными источниками угроз безопасности информации общей автоматизированной системы Организации являются:

работники, являющиеся легальными участниками процессов в АС и действующие в рамках предоставленных полномочий;

работники, являющиеся легальными участниками процессов в АС и действующие вне рамок предоставленных полномочий;

компьютерные злоумышленники, осуществляющие целенаправленные деструктивные воздействия, в том числе использование компьютерных вирусов и других типов вредоносных кодов и атак;

неблагоприятные события природного и техногенного характера;

поставщики программно-технических средств, расходных материалов, услуг и т.п.;

подрядчики, осуществляющие монтаж, пусконаладочные работы оборудования и его ремонт;

несоответствие существующей системы защиты информации требованиям надзорных и регулирующих органов, действующему законодательству;

сбои, отказы, разрушения (повреждения) программных и технических средств;

криминальные элементы.

7. Меры, методы и средства обеспечения безопасности информации

Главная цель организационных мер - сформировать политику в области обеспечения безопасности информации, отражающую подходы к защите информации, и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

7.1. Допуск работников к использованию информационных ресурсов.

Допуск работников Организации, а также других лиц (не являющихся работниками Организации) к работе в АС, уровень их полномочий и непосредственный доступ к ресурсам осуществляется в рамках разрешительной системы и регламентируется установленным порядком.

До предоставления непосредственного доступа к АС ее пользователи, а также руководящий и обслуживающий персонал ознакамливаются, в части их касающейся, с перечнем конфиденциальной информации и своим уровнем полномочий, а также организационно-распорядительной, нормативной, технической и эксплуатационной документацией, определяющей требования и порядок обработки такой информации.

Все лица, допущенные к работе в АС и обслуживающий персонал АС, несут персональную ответственность за нарушения установленного порядка автоматизированной обработки информации, правил хранения, использования и передачи, находящихся в их распоряжении защищаемых ресурсов системы.

7.2. Доступ к техническим средствам.

Эксплуатация защищаемых АРМ и серверов Организации организуется в условиях, исключающим возможность бесконтрольного проникновения и пребывания в помещениях посторонних лиц и обеспечивающих физическую сохранность находящихся в помещении защищаемых ресурсов.

7.3. Разграничение доступа к ресурсам АС, идентификация и аутентификация пользователей, парольная политика.

В целях предотвращения доступа в АС посторонних лиц обеспечивается возможность распознавания системой каждого законного пользователя (или ограниченных групп пользователей).

Каждому пользователю, допущенному к работе с конкретным информационным активом, сопоставляется персональное уникальное имя (идентификатор учётной записи пользователя), под которым он будет регистрироваться и работать в АС.

Аутентификация (подтверждение подлинности) пользователей должна осуществляться на основе использования паролей (секретных слов) или специальных средств аутентификации проверки уникальных характеристик (параметров) пользователей.

После распознавания пользователя система должна осуществлять авторизацию пользователя, определять, какие права предоставлены пользователю, т.е. какие данные и как он может использовать, какие программы может выполнять, когда, как долго и с каких терминалов может работать, какие ресурсы системы может использовать и т.п.

Технические средства разграничения доступа должны быть составной частью единой системы контроля доступа, в том числе и на контролируемую территории, в отдельные помещения и др.

7.4. Регламентация процессов обслуживания и осуществления модификации аппаратных и программных ресурсов.

Аппаратно-программная конфигурация АРМ, на которых обрабатывается защищаемая информация или с которых возможен доступ к защищаемым ресурсам, должна соответствовать кругу возложенных на пользователей данного АРМ функциональных обязанностей.

Ввод в эксплуатацию новых АРМ и все изменения в конфигурации технических и программных средств, существующих АРМ в АС осуществляются только с разрешения руководства Организации в установленном порядке.

Чтобы свести к минимуму вероятность повреждения АС Организации, вводится строгий контроль над внесением изменений. С этой целью устанавливаются правила внесения изменений. Эти правила гарантируют, что процедуры, связанные с безопасностью и контролем, не будут нарушены, что лица, занимающиеся поддержкой, получат доступ только к тем частям системы, которые необходимы для их работы, и что для выполнения любого изменения требуется получить официальное разрешение и подтверждение.

После внесения изменений в ИС, приложения должны анализироваться и тестироваться, чтобы гарантировать отсутствие вредных последствий для безопасности Организации.

Следует препятствовать внесению изменений в пакеты ПО, за исключением необходимых изменений. Все изменения должны строго контролироваться.

7.5. Использование ресурсов локальной сети Организации и глобальной информационной сети «Интернет».

Для выполнения своих служебных обязанностей каждый работник обеспечивается доступом к соответствующим сетевым ресурсам ЛВС Организации и ГИС «Интернет».

Использование работниками ресурсов локальной сети и ГИС «Интернет» в целях, не связанных с выполнением должностных обязанностей, **ЗАПРЕЩЕНО**.

Информация о посещаемых работниками ресурсах сети «Интернет» подлежит протоколированию для последующего анализа. Руководство Организации оставляет за собой право контролировать и анализировать данную информацию.

Руководство Организации оставляет за собой право блокировать или ограничивать доступ пользователей к ресурсам сети «Интернет», содержание которых не имеет отношения к исполнению служебных обязанностей, либо к ресурсам, содержание и направленность которых запрещены законодательством Российской Федерации.

7.6. Использование электронной почты Организации.

Ресурсы электронной почты Организации предоставляются работникам исключительно для выполнения должностных обязанностей.

Использование ресурсов электронной почты Организации в личных целях **ЗАПРЕЩЕНО**.

Информация об использовании работниками ресурсов электронной почты Организации и содержании пересылаемой корреспонденции подлежит протоколированию для последующего анализа.

Руководство Организации оставляет за собой право контролировать и анализировать данную информацию с целью предотвращения нарушений информационной безопасности и утечки сведений, конфиденциального характера.

Руководство Организации оставляет за собой право блокировать доступ работников к ресурсам электронной почты при выявлении фактов нарушения установленного порядка их использования.

7.7. Использование средств криптографической защиты и электронной подписи.

Под средствами криптографической защиты (далее – СКЗИ), в контексте нормативных документов понимаются специальные программы для шифрования данных.

Для обеспечения защиты конфиденциальной информации при реализации бизнес-процессов в Организации используются специальные программы, обеспечивающие применение электронной подписи (криптопровайдеры).

Электронная подпись может применяться для любой формы документа, обрабатываемого электронным способом. Электронная подпись обеспечивает защиту аутентификации и целостности электронных документов.

При использовании электронной подписи, необходимо учитывать требования действующего законодательства Российской Федерации, определяющего условия, при которых цифровая подпись имеет юридическую силу.

Компрометация или потеря криптографических ключей может привести к нарушению конфиденциальности, подлинности и (или) целостности информации, поэтому для эффективного применения криптографических методов в Организации осуществляется управление СКЗИ.

Функции по организации и управлению использованием СКЗИ возлагаются на отдел автоматизации и информационных технологий.

7.8. Защита от вредоносного ПО.

Обязанность по организации и обеспечению защиты информационных активов Организации от воздействия вредоносного ПО возлагается на отдел автоматизации и информационных технологий.

Для предупреждения внедрения на АРМ работников Организации вредоносного ПО пользователям настоятельно рекомендуется выполнять меры превентивного характера, определенные в отдельном порядке.

7.9. Обеспечение и контроль целостности программных и информационных ресурсов.

Контроль целостности программ, обрабатываемой информации и средств защиты, с целью обеспечения неизменности программной среды, определяемой предусмотренной технологией обработки, и защиты от несанкционированной корректировки информации может обеспечиваться:

средствами подсчета контрольных сумм;

средствами сравнения критичных ресурсов с их эталонными копиями (и восстановления в случае нарушения целостности);

средствами разграничения доступа (запрет доступа с правами модификации или удаления).

7.10. Контроль событий безопасности.

Контроль событий безопасности осуществляется при помощи программных или аппаратно-программных средств контроля.

Средства контроля должны обеспечивать обнаружение и регистрацию всех событий (действий пользователей, попыток НСД и т.п.), которые могут повлечь за собой нарушение политики безопасности и привести к возникновению инцидентов информационной безопасности.

7.11. Управление и контроль эффективности системы обеспечения безопасности информации.

Управление системой обеспечения безопасности информации в АС представляет собой целенаправленное воздействие на компоненты системы обеспечения безопасности, с целью достижения требуемых показателей и норм защищенности циркулирующей в АС информации в условиях реализации основных угроз безопасности.

Главной целью управления системой обеспечения безопасности информации является повышение надежности защиты информации в процессе ее обработки, хранения и передачи.

Управление системой обеспечения безопасности информации реализуется специализированной подсистемой управления, представляющей собой совокупность органов управления, технических и программных средств, а также организационных мероприятий.

Функциями подсистемы управления являются: информационная, управляющая и вспомогательная.

Функции органа управления информационной безопасностью в Организации возлагается на отдел автоматизации и информационных технологий.

Контроль эффективности системы защиты информации осуществляется с целью своевременного выявления и предотвращения утечки информации за счет несанкционированного доступа к ней, а также предупреждения возможных специальных воздействий, направленных на уничтожение информации, разрушение средств информатизации.

Оценка эффективности мер защиты информации проводится с использованием организационных, технических и программных средств контроля на предмет соответствия установленным требованиям.

8. Политика Организации в отношении обработки персональных данных

В автоматизированных системах структурных подразделений Организации циркулируют следующие категории персональных данных:

персональные данные, отнесенные в соответствии с Федеральным законом «О персональных данных» к биометрическим персональным данным;

персональные данные, которые не могут быть отнесены к специальным категориям персональных данных, к биометрическим персональным данным, к общедоступным или обезличенным персональным данным (иные персональные данные);

персональные данные, отнесенные в соответствии с Федеральным законом «О персональных данных» к общедоступным или обезличенным персональным данным.

Объем и содержание персональных данных, а также перечень действий и способы обработки персональных определены и осуществляются в соответствии с требованиями законодательства Российской Федерации.

Все персональные данные, как работников, так и контрагентов, получаются непосредственно от субъектов персональных данных, на основании их письменного согласия.

Обработка персональных данных в структурных подразделениях Организации осуществляется автоматизированным и смешанным способом обработки.

Автоматизированная обработка и хранение персональных данных осуществляется в базах данных и АС, размещенных на территории Российской Федерации.

Персональные данные, как работников Организации, так и контрагентов обрабатываются исключительно в целях обеспечения бизнес-процессов Организации и не подлежат трансграничной передаче.

Субъекты персональных данных имеют право:

на получение полной информации об обрабатываемых в Организации их персональных данных;

на доступ к обрабатываемым в Организации своим персональным данным, включая получение копий документов;

на уточнение своих персональных данных, а при необходимости, их блокирование или уничтожение, в случаях, определенных законодательством Российской Федерации;

на отзыв согласия на обработку своих персональных данных.

Все действия по обеспечению прав в отношении обработки персональных данных выполняются на основании письменного обращения субъекта персональных данных к руководству Организации.

По достижению целей обработки в информационных системах и при отсутствии необходимости дальнейшего хранения, персональные данные уничтожаются (обезличиваются) в порядке, определенном в законодательстве Российской Федерации с соблюдением установленных сроков.

Передача персональных данных третьему лицу, при необходимости, осуществляется на основании Федерального закона «О персональных данных» или с согласия субъекта персональных данных, оформленного установленным порядком. В том случае, если Организация поручает обработку персональных данных третьему лицу на основании договора, существенным условием такого договора является обязанность обеспечения третьим лицом конфиденциальности персональных данных и безопасности персональных данных при их обработке.

Требования по обеспечению безопасности персональных данных в ИСПДн реализуются комплексом организационных, технологических, технических и программных мер, средств и механизмов защиты информации.

Все информационные активы, принадлежащие ИСПДн, защищаются от воздействий вредоносного программного обеспечения.

Руководители подразделений, эксплуатирующих и обслуживающих ИСПДн, организуют выполнение требований безопасности персональных данных при их обработке в ИСПДн на рабочих местах.

Работники, непосредственно осуществляющие обработку персональных данных в ИСПДн, обязаны действовать в соответствии с установленным порядком и соблюдать требования документов по обеспечению ИБ.

Пользователям ИСПДн и работникам (в т.ч. привлеченным специалистам), осуществляющим обслуживание и поддержку ИСПДн, **ЗАПРЕЩЕНО:**

использовать и обрабатывать персональные данные вне рамок, установленных целями обработки, либо с превышением разрешенного объема информации, либо с превышением установленных полномочий и прав доступа к ИСПДн;

вносить несанкционированные изменения в структуру и состав технических средств и программного обеспечения ИСПДн, в том числе подключать к техническим средствам ИСПДн, неразрешенные для использования внешние мобильные устройства и отчуждаемые запоминающие устройства, вне зависимости от целей и продолжительности периода времени;

отключать или вносить изменения в настройки средств защиты информации ИСПДн;

осуществлять несанкционированное и (или) нерегистрируемое (бесконтрольное) копирование персональных данных.

Контроль обеспечения безопасности информации при использовании ИСПДн осуществляется работниками отдела автоматизации и информационных технологий, на которых возлагаются функции подразделения информационной безопасности (администраторов информационной безопасности), как с помощью штатных средств системы защиты информации, так и с помощью специальных средств контроля и технологического мониторинга.

9. Ответственность за нарушения в области информационной безопасности

Работники Организации должны выполнять требования и правила информационной безопасности при работе с информацией и информационными активами.

Требования нормативных документов и правила обеспечения информационной безопасности обязательны для выполнения всеми без исключения работниками Организации и должны учитываться во взаимоотношениях с контрагентами и представителями структур, взаимодействующих с Организацией.

Руководство Организации возлагает ответственность на руководителей структурных подразделений:

за организацию повседневной деятельности и выделение необходимых ресурсов для обеспечения информационной безопасности как неотъемлемой составляющей бизнес-процессов;

за своевременную идентификацию значимых информационных активов;

за предъявление установленных требований информационной безопасности к работникам Организации и контрагентам, использующим информационные активы Организации, и контроль за их выполнением.

При использовании ГИС «Интернет», при общении в социальных сетях и мессенджерах, использовании электронной почты, других средств телекоммуникаций и мобильных технических средств работникам Организации рекомендуется проявлять осмотрительность и сдержанность, чтобы не допускать рисков личной безопасности, а также избегать непреднамеренной утечки служебной информации.

По каждому серьезному нарушению требований информационной безопасности (инциденту информационной безопасности), допущенному работниками структурных подразделений Организации, руководством Организации инициируется разбирательство. К виновным в нарушениях необходимо применять адекватные меры воздействия. Мера ответственности работников за действия, совершенные в нарушение установленных правил информационной безопасности, должна определяться нанесенным ущербом, наличием злого умысла и другими факторами.

Каждый работник Организации, допущенный к использованию информационных активов, за несоблюдение (нарушение) требований информационной безопасности несет дисциплинарную, гражданско-правовую, административную и уголовную ответственность в соответствии с действующим законодательством Российской Федерации.

Контрагенты, представители структур, взаимодействующих с Организацией по различным направлениям, использующие информационные активы Организации, а также предоставленную Организацией информацию, несут ответственность в соответствии с договорными отношениями, заключенными с ООО «Анапское взморье», а также применимым законодательством.