Общество с ограниченной ответственностью

«Спортивно-оздоровительный комплекс «Атлант»

(ООО «СОК «Атлант»)

УТВЕРЖДАЮ
Директор ООО СОК «Атлант»

_____М.И.Щипакин

«_____» 17 ИЮН 2024 2024 г.

Дата введения в действие:

«_____» 17 ИЮН 2024 2024 г.

ПОЛОЖЕНИЕ

ООО «СОК «Атлант»

«по обеспечению информационной безопасности»

г. Ярославль

2024

Содержание

1. Общие положения

Настоящее Положение по обеспечению информационной безопасности (далее - Положение) определяет основные цели и задачи, а также общую стратегию и принципы обеспечения безопасности информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, обрабатываемой в информационных системах (в т.ч. информационных системах персональных данных и автоматизированных системах управления техническими процессами), а также при обработке информации без применения средств автоматизации в ООО «СОК «Атлант» (далее - Общество)

Положение служит основой для разработки комплекса организационных и технических мер по обеспечению информационной безопасности в Обществе, а также нормативных и методических документов, обеспечивающих ее реализацию, и не предполагает подмены функций государственных органов власти Российской Федерации, отвечающих за обеспечение безопасности информационных технологий и защиту информации.

Правовой базой для разработки настоящего положения служат требования действующих законодательных и нормативных документов по обеспечению информационной безопасности.

Настоящее Положение обязательно для выполнения всеми работниками Общества в пределах своих должностных обязанностей.

2. Правовое обеспечение

Обеспечение информационной безопасности в информационных системах Общества осуществляется в соответствии с законами Российской Федерации, указами и распоряжениями президента Российской Федерации, постановлениями и распоряжениями Правительства Российской Федерации, нормативными и руководящими документы Федеральных служб РФ, а именно:

- Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных»;
- Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне»;
- Постановление Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Постановление Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Приказ ФАПСИ от 13.06.2001 г. № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованиемередств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;
- Приказ ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСТЭК России от 14.03.2014 г. № 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»;
- Приказ ФСБ России от 10.07.2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием

средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

- Приказ ФАПСИ от 13.06.2001 г. № 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащейсведений, составляющих государственную тайну»;
- «Методический документ. Меры защиты информации в государственных информационных системах», утвержденный ФСТЭК России от 11.02.2014 г.

3. Цели и задачи обеспечения информационной безопасности

3.1. Целями обеспечения информационной безопасности в Обществе являются:

- Защита интересов Общества, работников и иных субъектов информационных отношений, взаимодействующих с Обществом, от возможного нанесения ущерба их деятельности посредством случайного или преднамеренного несанкционированного вмешательства в процесс функционирования информационных систем Общества, нарушения работы технических и программных средств, приводящего к недоступности информации, разглашению, искажению, уничтожению защищаемой информации и ее незаконному использованию;
- Обеспечение устойчивого и корректного функционирования технических и программных компонентов информационных систем Общества и предотвращение реализации угроз безопасности;
- выполнение требований действующего законодательства Российской Федерации, нормативно-технических документов ФСБ России и ФСТЭК России в области информационной безопасности.

3.2. Для достижения целей обеспечения информационной безопасности в Обществе обеспечивается решение следующих задач:

- Защита от вмешательства в процесс функционирования информационных систем посторонних лиц (возможность использования системы и доступ к ее ресурсам должны иметь только зарегистрированные пользователи);
- Разграничение доступа пользователей к техническим, программным и информационным ресурсам информационных систем (возможность доступа только к тем ресурсами выполнения только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих служебных обязанностей);
- Обеспечение аутентификации пользователей, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации), а также определение автора при создании и модификации информации;
- Регистрация и периодический контроль действий пользователей при работе в информационных системах Общества и периодический контроль корректности их действий;
- Контроль целостности (обеспечение неизменности) среды функционирования информационных систем Общества и ее восстановление в случае нарушения;
- Защита от несанкционированной модификации и контроль целостности используемых в информационных системах Общества программных средств и данных, а также защиту от несанкционированного внедрения вредоносных программ;
- Защита информации ограниченного доступа, хранимой и обрабатываемой в Обществе, от несанкционированного разглашения или искажения;
- Обеспечение исправности и нормального функционирования применяемых в информационных системах Общества средств защиты информации;
- Своевременное выявление источников угроз безопасности информации, причин и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений, создание механизма оперативного реагирования на угрозы безопасности информации;
- Создание условий для минимизации наносимого ущерба неправомерными

действиями, ослабление негативного влияния и ликвидация последствий нарушения информационной безопасности в Обществе.

3.3. Решение вышеперечисленных задач в Обществе осуществляется с помощью:

- Учета всех подлежащих защите информационных ресурсов (каналов связи, технических и программных средств, входящих в состав информационных систем);
- Регламентации процессов обработки подлежащей защите информации, действий работников, осуществляющих обслуживание и модификацию программных и технических средств информационных систем, на основе утвержденных локальных нормативных документов по вопросам обеспечения информационной безопасности в Обществе;
- Назначения и подготовки работников, ответственных за организацию и осуществление мероприятий по обеспечению информационной безопасности в Обществе;
- Наделения каждого работника минимально необходимыми для выполнения им своихфункциональных обязанностей полномочиями по доступу к информационным системам;
- Знания и строгого соблюдения всеми работниками, использующими и обслуживающими технические и программные средства информационных систем, требований локальных нормативных документов по вопросам обеспечения информационной безопасности в Обществе;
- Контроля соблюдения пользователями информационных систем требований по обеспечению информационной безопасности;
- Персональной ответственности за свои действия каждого работника, участвующего в рамках своих функциональных обязанностей в процессах обработки информации и имеющего доступ к ресурсам информационных систем;
- Принятия мер по обеспечению физической целостности технических средств информационных систем и поддержанием необходимого уровня защищенности их компонентов;
- Использования физических и технических (программно-аппаратных) средств защитыинформации;
- Проведения анализа эффективности принятых мер и применяемых средств защиты информации в Обществе.

4. Объекты защиты

Объектами защиты в Обществе являются:

- Обрабатываемая информация, в т.ч. персональные данные, информация, составляющая коммерческую тайну и иная конфиденциальная информация, не составляющая государственную тайну;
- Технологическая информация, в т.ч. информация о параметрах (состоянии) управляемого (контролируемого) объекта или процесса (входная (выходная) информация, управляющая (командная) информация , контрольно-измерительная информация, иная критически важная (технологическая) информация);
- Программно-технический комплекс, включающий технические средства (в том числе автоматизированные рабочие места, промышленные серверы, телекоммуникационное оборудование, каналы связи, программируемые логические контроллеры, исполнительные устройства) , программное обеспечение (в том числе микропрограммное, общесистемное, прикладное)
- Средства защиты информации;
- Объекты и помещения, в которых размещены технические средства, входящие в состав информационных систем Общества.

5. Меры по обеспечению информационной безопасности

5.1. Для реализации целей и решения задач по обеспечению информационной безопасности в Обществе применяются организационные и технические меры защиты информации, предусмотренные действующим законодательством Российской Федерации.

5.2. Перечень реализуемых в Обществе мер защиты информации определяется в соответствии с классом защищенности или уровнем защищенности персональных данных, определяемым в соответствии с действующим законодательством Российской Федерации.

5.3. Принимаемые организационные и технические меры обеспечивают доступность обрабатываемой информации (исключение неправомерного блокирования информации), ее целостность (исключение неправомерного уничтожения, модифицирования информации), и конфиденциальность (исключение неправомерного доступа, копирования, предоставления или распространения информации).

5.4. Принимаемые организационные и технические меры не должны оказывать отрицательного влияния на штатный режим функционирования информационных систем Общества.

5.5. Состав, порядок и методы реализации применяемых организационных и технических мер регламентируются локальными нормативными документами Общества. Работники, допущенные к работе в информационных системах Общества, обязаны знать и соблюдать требования данных документов в пределах своих должностных обязанностей.

5.6 Меры по обеспечению информационной безопасности в информационных системах обеспечивают

5.6.1. В части идентификации и аутентификации субъектов доступа и объектов доступа:

- Однозначную идентификацию и аутентификацию всех видов пользователей (внутренних и внешних). Для АСУТП, предусматривается также идентификация и аутентификация устройств;
- Управление идентификаторами и средствами аутентификации;
- Защиту обратной связи при вводе аутентификационной информации.

5.6.2. В части управления доступом субъектов доступа к объектам доступа:

- Управление учетными записями пользователей и назначение их полномочий (ролей)в рамках минимально необходимых для выполнения ими своих должностных обязанностей;
- Санкционирование доступа к объектам доступа в соответствии с минимально необходимыми правами и привилегиями;
- Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационных систем;
- Реализацию защищенного удаленного доступа к информационным системам Общества через внешние информационно-телекоммуникационные сети и из внешних информационных систем (если таковой предусмотрен).

5.6.3. В части ограничения программной среды и управления обновлениями программного обеспечения:

- Управление установкой (инсталляцией) программного обеспечения, в том числе определение перечня программного обеспечения, подлежащего установке, настройка параметров установки и контроль за установкой программного обеспечения;
- Получение обновлений программного обеспечения и средств защиты информации из доверенных источников, контроль их целостности, проведение тестирования и установку обновлений.

5.6.4. В части защиты машинных носителей информации:

- Учет машинных носителей информации и управление физическим доступом к ним;
- Контроль использования интерфейсов ввода вывода;
- Контроль уничтожения (стирания) информации на машинных носителях информации при их передаче между пользователями и в сторонние организации, в том числе для ремонта или утилизации.

5.6.5. В части регистрации событий безопасности:

- Определение событий безопасности, подлежащих регистрации, а также состава и содержания информации;
- Реагирование на сбои при регистрации событий безопасности;
- Определение сроков хранения и защиты информации о событиях безопасности;
- Мониторинг (просмотр и анализ) событий безопасности, подлежащих регистрации, с установленной периодичностью и своевременное выявление признаков инцидентов безопасности в информационных системах Общества.

5.6.6. В части антивирусной защиты:

- Использование средств антивирусной защиты на всех компонентах информационных систем Общества где возможно применение данных средств защиты и где их применение не нарушает нормального функционирования информационных систем общества;
- Использование компенсирующих мер при невозможности использование средств антивирусной защиты;
- Регулярное обновление базы данных признаков вредоносных компьютерных программ на всех компонентах информационных систем Общества, использующих средства антивирусной защиты.

5.6.7. В части контроля (анализа) защищенности информации:

- Выявление, анализ уязвимостей информационных систем Общества и оперативное устранение вновь выявленных уязвимостей;
- Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации;
- Контроль состава, работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации.

5.6.8. В части обеспечения целостности и доступности информации:

- Осуществление резервного копирования защищаемой информации и обеспечение возможности её восстановления;
- Обеспечение возможности восстановления программного обеспечения при нештатных ситуациях;
- Контроль целостности программного обеспечения, применяемого в АСУТП Общества.

5.6.9. В части защиты технических средств:

- Организацию контролируемой зоны Общества, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования;
- Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения Общества, в которых они установлены;
- Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр;
- Защиту от внешних воздействий.

5.6.10. В части защиты информационных систем и их компонентов:

- Разделение функций по управлению (администрированию) информационными системами Общества с иными функциями;
- Сокрытие архитектуры и конфигурации информационных систем общества;
- Обеспечение защиты обрабатываемой информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи.

5.6.11. В части реагирования на инциденты информационной безопасности:

- Обеспечение выявления инцидентов информационной безопасности;
- Проведение анализа и устранение последствий выявления инцидентов информационной безопасности;
- Принятие мер по предотвращению повторного возникновения инцидентов

информационной безопасности.

5.6.12. В части управления конфигурацией информационных систем Общества:

- Управление изменениями конфигурации информационных систем общества;
- Проведение анализа потенциального воздействия планируемых изменений в конфигурации информационных систем Общества на обеспечение защиты информации.

5.7. Для реализации мер защиты информации в информационных системах общества применяются средств защиты информации, включая средства криптографической защиты информации (далее - средства защиты). Состав применяемых средств защиты определяется в соответствии с действующим законодательством Российской Федерации.

5.8. К применяемым в информационных системах Общества средствам защиты предъявляются следующие требования:

- Возможность обеспечения нейтрализации актуальных угроз безопасности информации, обрабатываемой в информационных системах Общества;
- Обеспечение защиты информации в соответствии с установленным классом или уровнем защищенности персональных данных информационных систем Общества;
- Высокая надежность функционирования в условиях круглосуточной работы;
- Применяемые средства защиты не должны негативно сказываться на функционировании информационных систем общества.

5.9. Основной задачей при выборе средств защиты является обеспечение целостного взаимодействия и тесной интеграции с информационными системами общества. При этом должен соблюдаться принцип разумной достаточности применяемых средств защиты информации.

5.10. При эксплуатации средств защиты все работники Общества должны выполнять требования действующего законодательства Российской Федерации, локальных нормативных документов Общества, а также эксплуатационной документации производителя средств защиты в пределах своих должностных обязанностей.

6. Процессы управления информационной безопасностью

6.1. Управление рисками

Выбор мер по обеспечению информационной безопасности и средств защиты, применяемых в Обществе, основывается на проведении анализа рисков нарушения основных свойств безопасности информации, обрабатываемой в Обществе.

Основой оценки рисков является оценка условий и факторов, которые могут стать причиной нарушения основных свойств безопасности информации в информационных системах Общества.

Результатом проведения анализа рисков является комплекс мер, направленных на снижение возможного негативного влияния на основную деятельность Общества при реализации той или иной угрозы и обеспечивающих достаточный уровень защищенности информационных систем Общества.

6.2. Управление инцидентами информационной безопасности

Для обеспечения эффективного разрешения инцидентов информационной безопасности в Обществе, минимизации потерь и уменьшения риска возникновения повторных инцидентов осуществляется эффективное управление инцидентами информационной безопасности.

В отношении каждого произошедшего инцидента выполняется его анализ, и разработка эффективных мер реагирования на данный инцидент.

6.3. Мониторинг текущего уровня обеспечения информационной безопасности

Процесс мониторинга обеспечения информационной безопасности в Обществе включает в себя контроль выполнения применяемых организационных и технических мер обеспечения информационной безопасности, анализ параметров конфигурации и настройки технических и программных средств, а также средств защиты информации.

При проведении мероприятий, связанных с контролем функционирования применяемых мер обеспечения информационной безопасности, работниками Общества соблюдаются следующие принципов:

- Не нарушать функционирование текущей деятельности Общества;
- Действовать в соответствии с локальными нормативными документами Общества по обеспечению информационной безопасности;

- Не скрывать факты выявленных инцидентов и нарушений требований информационной безопасности;
- Оформлять отчеты, подтверждающие выполнение мероприятий по обеспечению информационной безопасности.

Информация, полученная в ходе проведения контролирующих мероприятий о действиях, событиях и параметрах, имеющих отношение к функционированию защитных мер, консолидируется и храниться в местах, исключающих получение к ней несанкционированного доступа.

6.4. Аудит обеспечения информационной информации

В целях оценки текущего уровня обеспечения информационной безопасности в информационных системах Общества на проводится аудит информационной безопасности.

Аудит информационной безопасности осуществляться силами структурного подразделения, ответственного за обеспечение информационной безопасности. Для проведения аудита также могут привлекаться сторонние организации, имеющие лицензию на осуществление данного вида деятельности.

Результатом выполнения аудитов по информационной безопасности являются отчеты о выполненном аудите информационной безопасности.

По результатам аудита разработаются действия, необходимые для устранения обнаруженных в процессе аудита несоответствий и вызвавших их причин.

6.5. Управление персоналом

При приеме новых работников производится обязательное проведение проверки достоверности сообщаемых ими данных и оценки их профессиональных навыков.

В отношении работников, на регулярной основе осуществляется повышение их осведомленности в вопросах обеспечения информационной безопасности.

7. Зоны ответственности участников процесса обеспечения информационной безопасности

7.1. Руководство Общества:

- Создает условия, при которых каждый работник Общества знает свои обязанности изадачи в отношении обеспечения информационной безопасности в Обществе и обеспечивает наличие необходимого разделения функций и полномочий в целях недопущения конфликта интересов.
- Назначает работников, ответственных за реализацию процессов обеспечения информационной безопасности в Обществе.
- Обеспечивает достаточную численность и квалификацию персонала, ответственного за построение и поддержание процессов обеспечения информационной безопасности в Обществе,внедрение и управление средствами защиты информации, а также контроль и мониторинг текущего состояния обеспечения информационной безопасности в информационных системах Общества.

7.2. Структурное подразделения, ответственное за обеспечение информационной безопасности в Обществе:

- Подготавливает предложения по доработке нормативных документов, регламентирующих обеспечение информационной безопасности в Обществе;
- Вырабатывает комплекс мер по обеспечению информационной безопасности в информационных системах Общества и контролируют их реализацию;
- Обеспечивает функционирование средств защиты информации, используемых в информационных системах общества;
- Контролирует выполнение установленных правил и процедур обеспечения информационной безопасности в Обществе.

7.3. Структурное подразделение, ответственное за эксплуатацию информационных систем Общества:

- Разрабатывает процедуры эффективного управления техническими и программными

средствами информационных систем Общества и применяет их в практической деятельности;

- Осуществляет мероприятия по поддержке сопровождения и использования информационных систем;
- Осуществляет поддержку функционирования информационных систем и принимает необходимые меры по конфигурированию систем для обеспечения необходимого уровня информационной безопасности;
- Обеспечивает отказоустойчивость всего программно-аппаратного комплекса и выполнение процедур восстановления работоспособности после отказов компонентов.

7.4. Руководители структурных подразделений:

- Обязаны соблюдать требования действующего законодательства Российской Федерации и внутренних документов Общества в части обеспечения информационной безопасности;
- Обеспечивают контроль за соблюдением норм и правил обеспечения информационной безопасности в своем структурном подразделении и информируют структурное подразделение, ответственное за обеспечение информационной безопасности, нарушениях действующих правил обеспечения информационной безопасности;
- Организуют проведение необходимого инструктажа по вопросам выполнения правилинформационной безопасности для всех работников своего структурного подразделения;
- Контролируют выполнение работниками в своем структурном подразделении установленных правил в целях обеспечения сохранности технических средств и носителей информации;
- Контролируют доступ работников к необходимым им информационными ресурсам в соответствии с их должностными обязанностями.

7.5. Работники Общества:

- Выполняют требования локальных нормативных документов Общества, регламентирующих вопросы обеспечения информационной безопасности;
- Соблюдают конфиденциальность данных, доступ к которым был ими получен в рамках выполнения своих должностных обязанностей;
- Обеспечивают сохранность технических средств и носителей информации, используемых ими в работе;
- Своевременно информируют руководителя своего структурного подразделения или структурное подразделение, ответственное за обеспечение информационной безопасности о всех случаях нарушения информационной безопасности.

7.6. Сторонние физические и юридические лица:

- Соблюдают и выполняют требования локальных нормативных документов Общества регламентирующие вопросы обеспечения информационной безопасности при исполнении договорных обязательств.

8. Ответственность нарушителей информационной безопасности

Ответственность за нарушение информационной безопасности в Общества несет каждый работник Общества в пределах своих должностных обязанностей.

Все работники Общества, допущенные к работе в информационных системах Общества, а также ответственные за обеспечение информационной безопасности в информационных системахОбщества, обязаны ознакомиться с данным положением под подпись.

Работники несут персональную ответственность за нарушение требований настоящего положения в пределах своих должностных обязанностей в соответствии с локально нормативнымидокументами Общества, а также действующим законодательством Российской Федерации.

Термины и определения

Автоматизированная система управления технологическим процессом - система, состоящая из персонала и комплекса технических и программных средств, предназначенных для автоматизации управления технологическим оборудованием.

Аутентификация - действия по проверке подлинности субъекта доступа и/или объекта доступа, а также по проверке принадлежности субъекту доступа и/или объекту доступа предъявленного идентификатора доступа и аутентификационной информации.

Идентификация - действия по присвоению субъектам и объектам доступа идентификаторов и/или по сравнению предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информационная система - совокупность содержащихся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Инцидент информационной безопасности - Непредвиденное или нежелательное событие (группа событий) ИБ, которое привело (могут привести) к нарушению функционирования информационного ресурса или возникновению угроз безопасности информации или нарушению требований по защите информации.

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

Средство защиты информации - техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

Лист согласования документа

Положение
«По обеспечению информационной безопасности»

Главный инженер Долинкин В.Л.

Менеджер по персоналу Фролова О.В.

Лист регистрации изменений

№ изм.	Дата утверждения изменения	Кем внесено изменение		Дата внесения изменения
		Подпись	Расшифровка подписи	