Общество с ограниченной ответственностью «Фан-Тур»

ИНН 7717136079 ОГРН 1027717008857
127427, Г.МОСКВА, ВН.ТЕР.Г. МУНИЦИПАЛЬНЫЙ ОКРУГ МАРФИНО, УЛ КАШЁНКИН ЛУГ, Д. 8, К. 1, КОМ. 13

«УТВЕРЖДАЮ»

ООО “Фан-Тур”

_____ / Д.А. Горожанкин /

Приказ №1-перс от «01» апреля 2025 г.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ООО “Фан-Тур”

г. Москва,
2025г.

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

ЭП – электронно-цифровая подпись

АРМ –-автоматизированное рабочее место

ИС – информационная система

ИБ – информационная безопасность

МЭ – межсетевой экран

НСД – несанкционированный доступ

НДВ- не декларированные возможности

ОС – операционная система

ПДн – персональные данные

ПО – программное обеспечение

СЗИ – средства защиты информации

СКЗИ – средства криптографической защиты информации Суперпользователь – администратор ИС, имеющий право на
выполнение всех без исключения операций

ООО – Общество с ограниченной ответственностью

ВВЕДЕНИЕ

Политика информационной безопасности Общества (далее – Политика) разработана в соответствии с требованиями действующего законодательства и нормативных актов Российской Федерации: Федерального закона от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 8 августа 2001 г. N 128-ФЗ «О лицензировании отдельных видов деятельности», Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» , постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Предметом настоящего документа является:

-порядок доступа к информационным системам;

-сетевая безопасность;

-локальная безопасность;

-физическая безопасность (доступ в помещения);

-обеспечение защиты персональных данных;

-дублирование, резервирование и хранение информации;

-ответственность за соблюдение положений Политики ИБ

1. ОБЩИЕ ПОЛОЖЕНИЯ

Цели и задачи

Концептуальная схема информационной безопасности Общества направлена на защиту его информационных активов от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий персонала, технических сбоев, неправильных технологических и организационных решений в процессах обработки, передачи и хранения информации и обеспечение нормального функционирования технологических процессов.

Направление информационной безопасности создано в Обществе со следующими задачами и функциями, определяемыми постановлением Правительства 915-12 "О лицензировании отдельных видов деятельности" и Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»:

- разработка и совершенствование нормативно-правовой базы обеспечения информационной безопасности;

- выявление, оценка и прогнозирование угроз информационной безопасности; организация технической защиты информации, участие в проектировании систем защиты;

- проведение периодического контроля состояния ИБ, учет и анализ результатов с выработкой решений по устранению уязвимостей и нарушений;

- контроль за использованием закрытых каналов связи и ключей с цифровыми подписями;

- организация плановых проверок режима защиты, и разработка соответствующей документации, анализ результатов, расследование нарушений;

- разработка и осуществление мероприятий по защите персональных данных; организация взаимодействия со всеми структурами, участвующими в их обработке, выполнение требований законодательства к информационным системам персональных данных, контроль действий операторов, отвечающих за их обработку.

2. ОРГАНИЗАЦИОННО-ПРАВОВОЙ СТАТУС СОТРУДНИКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- сотрудники имеют право беспрепятственного доступа во все помещения, где установлены технические средства с Информационными системами, право требовать от руководства подразделений и администратора прекращения автоматизированной обработки информации, персональных данных, при наличии непосредственной угрозы защищаемой информации;

- имеют право получать от пользователей и администраторов необходимую информацию по вопросам применения информационных технологий, в части касающейся вопросов информационной безопасности;

- Системный администратор имеет право проводить аудит действующих и вновь внедряемых ИС, ПО, на предмет реализации требований защиты и обработки информации, соответствию требований законодательства, запрещать их эксплуатацию, если не отвечают требованиям или продолжение эксплуатации может привести к серьезным последствиям в случае реализации значимых угроз безопасности;

-сотрудники имеют право контролировать исполнение утвержденных нормативных и организационно-распорядительных документов, касающихся вопросов информационной безопасности.

3. ОБЛАСТЬ ДЕЙСТВИЯ

Требования настоящей Политики распространяются на всех сотрудников Общества (штатных, временных, работающих по контракту и т.п).

Положения настоящей Политики применимы для использования во внутренних нормативных и методических документах, а также в договорах с контрагентами.

4. ПОРЯДОК ДОСТУПА ПОЛЬЗОВАТЕЛЕЙ К ИНФОРМАЦИОННЫМ СИСТЕМАМ, В КОТОРЫХ ОБРАБАТЫВАЕТСЯ ИНФОРМАЦИЯ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА

Управление доступом к информационным системам реализовано с помощью

штатных средств (операционных систем MS Windows) в целях идентификации и проверки подлинности субъектов доступа при входе в ИС, а так же для их регистрации входа (выхода) в систему (из системы).

Требование идентификации и аутентификации при входе в информационную систему определяется приказом ФСТЭК № 21 от 18.02.2013г.

В составе ИСПДн используются сертифицированные или разрешенные к применению ФСТЭК средства защиты информации от НСД.

Все действия пользователей ИС регистрируются в журналах событий системного и прикладного ПО. Данные электронные журналы доступны для чтения, анализа и резервного копирования только администратору соответствующего ПО, который несет персональную ответственность за полноту и точность отражения в журнале имевших место событий.

Запрещается доступ суперпользователей к серверам и базам данных под единой или предопределенной учетной записью.

Любой доступ к базам данных ИС без фиксации в соответствующих журналах или лог-файлах запрещен.

В случае увольнения сотрудника, имеющего права суперпользователя, пароли доступа к серверам и базам данных меняются в тот же день.

Порядок доступа, получения логинов и паролей, определяется Порядком предоставления прав доступа пользователям ИСПДн, Положением о разграничении прав доступа к обрабатываемым ПДн, Порядком выдачи и смены паролей для доступа к ИСПДн.

5. СЕТЕВАЯ БЕЗОПАСНОСТЬ

5.1 Доступ из Интернет в сеть Общества:

- доступ во внутреннюю сеть осуществляется только через настроенный межсетевой экран;
- доступ из вне периметра сети разрешен только по распоряжению ООО “Фан-Тур” по определенному порту и на определенное время;
- не допускается удаленный доступ в локальную сеть с использованием не персонифицированных, групповых и анонимных учетных записей;
- не допускается использование программ удаленного администрирования типа TeamViewer. Как исключение, по согласованию с руководством возможно подключение для удаленной настройки ПО на ограниченное время. Настройка и конфигурация средств обнаружения вторжений, межсетевых экранов должны обеспечивать оперативное обнаружение несанкционированного доступа к ресурсам сети для принятия мер блокирования проникновения нейтрализации последствий.

При администрировании удаленного доступа к ресурсам корпоративной сети Общества предъявляются следующие требования:

- удаленный доступ пользователей к ресурсам и сервисам компьютерной сети Общества обеспечивается на основе зарегистрированных персональных учетных записей, с использованием технологии VPN, других протоколов шифрования ;
- доступ предоставляется сроком на 3 месяца, при необходимости продлевается с разрешения директора;
- делается соответствующая запись в Журнале учета предоставления удаленного доступа;
- список сотрудников, которым предоставлен удаленный доступ поддерживается в актуальном состоянии.

5.2 В целях обеспечения безопасности и нормального функционирования компьютерных сетей запрещается:

- самовольно подключать компьютерное оборудование (беспроводные точки доступа, маршрутизаторы, компьютеры и др.) к сети Общества и присваивать ему сетевое;
- перемещать компьютеры между сетевыми розетками и другими коммуникационными устройствами без согласования с системным администратором;
- использовать информационные ресурсы Общества для сетевых игр, распространения коммерческой рекламы; организации СПАМа.
- сканировать узлы сети неуполномоченными на то сотрудниками.

6. СРЕДСТВА ЗАЩИТЫ, МАРШРУТИЗАТОРЫ И МЕЖСЕТЕВЫЕ ЭКРАНЫ:

Приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. N 21 определяет как необходимость организацию управления (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы.

Для анализа защищенности ИС применяются специализированные программно-аппаратные средства – сканеры безопасности. Проводится выявление и анализ уязвимостей и несоответствия в настройках ОС, ПО, СУБД, сетевого оборудования. Выявленные уязвимости протоколируются и передаются системному администратору для устранения в установленные

сроки. Запрещается использовать ПО снятое с поддержки, имеющее уязвимости, с просроченными сертификатами.

Подсистема обнаружения вторжений, обеспечивает выявление сетевых атак на элементы ИС подключенные к сетям общего пользования и (или) международного обмена.

Функционал подсистемы реализуется программными и программноаппаратными средствами, на межсетевых экранах. Администратор сети ведет протоколирование и регулярный мониторинг доступа, контролирует содержание трафика с использованием специализированного ПО, проводит анализ логфайлов.

На межсетевом экране заводится лог-файл, куда записываются все обращения к ресурсам (попытки создания соединений). Доступ к лог-файлам имет администратор сети.

Доступ из одного сегмента сети в другой ограничивается и разделяется маршрутизаторами. Настройкой маршрутизаторов занимается отдел сетевого и системного администрирования.

Приобретение и установка средств и систем защиты ИС осуществляются по согласованию с системным администратором.

Сеть ИСПДн выделена в отдельный сегмент и защищена межсетевым экраном.

7. ЛОКАЛЬНАЯ БЕЗОПАСНОСТЬ

7.1 Антивирусная защита

Антивирусная защита предназначена для обеспечения антивирусной защиты серверов и АРМ пользователей Общества.

На каждом работающем компьютере, или сервере при вводе в эксплуатацию или после переустановки системным администратором в обязательном порядке устанавливается и активируется антивирусная программа.

Отключение или не обновление антивирусных средств не допускается. Установка и обновление антивирусных средств в организации контролируется системным администратором.

Система обнаружения атак, встроенная в антивирусную программу, сохраняет информацию об атаках и подозрительной активности в лог-файлы, которые анализирует ответственный системный администратор.

В случае массированной вирусной атаки системный администратор принимает меры к локализации, блокированию распространения, определяет источник заражения, характер действия и распространения вируса, нейтрализуют последствия атаки. При необходимости ставятся патчи и необходимые обновления ПО, закрывающие уязвимости, используемые вирусами.

Пользователи руководствуются требованиями антивирусной защиты, изложенными в Правилах использования информационных систем.

7.2 Защита электронного документооборота.

Передача информации конфиденциального характера за периметр сети осуществляется только по защищенным каналам. Защищенные каналы строятся с использованием криптозащиты, на базе решений VipNet, VPN, Банк-клиент и др.

Криптографическая защита предназначена для исключения НСД к защищаемой информации, при ее передачи по каналам связи сетей общего пользования и (или) международного обмена.

Криптографическая защита реализуется путем внедрения криптографических программно-аппаратных комплексов КриптоПро или иных аналогичных программ.

Электронные подписи выдаются удостоверяющим центром на определенное лицо, по его документам на основании заключенного договора. Инициатором заключения договора является

системный администратор или руководитель Общества. После получения ключа ЭП, снимается копия сертификата и регистрируется в журнале у системного администратора.

Ключи электронных подписей должны храниться в сейфах ответственных лиц. Доступ неуполномоченных лиц к носителям ключей должен быть исключен. Передача ключей запрещена.

Запрещается оставлять носители с ЭП установленными в компьютер, при покидании рабочего места.

Компьютеры, на которых установлены средства криптозащиты, должны соответствовать требованиям, изложенным в документации по КриптоПро.

Внутренний документооборот является подсистемой ИСПДн, осуществляется в защищенном исполнении с использованием ПО, для которого актуальны угрозы 3-го типа, связанные с наличием НДВ в ПО.

7.3 Разграничение прав доступа к информационным системам и системам хранения данных, защита от НСД

Для доступа к информационным системам сотрудник Общества должен ввести логин и пароль.

При предоставлении доступа к ОС, приложениям ИС, реализуется принцип минимума привилегий доступа.

В целях защиты информации организационно и технически разделяются подразделения Общества, имеющие доступ и работающие с различной информацией (в разрезе ее конфиденциальности и смысловой направленности). Данная задача решается с использованием возможностей конкретных ИС, где в целях обеспечения защиты данных доступ и права пользователей ограничивается набором прав и ролей. В случае обработки информации конфиденциального характера права назначаются администратором ИС по ролевой матрице доступа, в соответствии с функциональными обязанностями, определяемыми должностью.

Администратором ИС проводится анализ журналов доступа к ресурсам ИС, фиксируются попытки НСД.

Для защиты от НСД на компьютерах в сегментах сети, где обрабатывается информация конфиденциального характера используются продукты, рекомендованные системным администратором. Не допускается использование учетных записей уволенных сотрудников.

7.4 Использование электронной почты, сети Интернет

Не допускается распространять материалы, использование и распространение которых ограничено действующим законодательством РФ.

Пересылка информации конфиденциального характера осуществляется только с использованием корпоративной почты.

Электронная почта на рабочем месте сотрудника используется только для служебной, и иной, предусмотренной должностными обязанностями переписки.

Логин и пароль к корпоративной электронной почте для сотрудников выдает системный администратор.

Запрещается открывать письма с подозрительными вложениями, с незнакомого адреса и.т.п., о получении подобных писем сообщается системному администратору.

Запрещается публиковать информацию конфиденциального характера в социальных сетях, пересылать через системы мгновенного обмена сообщениями (ICQ, Jabber, мобильных мессенджерах и. т. п.).

Запрещается использование облачных сервисов на рабочих местах сотрудников, обрабатывающих информацию конфиденциального характера.

Доступ через беспроводную сеть разрешается только к общедоступным ресурсам сети. Беспроводные точки устанавливает и администрирует системный администратор.

Самостоятельно скачивать и устанавливать программное обеспечение разрешается только уполномоченным на то сотрудниками.

Запрещается несогласованная установка роутеров WiFi.

8.ФИЗИЧЕСКАЯ БЕЗОПАСНОСТЬ

Все объекты критичные с точки зрения информационной безопасности (сервера баз данных, маршрутизаторы) находятся в контролируемых зонах.

При неавтоматизированной обработке информации конфиденциального характера документы (личные дела сотрудников, карточки пациентов, карточки лицевых счетов, картотека и.т.д.) должны храниться в местах (шкафах), исключаемых несанкционированный доступ к ним. Требования к обеспечению безопасности определены в документе Порядок доступа в помещения, в которых обрабатывается информация конфиденциального характера.

В контролируемых зонах Общества ведется видеонаблюдение.

9. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

Все сотрудники Общества, являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные внутренними нормативными документами правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности обработки ПДн.

Компетентность пользователей в области обеспечения ИБ достигается обучением правилам безопасной (с точки зрения ИБ) работы, осведомленности об источниках потенциальных угроз и периодическими проверками их знаний и навыков. Занятия с пользователями проводятся системным администратором на регулярной основе не реже двух раз в год.

При допуске сотрудника к выполнению обязанностей связанных с обработкой персональных данных непосредственный начальник подразделения, в которое он поступает, организует ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн, подает служебную системному администратору о предоставлении доступа к ИСПДн с указанием предполагаемой роли сотрудника.

Далее сотрудник проходит инструктаж у системного администратора и расписывается об ознакомлении с Положением о защите персональных данных, получает у администратора ИСПДн логин и пароль к учетной записи с правами, согласно ролевой матрицы доступа.

Порядок работы с запросами на предоставление сведений по персональным данным определяется утвержденными локальными нормативными документами.

Общедоступными персональными данными сотрудников являются фамилия, имя, отчество, занимаемая должность, подразделение, а пациентов- фамилия, имя, отчество, номер карты.

Сотрудники Общества должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица.

Сотрудникам, обрабатывающим ПДн, запрещается устанавливать любое программное обеспечение, подключать личные мобильные устройства и отчуждаемые незарегистрированные носители информации, а также записывать на них защищаемую информацию, за исключением случаев, предусмотренных функциональными обязанностями.

Сотрудникам запрещается разглашать содержание защищаемой информации, которая стала им известна при работе с информационными системами Общества, третьим лицам, согласно Положения о защите персональных данных.

Запрещается хранение информации конфиденциального характера локально на компьютере, не оснащенном программными средствами предотвращения несанкционированного доступа.

Допуск к ИСПДн третьих лиц для осуществления ими договорных обязательств осуществляется при выполнении требований, предъявляемых к защите информации и

соблюдения конфиденциальности, отражаемых в договоре, согласованном с ОСБ на этапе заключения.

СКЗИ при обработке персональных данных в Обществе не используются.

10. ДУБЛИРОВАНИЕ, РЕЗЕРВНОЕ КОПИРОВАНИЕ И ХРАНЕНИЕ ИНФОРМАЦИИ

Для обеспечения физической целостности данных, во избежание умышленного или неумышленного уничтожения или искажения защищаемой информации и конфигураций информационных систем организуется резервное копирование баз данных, конфигураций, файлов настроек, конфигурационных файлов.

Для обеспечения гарантированного восстановления особо важной информации, которая может быть утеряна вследствие аппаратных сбоев, воздействия вирусов-шифровальщиков производится ежедневное резервное копирование содержимого дисков. Данный процесс запускается по служебной записке сотрудника на имя директора Общества.

Ответственными за организацию резервного копирования, хранения копий и восстановления информации являются администраторы ИС.

Еженедельно архивная копия базы данных ИСПДн дублируется Системным администратором с использованием соответствующего оборудования на отчуждаемый носитель.

11. ОТВЕТСТВЕННОСТЬ ЗА СОБЛЮДЕНИЕ ПОЛОЖЕНИЙ ПОЛИТИКИ ИБ

Общее руководство обеспечением информационной безопасности осуществляет ООО “Фан-Тур”.

Ответственным за поддержание положений настоящей Политики в актуальном состоянии, создание, внедрение и внесение изменений в процессы информационной безопасности системный администратор.

Нарушение требований Политики, локальных нормативных актов по обеспечению ИБ является чрезвычайным происшествием и влечет за собой последствия, предусмотренные действующим законодательством Российской Федерации, локальными нормативными актами, договорами, заключенными между обществом и сотрудниками (пациентами).

Степень ответственности за нарушение требований локальных нормативных актов в области ИБ определяется в каждом конкретном случае

Руководители структурных подразделений, несут персональную ответственность за обеспечение ИБ в возглавляемых ими подразделениях, обязаны незамедлительно сообщать системному администратору о всех инцидентах, связанных с нарушениями требований информационной безопасности.

Виды ответственности, предусмотренные федеральными законами об обращении с информацией конфиденциального характера:

- гражданско-правовая ответственность;
- дисциплинарная ответственность;
- уголовная ответственность;
- административная ответственность.

12. ПОРЯДОК ПЕРЕСМОТРА ПОЛИТИКИ ИБ

Пересмотр Политики информационной безопасности производится не реже одного раза в три года и имеет целью приведение в соответствие определенных Политикой защитных мер реальным условиям и текущим требованиям к защите информации.

Внеплановое внесение изменений в настоящую Политику может производиться по результатам анализа инцидентов ИБ, актуальности, достаточности и эффективности используемых мер обеспечения ИБ, результатам проведения внутренних аудитов ИБ и других контрольных мероприятий

Пересмотр Политики осуществляется рабочей группой и утверждается ООО “Фан-Тур”.