ПРИЛОЖЕНИЕ

к Приказу № ____ от «__» _____ 20__ г.

ООО «Доктор Наников»

ООО «Доктор Наников»

Инструкция
лица, ответственного за обеспечение безопасности персональных данных

Ставрополь, 20__ г.

Содержание

Термины и определения 3
1 Общие положения 6
2 Обязанности Ответственного за обеспечение безопасности персональных данных 6
2.1 Идентификация и аутентификация субъектов доступа и объектов доступа 7
2.2 Управление доступом 7
2.3 Ограничение программной среды 9
2.4 Защита машинных носителей 9
2.5 Регистрация событий безопасности 9
2.6 Антивирусная зашита 9
2.7 Обнаружение вторжений 10
2.8 Контроль (анализ) защищенности персональных данных 10
2.9 Обеспечение целостности информационной системы персональных данных и персональных данных 12
2.10 Обеспечения доступности персональных данных 12
2.11 Защита среды виртуализации 12
2.12 Защита технических средств 12
2.13 Выявление инцидентов и реагирование на них 12
2.14 Управление конфигурацией информационной системы персональных данных и системы защиты персональных данных 13
3 Ответственность 13
4 Порядок пересмотра 13
Приложение 1. Ежегодный план мероприятий по обеспечению безопасности персональных данных 14
Приложение 2. Отчет о выполнении ежегодного плана мероприятий по обеспечению безопасности персональных данных 15

Термины и определения

Администратор системы защиты персональных данных (Администратор СЗПДн) – пользователь, уполномоченный выполнять некоторые действия (имеющий полномочия) по администрированию (управлению) системы защиты персональных данных в соответствии с установленной ролью.

Анализ уязвимостей – мероприятия по выявлению, идентификации и оценке уязвимостей информационной (автоматизированной) системы в интересах определения возможности реализации угроз безопасности информации и способов предотвращения ущерба.

Аутентификационная информация [информация аутентификации] – информация, используемая для установления подлинности (верификации) субъекта доступа в информационной (автоматизированной) системе.

Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора (подтверждение подлинности субъекта доступа в информационной (автоматизированной) системе).

Внешняя информационная система – информационная система, взаимодействующая с информационной системой оператора из-за пределов границ информационной системы оператора.

Внешняя информационно-телекоммуникационная сеть – информационно-телекоммуникационная сеть, взаимодействующая с информационной системой оператора из-за пределов границ информационной системы оператора.

Доступность информации – свойство безопасности информации, при котором субъекты доступа, имеющие права доступа, могут беспрепятственно их реализовать.

Идентификатор – представление (строка символов), однозначно идентифицирующее субъект и (или) объект доступа в информационной (автоматизированной) системе.

Идентификация – присвоение субъектам доступа, объектам доступа идентификаторов (уникальных имен) и (или) сравнение предъявленного идентификатора с перечнем присвоенных идентификаторов.

Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Инцидент – непредвиденное или нежелательное событие (группа событий) безопасности, которое привело (могут привести) к нарушению функционирования информационной (автоматизированной) системы или возникновению угроз безопасности информации (нарушению конфиденциальности, целостности, доступности).

Компонент программного обеспечения – составная часть (программный модуль) программного обеспечения, выполняющая определенную функцию.

Компонент информационной системы – часть информационной (автоматизированной) системы, включающая некоторую совокупность информации и обеспечивающих ее обработку отдельных информационных технологий и технических средств.

Конфиденциальность информации – свойство безопасности информации, при котором доступ к ней осуществляют только субъекты доступа, имеющие на него право.

Лица, допущенные к обработке персональных данных – работники структурных подразделений и иные лица, допущенные к обработке персональных данных, в соответствии с приказом руководителя организации (или иного уполномоченного лица).

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Объект доступа – единица информационного ресурса информационной (автоматизированной) системы (файл, техническое средство, узел сети, линия (канал) связи, мобильное устройство, программа, том, каталог, запись, поле записей и иные объекты), доступ к которой регламентируется правилами разграничения доступа и по отношению к которой субъекты доступа выполняют операции.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными. Под оператором персональных данных в настоящей Инструкции понимается Государственное бюджетное учреждение здравоохранения Ставропольского края «Городская клиническая консультативно-диагностическая поликлиника» города Ставрополя (далее – ГБУЗ СК «ГККДП» г. Ставрополя).

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

Пользователь – лицо, которому разрешено выполнять некоторые действия (операции) по обработке информации в информационной (автоматизированной) системе или использующее результаты ее функционирования.

Программная среда – совокупность программного обеспечения, используемого в информационной (автоматизированной) системе для решения одной или нескольких задач.

Роль – предопределенная совокупность правил, устанавливающих допустимое взаимодействие между пользователем и информационной (автоматизированной) системой.

Система защиты персональных данных (СЗПДн) – комплекс организационных и (или) технических мер, определенных с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах персональных данных.

Событие безопасности (информационной) – идентифицированное возникновение состояния информационной(автоматизированной) системы (сегмента, компонента информационной (автоматизированной) системы), сервиса или сети, указывающее на возможное нарушение безопасности информации, или сбой средств защиты информации, или ранее неизвестную ситуацию, которая может быть значимой для безопасности информации.

Субъект доступа – пользователь, процесс, выполняющие операции (действия) над объектами доступа и действия которых регламентируются правилами разграничения доступа.

Техническое средство – аппаратное или программно-аппаратное устройство, осуществляющее формирование, обработку, передачу или прием информации в информационной (автоматизированной) системе.

Удаленный доступ – процесс получения доступа (через внешнюю сеть) к объектам доступа информационной (автоматизированной) системы из другой информационной системы (сети) или со средства вычислительной техники, не являющегося постоянно (непосредственно) соединенным физически или логически с информационной системой, к которой он получает доступ.

Управление доступом – ограничение и контроль доступа субъектов доступа к объектам доступа в информационной (автоматизированной) системе в соответствии с установленными правилами разграничения доступа.

Устройство – конструктивно законченный технический элемент, имеющий определенное функциональное назначение в информационной (автоматизированной) системе.

Уязвимость информационной (автоматизированной) системы – недостаток (слабость) информационной (автоматизированной) системы, который (которая) создает потенциальные или реально существующие условия для реализации или проявления угроз безопасности информации.

Целостность информации – свойство безопасности информации, при котором отсутствует любое ее изменение либо изменение субъектами доступа, имеющими на него право.

1 Общие положения

Настоящий документ ООО «Доктор Наников» Инструкция лица, ответственного за обеспечение безопасности персональных данных» (далее – Инструкция) определяет функции и обязанности лица, ответственного за обеспечение безопасности ПДн ООО «Доктор Наников» (далее – Ответственный за обеспечение безопасности ПДн).

Ответственный за обеспечение безопасности ПДн назначается приказом руководителя (или иного уполномоченного лица) из числа работников ООО «Доктор Наников»

Администратор СЗПДн руководствуется в своей работе нормативными правовыми актами Российской Федерации и методическими документами регулирующих органов, регламентирующими деятельность по обработке и обеспечению безопасности (защите) ПДн, а также локальными актами ООО «Доктор Наников» Краткое наименование в части обеспечения безопасности ПДн. Администратор СЗПДн по вопросам, касающимся обеспечения безопасности ПДн, обязан выполнять распоряжения лица, ответственного за организацию обработки ПДн (далее – Ответственный за организацию обработки ПДн).

На время отсутствия Ответственного за обеспечение безопасности ПДн (отпуск, болезнь, пр.) его обязанности исполняет лицо, назначенное в установленном порядке, которое приобретает права и ответственность за надлежащее исполнение возложенных на него обязанностей.

2 Обязанности Ответственного за обеспечение безопасности персональных данных

Ответственный за обеспечение безопасности ПДн совместно с руководством ООО «Клиника Доктор КИТ» Краткое наименование и другими должностными лицами ООО «Доктор Наников» участвует в обеспечении безопасности ПДн в ИСПДн ООО «Доктор Наников»в соответствии с требованиями законодательства Российской Федерации о ПДн, в том числе:

- принимает участие в определении уровня защищенности ПДн в ИСПДн;
- принимает участие в определении актуальных угроз безопасности ПДн при их обработке в ИСПДн;
- принимает участие в формировании требований по обеспечению безопасности ПДн и формировании технических и организационных мер по обеспечению безопасности ПДн. При необходимости вносит предложения по корректировке набора организационных и технических мер по обеспечению безопасности ПДн;
- принимает участие в создании системы защиты персональных данных;
- осуществляет контроль соблюдения в ООО «Доктор Наников» принципов обработки персональных данных;

- участвует в проведении расследований случаев несанкционированного доступа к ПДн и других нарушений правил обработки ПДн;
- организует и осуществляет процессы удаления и уничтожения ПДн;
- участвует в проведении расследований случаев несанкционированного доступа к ПДн и других нарушений правил обработки ПДн;
- осуществляет процессы удаления и уничтожения ПДн в соответствии с разделом 6 документа ООО «Доктор Наников» Положение об обработке персональных данных», в том числе контролирует процессы удаления и уничтожения ПДн в ИСПДн или на машинных носителях ПДн.

2.1 Идентификация и аутентификация субъектов доступа и объектов доступа

Ответственным за обеспечение безопасности ПДн совместно Администратором СЗПДн, Администратором ИСПДн определяется перечень типов устройств, используемых в ИСПДн и подлежащих идентификации и аутентификации до начала информационного взаимодействия.

2.2 Управление доступом

Ответственный за обеспечение безопасности ПДн осуществляет следующие функции по управлению учетными записями пользователей, в том числе внешних пользователей:

- осуществляет контроль, пересмотр и изменение (корректировка) прав доступа пользователей, прекращение доступа пользователей;
- при получении Заявки на предоставление/изменение прав доступа:
  - верифицирует пользователя (осуществляет проверку личности пользователя, его должностных (функциональных) обязанностей) для заведения учетной записи пользователя;
  - определяет тип учетной записи (внутреннего пользователя, внешнего пользователя; системная, приложения; гостевая (анонимная), временная и (или) иные типы записей);
  - определяет минимально необходимые права и привилегии (в том числе необходимость предоставления удаленного доступа и использования съемных машинных носителей информации), основываясь на должностных (функциональных) обязанностей и на задачах, решаемых пользователями в ИСПДн.

Ответственный за обеспечение безопасности ПДн осуществляет следующие функции по реализации защищенного удаленного доступа:

- устанавливает (в том числе документально) виды доступа, разрешенные для удаленного доступа к объектам доступа ИСПДн;
- обеспечивает ограничение использования удаленного доступа в соответствии с задачами (функциями) ИСПДн, для решения которых такой доступ необходим;

- предоставляет удаленный доступ только тем пользователям, которым он необходим для выполнения установленных должностных обязанностей (функций).

Ответственный за обеспечение безопасности ПДн регламентирует и контролирует использование в ИСПДн технологий беспроводного доступа, в том числе:

- ограничивает использование технологий беспроводного доступа (беспроводной передачи данных, беспроводного подключения оборудования к сети, беспроводного подключения устройств к средству вычислительной техники) в соответствии с задачами (функциями) ИСПДн, для решения которых такой доступ необходим;
- предоставляет беспроводной доступ только тем пользователям, которым он необходим для выполнения установленных должностных обязанностей (функций);
- осуществляет мониторинг использования технологий беспроводного доступа.

Ответственный за обеспечение безопасности ПДн регламентирует и контролирует использование в ИСПДн мобильных технических средств, в том числе:

- устанавливает (в том числе документально) виды доступа (беспроводной, проводной (коммутируемый), широкополосный и иные виды доступа), разрешенных для доступа к объектам доступа ИСПДн с использованием мобильных технических средств, входящих в состав ИСПДн, в соответствии с задачами (функциями) ИСПДн, для решения которых такой доступ необходим;
- ограничивает использование мобильных технических средств в соответствии с задачами (функциями) ИСПДн, для решения которых использование таких средств необходимо;
- предоставляет доступ с использованием мобильных технических средств только тем пользователям, которым он необходим для выполнения установленных должностных обязанностей (функций);
- обеспечивает запрет возможности запуска без команды пользователя в ИСПДн программного обеспечения (программного кода), используемого для взаимодействия с мобильным техническим средством;
- осуществляет мониторинг использования мобильных технических средств.

Ответственный за обеспечение безопасности ПДн осуществляет управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы), в том числе:

- осуществляет предоставление доступа в соответствии с Заявкой на предоставление/изменение прав доступа;
- определяет типы прикладного программного обеспечения ИСПДн, к которым разрешен доступ авторизованным (уполномоченным) пользователям из внешних информационных систем;

- определяет системные учетные записи, используемые в рамках данного взаимодействия;
- определяет порядок предоставления доступа к ИСПДн авторизованными (уполномоченным) пользователями из внешних информационных систем;
- определяет порядок обработки, хранения и передачи информации с использованием внешних информационных систем.

2.3 Ограничение программной среды

Ответственный за обеспечение безопасности ПДн осуществляет следующие функции по ограничению программной среды:

- согласует перечень компонентов программного обеспечения (состава и конфигурации), подлежащих установке в ИСПДн после загрузки операционной системы, определенный Администратором ИСПДн и Администратором СЗПДн;
- осуществляет контроль установленного (инсталлированного) в ИСПДн программного обеспечения (состав компонентов, параметры установки, конфигурация компонентов) на предмет соответствия его утвержденному перечню («Перечень программного обеспечения и (или) его компонентов, разрешенных к установке в информационных системах персональных данных»).

2.4 Защита машинных носителей

Ответственный за обеспечение безопасности ПДн осуществляет контроль выполнения процедур по учету машинных носителей ПДн, выполняемых Администратором СЗПДн.

2.5 Регистрация событий безопасности

Ответственный за обеспечение безопасности ПДн совместно с Администратором СЗПДн и Администратором ИСПДн определяет перечень событий безопасности, регистрация которых осуществляется в текущий момент времени, исходя из возможностей реализации угроз безопасности информации.

2.6 Антивирусная зашита

Ответственный за обеспечение безопасности ПДн осуществляет следующие функции по антивирусной защите:

- организует процесс настройки параметров средств антивирусной защиты;
- организует процесс предварительной проверки устанавливаемого (обновляемого) программного обеспечения на отсутствие вирусов;
- организует процесс своевременного обновления программного обеспечения средств антивирусной защиты и базы данных признаков вредоносных компьютерных программ (вирусов);
- проводит периодический контроль работы средств антивирусной защиты.

2.7 Обнаружение вторжений

Ответственный за обеспечение безопасности ПДн осуществляет следующие функции по обнаружению вторжений:

- организует процесс настройки параметров средств обнаружения вторжений;
- организует процесс своевременного обновления программного обеспечения средств обнаружения вторжений и базы решающих правил;
- проводит периодический контроль работы средств обнаружения вторжений.

2.8 Контроль (анализ) защищенности персональных данных

Ответственный за обеспечение безопасности ПДн осуществляет следующие функции по анализу уязвимостей ИСПДн и их устранению:

- анализ Отчетов Администратора СЗПДн по результатам выявления (поиска) уязвимостей и оценку достаточности реализованных мер защиты информации;
- анализ изменения угроз безопасности информации в ИСПДн, возникающих в ходе его эксплуатации, и оценка возможных последствий реализации угроз безопасности информации в ИСПДн;
- включение мероприятий по устранению уязвимостей в план мероприятий по обеспечению безопасности ПДн;
- обеспечение устранения выявленных уязвимостей, в том числе путем установки обновлений программного обеспечения средств защиты информации, общесистемного программного обеспечения, прикладного программного обеспечения или микропрограммного обеспечения технических средств Администратором СЗПДн или Администратором ИСПДн;
- информирование пользователей ИСПДн, Администраторов ИСПДн, Администраторов СЗПДн о результатах поиска уязвимостей и оценки достаточности реализованных мер защиты информации.

Ответственный за обеспечение безопасности ПДн осуществляет периодический контроль установки обновлений программного обеспечения, включая обновления программного обеспечения средств защиты информации, баз данных признаков вредоносных компьютерных программ (вирусов) средств антивирусной защиты, баз решающих правил систем обнаружения вторжений, баз признаков уязвимостей средств анализа защищенности, иных баз данных, необходимых для реализации функций безопасности средств защиты информации.

Ответственный за обеспечение безопасности ПДн осуществляет контроль соответствия настроек программного обеспечения и средств защиты информации параметрам настройки, приведенным в эксплуатационной документации на СЗПДн и средства защиты информации.

Ответственный за обеспечение безопасности ПДн осуществляет контроль состава технических средств, программного обеспечения и средств защиты информации, в том числе:

- осуществляет контроль соответствия состава технических средств, программного обеспечения и средств защиты информации приведенному в эксплуатационной документации с целью поддержания актуальной (установленной в соответствии с эксплуатационной документацией) конфигурации ИСПДн и принятие мер, направленных на устранение выявленных недостатков;
- осуществляет контроль состава технических средств, программного обеспечения и средств защиты информации на соответствие сведениям действующей (актуализированной) эксплуатационной документации и принятие мер, направленных на устранение выявленных недостатков;
- осуществляет контроль выполнения условий и сроков действия сертификатов соответствия на средства защиты информации и принятие мер, направленных на устранение выявленных недостатков;
- обеспечивает исключение (восстановление) из состава ИСПДн несанкционированно установленных (удаленных) технических средств, программного обеспечения и средств защиты информации.

Ответственный за обеспечение безопасности ПДн осуществляет контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в ИСПДн, в том числе:

- контроль правил генерации и смены паролей пользователей;
- контроль заведения и удаления учетных записей пользователей;
- контроль реализации правил разграничения доступом;
- контроль реализации полномочий пользователей;
- контроль наличия документов, подтверждающих разрешение изменений учетных записей пользователей, их параметров, правил разграничения доступом и полномочий пользователей;
- обеспечивает устранение нарушений, связанных с генерацией и сменой паролей пользователей, заведением и удалением учетных записей пользователей, реализацией правил разграничения доступом, установлением полномочий пользователей.

2.9 Обеспечение целостности информационной системы персональных данных и персональных данных

Ответственный за обеспечение безопасности ПДн осуществляет контроль выполнения процедур по обеспечению целостности ИСПДн и ПДн, выполняемых Администратором СЗПДн и Администратором ИСПДн.

2.10 Обеспечения доступности персональных данных

Ответственный за обеспечение безопасности ПДн осуществляет контроль выполнения процедур по обеспечению доступности ПДн, выполняемых Администратором СЗПДн и Администратором ИСПДн, в том числе согласует перечень информации (типов информации), подлежащей периодическому резервному копированию на резервные машинные носители информации.

2.11 Защита среды виртуализации

Ответственный за обеспечение безопасности ПДн осуществляет следующие функции по защите среды виртуализации:

- организует процесс настройки параметров средств защиты среды виртуализации;
- организует процесс своевременного обновления средств защиты среды виртуализации;
- проводит периодический контроль работы средств защиты среды виртуализации.

2.12 Защита технических средств

Ответственный за обеспечение безопасности ПДн осуществляет контроль выполнения процедур по защите технических средств, средств защиты информации, средств обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, в том числе:

- осуществляет контроль ведения Журнала учета посещений;
- осуществляет контроль размещения устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр.

2.13 Выявление инцидентов и реагирование на них

Ответственный за обеспечение безопасности ПДн осуществляет следующие функции по выявлению и реагированию на компьютерные инциденты:

- ведет единую электронную базу карточек компьютерных инцидентов. Карточка вносится в единую базу в срок, не превышающий 3-х рабочих дней со дня закрытия компьютерного инцидента;
- совместно с Администратором СЗПДн анализирует компьютерные инциденты для выработки мероприятий по их предотвращению;
- проводит мероприятия по ликвидации последствий компьютерных инцидентов в зависимости от результата анализа компьютерного инцидента;

- проводит служебное расследование по факту возникшего компьютерного инцидента;
- обеспечивает восстановление функционирования ИСПДн и СЗПДн.

2.14 Управление конфигурацией информационной системы персональных данных и системы защиты персональных данных

Ответственный за обеспечение безопасности ПДн осуществляет следующие функции по управлению конфигурацией ИСПДн и СЗПДн:

- согласовывает перечень изменений в конфигурации ИСПДн и СЗПДн, подготовленный Администраторами ИСПДн и СЗПДн;
- осуществляет контроль документирования информации (данных) об изменениях в конфигурации ИСПДн и СЗПДн.

3 Ответственность

Ответственный за обеспечение безопасности ПДн несет ответственность:

- за преднамеренные и непреднамеренные нарушения положений, предусмотренных настоящей Инструкцией, в пределах, определенных действующим законодательством Российской Федерации;
- за правонарушения, совершенные в процессе осуществления своей деятельности, в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации;
- за причинение материального ущерба – в пределах, определенных действующим трудовым и гражданским законодательством Российской Федерации.

4 Порядок пересмотра

Актуализация настоящей Инструкции осуществляется на плановой и внеплановой основе:

- плановая актуализация настоящей Инструкции должна осуществляться не реже одного раза в 3 года;
- внеплановая актуализация настоящей Инструкции может производиться по результатам контрольных мероприятий по выполнению требований законодательства Российской Федерации о ПДн, по результатам рассмотрения предложений Ответственного за организацию обработки ПДн, а также при изменении законодательства Российской Федерации о ПДн.

Приложение 1. Ежегодный план мероприятий по обеспечению безопасности персональных данных

№ п/п	Обязанности	Задачи	Периодичность	Лицо, ответственное за выполнение мероприятия
1	Обработка инцидентов безопасности ПДн	Обработка инцидентов безопасности ПДн	1 раз/ 1 мес.	Ответственный за обеспечение безопасности ПДн
		Ведение статистики инцидентов безопасности ПДн и отслеживание динамики по данной статистике	1 раз/ 3 мес.	Ответственный за обеспечение безопасности ПДн
2	Контроль за принимаемыми мерами по обеспечению безопасности ПДн и уровня защищенности ИСПДн	Контроль этапов жизненного цикла и учет СЗПДн	1 раз/ 1 год.	Ответственный за обеспечение безопасности ПДн
		Оценка эффективности реализованных в рамках СЗПДн мер	1 раз/ 1 год.	Ответственный за обеспечение безопасности ПДн
3	Контроль и поддержание штатной работы СЗПДн	Управление учетными данными (в т.ч. ключевой информацией) и правами доступа к ПДн	1 раз/ 1 мес.	Ответственный за обеспечение безопасности ПДн
		Тестирование работоспособности СЗПДн	1 раз/ 6 мес.	Ответственный за обеспечение безопасности ПДн
		Контроль организации приостановки работы с ПДн в случае нарушений функционирования СЗПДн	1 раз/ 6 мес.	Ответственный за обеспечение безопасности ПДн
		Контроль восстановления штатной работы СЗПДн после нарушения штатной работы СЗПДн	1 раз/ 6 мес.	Ответственный за обеспечение безопасности ПДн
		Контроль и учет изменений в СЗПДн	1 раз/ 1 год.	Ответственный за обеспечение безопасности ПДн
		Ведение статистики нарушений безопасности ПДн и отслеживание динамики по данной статистике	1 раз/ 3 мес.	Ответственный за обеспечение безопасности ПДн

Приложение 2. Отчет о выполнении ежегодного плана мероприятий по обеспечению безопасности персональных данных

ОТЧЕТ
о выполнении ежегодного плана мероприятий по обеспечению безопасности персональных данных за 2024 г.

Наников Каспар Александрович, выполняя функции лица, ответственного за обеспечение безопасности персональных данных в ООО «Доктор Наников» в соответствии с «Ежегодным планом мероприятий по обеспечению безопасности персональных данных на 2021 год», утвержденным Приказом №_____ от __.__.____ и на основании документа «Доктор Наников». Инструкция лица, ответственного за обеспечение безопасности персональных данных» составил настоящий Отчет:

№ п/п	Наименование мероприятия	Ответственный за реализацию мероприятия	Результат выполнения мероприятия
1	Обработка инцидентов безопасности ПДн	Наников К.А.	Инциденты НЕ выявлено
2	Контроль этапов жизненного цикла и учет СЗПДн	Наников К.А.	Инциденты НЕ выявлено
3	проведена проверка компонентов ИСПДн (автоматизированных рабочих мест, серверов, других средств вычислительной техники) на наличие вредоносных компьютерных программ (вирусов) с установленной периодичностью	Наников К.А.	Инциденты НЕ выявлено
4	Проведена работа по тестированию работоспособности СЗПДн	Наников К.А.	Инциденты НЕ выявлено

_____ _____

(должность) *(Фамилия И.О.)*