ООО МИП
«ДНК-ДИАГНОСТИКА»

Тел.: 8 (928) 891-34-78
Email: petimat09@gmail.com
dnk-labs.ru

ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ МАЛОЕ ИННОВАЦИОННОЕ ПРЕДПРИЯТИЕ «ДНК-ДИАГНОСТИКА»

ПРИКАЗ

№ 07 **Грозный** «12» августа 2026 г.

О реализации мер по защите персональных данных в информационных системах персональных данных

В целях обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных ООО МИП «ДНК-ДИАГНОСТИКА» и выполнения требований приказа Федеральной службы по техническому и экспортному контролю от 18 февраля 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», п р и к а з ы в а ю :

1. Утвердить:

– Регламент идентификации и аутентификации в информационных системах персональных данных (ПРИЛОЖЕНИЕ № 1);

– Регламент управления доступом в информационных системах персональных данных (ПРИЛОЖЕНИЕ № 2);

– Регламент регистрации событий безопасности в информационных системах персональных данных (ПРИЛОЖЕНИЕ № 3);

– Регламент антивирусной защиты в информационных системах персональных данных (ПРИЛОЖЕНИЕ № 4);

– Регламент контроля (анализа) защищенности в информационных системах персональных данных (ПРИЛОЖЕНИЕ № 5);

– Регламент защиты технических средств информационных систем персональных данных (ПРИЛОЖЕНИЕ № 6);

– Регламент защиты информационных систем персональных данных, их средств, систем связи и передачи данных (ПРИЛОЖЕНИЕ № 7).

2. Контроль за исполнением настоящего приказа возложить на ответственного за обеспечение безопасности персональных данных.

Генеральный директор П.М. Джамбетова

ПРИЛОЖЕНИЕ № 1
к приказу ООО МИП «ДНК-ДИАГНОСТИКА»
от «10» 08 2026 г. № 07

Регламент идентификации и аутентификации
в информационных системах персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий Регламент разработан с целью установления ООО МИП «ДНК-ДИАГНОСТИКА» (далее – ООО МИП «ДНК-ДИАГНОСТИКА») общих правил, требований и процедур идентификации и аутентификации при разработке, внедрении и совершенствовании правил, механизмов и технологий управления доступом к информационным системам персональных данных ООО МИП «ДНК-ДИАГНОСТИКА» (далее – ИСПДн).

1.2. Настоящий документ не применяется в отношении ИСПДн, включенных в перечень объектов, подлежащих защите в ООО МИП «ДНК-ДИАГНОСТИКА» в соответствии с требованиями приказа Федеральной службы по техническому и экспортному контролю от 11 апреля 2025 г. № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений», утвержденный локальным актом ООО МИП «ДНК-ДИАГНОСТИКА».

1.3. Меры защиты персональных данных, реализация которых описана в рамках настоящего Регламента, представлены в таблице 1.

Таблица 1 – Меры защиты персональных данных, реализация которых описана в рамках настоящего Регламента

Условное обозначение и номер меры	Меры защиты персональных данных
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации
ИАФ.5	Защита обратной связи при вводе аутентификационной информации
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)

1.4. Состав мер определен на основании уровня защищенности персональных данных и структурно-функциональных характеристик ИСПДн.

1.5. Регламент предназначен для специалистов по защите персональных данных.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. Аутентификационная информация (информация аутентификации) – информация, используемая для установления подлинности (верификации) субъекта доступа в информационной системе персональных данных.

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

2.3. Идентификатор доступа (идентификатор) – уникальный признак субъекта или объекта доступа (представление (строка символов), однозначно идентифицирующее субъект и (или) объект доступа в информационной системе персональных данных).

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

2.5. Несанкционированный доступ (НСД) – доступ к информации или к ресурсам информационной системы персональных данных, осуществляемый с нарушением установленных прав и (или) правил доступа.

2.6. Объект доступа – единица информационного ресурса информационной системы персональных данных (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.

2.7. Пароль – идентификатор субъекта доступа, который является его (субъекта) секретом.

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

2.9. Специалист по защите персональных данных (Ответственный) – сотрудник ООО МИП «ДНК-ДИАГНОСТИКА», выполняющий непосредственные функции по защите персональных данных, в том числе по управлению системой защиты персональных данных, по управлению конфигурацией ИСПДн и ее системой защиты, по выявлению компьютерных инцидентов и реагированию на них.

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

2.11. Управление доступом – ограничение и контроль доступа субъектов доступа к объектам доступа в информационной системе персональных данных в соответствии с установленными правилами разграничения доступа.

3. ЦЕЛЬ И ЗАДАЧИ РЕАЛИЗАЦИИ ПРОЦЕССОВ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ

3.1. Целью реализации процессов идентификации и аутентификации в ИСПДн является распознавание субъекта доступа с необходимой уверенностью в том, что он является именно тем, за кого себя выдает.

3.2. Реализация процессов идентификации и аутентификации достигается решением следующих задач:

– формированием и регистрацией информации о субъекте (объекте) доступа, а также присвоением субъекту (объекту) доступа идентификатора доступа и его регистрацией в перечне присвоенных идентификаторов;

– хранением и поддержанием в актуальном состоянии (обновлением) идентификационной и аутентификационной информации субъекта (объекта) доступа в соответствии с установленными правилами;

– опознаванием субъекта доступа, запросившего доступ к объекту доступа, по предъявленному идентификатору;

– аутентификацией, включающей проверку подлинности субъекта (объекта) доступа и принадлежности ему предъявленных идентификатора и аутентификационной информации.

4. ОБЩИЕ ТРЕБОВАНИЯ

4.1. Процессы идентификации и аутентификации в ИСПДн подлежат реализации при управлении доступом к следующим частям ИСПДн:

– автоматизированные рабочие места;

– интерфейс управления микропрограммным обеспечением BIOS/UEFI;

– прикладное программное обеспечение.

4.2. Идентификация и аутентификация должна осуществляться в отношении:

– пользователей ИСПДн ООО МИП «ДНК-ДИАГНОСТИКА», являющихся сотрудниками ООО МИП «ДНК-ДИАГНОСТИКА»;

– пользователей ИСПДн ООО МИП «ДНК-ДИАГНОСТИКА», не являющихся сотрудниками ООО МИП «ДНК-ДИАГНОСТИКА»;

– процессов, запускаемых от имени пользователей;

– процессов, запускаемых от имени системных учетных записей.

4.3. Процессы, запускаемые от имени пользователя, должны однозначно сопоставляться с идентификатором пользователя.

4.4. В качестве идентификатора пользователя при доступе должен использоваться набор буквенно-цифровых символов (логин).

4.5. В ИСПДн должен использоваться механизм аутентификации на основе пароля.

5. ТРЕБОВАНИЯ К СОЗДАНИЮ, ПРИСВОЕНИЮ И УНИЧТОЖЕНИЮ ИДЕНТИФИКАТОРОВ

5.1. Создание, присвоение и уничтожение идентификатора должно осуществляться Ответственным.

5.2. Ответственный обеспечивает однозначную идентификацию пользователя и (или) устройства путем формирования уникального персонального идентификатора.

5.3. Повторное использование идентификатора пользователя не допускается в течение одного года со дня уничтожения.

5.4. Блокирование идентификатора пользователя должно осуществляться после 30 дней неиспользования.

5.5. Уничтожение идентификатора пользователя, являющегося сотрудником ООО МИП «ДНК-ДИАГНОСТИКА», производится при прекращении полномочий (увольнении) сотрудника.

5.6. Уничтожение идентификатора пользователя, не являющегося сотрудником ООО МИП «ДНК-ДИАГНОСТИКА», производится в случаях установленных требованиями по подключению внешних пользователей.

6. УПРАВЛЕНИЕ СРЕДСТВАМИ АУТЕНТИФИКАЦИИ

6.1. Генерация (назначение) паролей

6.1.1. Генерация и выдача начальной аутентификационной информации (пароля) пользователю осуществляется Ответственным.

6.1.2. Средства, реализующие идентификацию и аутентификацию пользователей, должны обеспечивать настройку характеристик паролей, представленных в таблице 2.

Таблица 2 – Требования к настройкам характеристик паролей

№ п/п	Характеристика	Значение	Примечание
1.	Минимальная длина пароля	10	Минимальное количество знаков, которое должно содержаться в пароле
2.	Соответствие требованиям к сложности пароля	Включено	Не содержать имени учетной записи пользователя или частей полного имени пользователя длиной более двух рядом стоящих знаков. Содержать знаки минимум трех из четырех перечисленных ниже категорий: - латинские заглавные буквы (от A до Z); - латинские строчные буквы (от a до z); - цифры (от 0 до 9) - специальные символы (например, !, $, #, %).
3.	Максимальный срок действия пароля	6 месяцев	Период времени (в днях), в течение которого можно использовать пароль, пока система не потребует от пользователя сменить его
4.	Максимальное количество неуспешных попыток аутентификации	5	Максимальное количество неуспешных попыток ввода неправильного пароля до блокировки

№ п/п	Характеристика	Значение	Примечание
5.	Минимальное количество измененных символов при создании новых паролей	5	Минимальное количество символов, которые требуется изменить при создании нового пароля по отношению к старому паролю
6.	Журнал паролей	4	При создании новых паролей запрещается использование пользователями определенного количества последних использованных паролей

6.2. Хранение паролей

6.2.1. Средства, реализующие идентификацию и аутентификацию, должны обеспечивать защиту аутентификационной информации от несанкционированного доступа к ней и ее модификации.

6.3. Порядок смены аутентификационной информации

6.3.1. Смена паролей производится на плановой и внеплановой основе.

6.3.2. Плановая смена паролей осуществляется:

– при истечении максимального срока действия пароля;

– при поставках нового оборудования с предустановленной аутентификационной информацией (средств аутентификации), при внедрении системы защиты персональных данных ИСПДн;

– после внедрения системы защиты персональных данных ИСПДн.

6.3.3. Внеплановая смена паролей осуществляется в следующих случаях:

– компрометация или подозрение в компрометации пароля;

– прекращение полномочий (увольнение, изменение обязанностей и другие обстоятельства) сотрудников ООО МИП «ДНК-ДИАГНОСТИКА»;

– по указанию Ответственного.

7. ЗАЩИТА ОБРАТНОЙ СВЯЗИ ПРИ ВВОДЕ АУТЕНТИФИКАЦИОННОЙ ИНФОРМАЦИИ

7.1. Средства, реализующие идентификацию и аутентификацию, должны обеспечивать исключение отображения для пользователя действительного значения аутентификационной информации и (или) количества вводимых пользователем символов аутентификационной информации. Вводимые символы пароля должны отображаться условными знаками: «*», «●» или иными знаками.

8. ДЕЙСТВИЯ ПРИ КОМПРОМЕТАЦИИ АУТЕНТИФИКАЦИОННОЙ ИНФОРМАЦИИ

8.1. Компрометация действующих паролей является внештатной ситуацией.

8.2. Скомпрометированные пароли и связанные с ними персональные идентификаторы (логины) пользователей должны блокироваться при обнаружении факта компрометации.

9. ОТВЕТСТВЕННОСТЬ

9.1. Ответственный несет персональную ответственность за ненадлежащее исполнение или неисполнение положений настоящего Регламента.

ПРИЛОЖЕНИЕ № 2
к приказу ООО МИП «ДНК-ДИАГНОСТИКА»
от «10» 08 2026 г. № 07

Регламент управления доступом
в информационных системах персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий Регламент разработан с целью установления ООО МИП «ДНК-ДИАГНОСТИКА» (далее – ООО МИП «ДНК-ДИАГНОСТИКА») общих правил, требований и процедур управления доступом в информационных системах персональных данных ООО МИП «ДНК-ДИАГНОСТИКА» (далее – ИСПДн).

1.2. Настоящий документ не применяется в отношении ИСПДн, включенных в перечень объектов, подлежащих защите в ООО МИП «ДНК-ДИАГНОСТИКА» в соответствии с требованиями приказа Федеральной службы по техническому и экспортному контролю от 11 апреля 2025 г. № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений», утвержденный локальным актом ООО МИП «ДНК-ДИАГНОСТИКА».

1.3. Меры защиты персональных данных, реализация которых описана в рамках настоящего Регламента, представлены в таблице 1.

Таблица 1 – Меры защиты персональных данных, реализация которых описана в рамках настоящего Регламента

Условное обозначение и номер меры	Меры защиты персональных данных
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)

1.4. Состав мер определен на основании уровня защищенности персональных данных и структурно-функциональных характеристик ИСПДн.

1.5. Правила и процедуры управления информационными потоками между устройствами, сегментами ИСПДн, а также между ИСПДн описаны в рамках Регламента защиты информационной системы персональных данных, ее средств, систем связи и передачи данных.

1.6. Регламент предназначен для специалистов по защите персональных данных.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. Аутентификационная информация (информация аутентификации) – информация, используемая для установления подлинности (верификации) субъекта доступа в информационной системе персональных данных.

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

2.3. Идентификатор доступа (идентификатор) – уникальный признак субъекта или объекта доступа (представление (строка символов), однозначно идентифицирующее субъект и (или) объект доступа в информационной системе персональных данных).

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

2.5. Несанкционированный доступ – доступ к информации или к ресурсам информационной системы персональных данных, осуществляемый с нарушением установленных прав и (или) правил доступа.

2.6. Объект доступа – единица информационного ресурса информационной системы персональных данных (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.

2.7. Пароль – идентификатор субъекта доступа, который является его (субъекта) секретом.

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

2.9. Специалист по защите персональных данных (Ответственный) – сотрудник ООО МИП «ДНК-ДИАГНОСТИКА», выполняющий непосредственные функции по защите персональных данных, в том числе по управлению системой защиты персональных данных, по управлению конфигурацией ИСПДн и ее системой защиты, по выявлению компьютерных инцидентов и реагированию на них.

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

2.11. Управление доступом – ограничение и контроль доступа субъектов доступа к объектам доступа в информационной системе персональных данных в соответствии с установленными правилами разграничения доступа.

3. ТРЕБОВАНИЯ К СИСТЕМЕ УПРАВЛЕНИЯ ДОСТУПОМ

3.1. Управление доступом должно быть направлено на недопущение несанкционированного доступа к объектам доступа со стороны субъектов доступа, для которых запрашиваемый доступ не разрешен.

3.2. Доступ пользователей к информационным ресурсам ИСПДн предоставляется Ответственным, исходя из следующих условий:

– доступ необходим для выполнения пользователем должностных обязанностей в соответствии со своей должностной инструкцией;

– доступ необходим для выполнения пользователем обязанностей другого пользователя по поручению (в виде служебной записки) руководителя соответствующего подразделения;

– доступ необходим для выполнения пользователем обязанностей другого пользователя по письменному указанию Главного врача ООО МИП «ДНК-ДИАГНОСТИКА»;

– доступ необходим для выполнения пользователем работ по письменному указанию Главного врача ООО МИП «ДНК-ДИАГНОСТИКА»;

– доступ необходим для выполнения пользователем работ в ходе реализации контрактов, договоров, заключенных с ООО МИП «ДНК-ДИАГНОСТИКА» (для сотрудников «сторонних» организаций).

3.3. Физический доступ пользователей к техническим средствам ИСПДн осуществляется в соответствии с установленным в ООО МИП «ДНК-ДИАГНОСТИКА» порядком доступа сотрудников ООО МИП «ДНК-ДИАГНОСТИКА» в помещения, в которых осуществляется обработка персональных данных и (или) размещены ИСПДн.

3.4. Пользователи допускаются к информационному ресурсу на основании заявок, в соответствии с установленным порядком, представленным в пункте 7 настоящего Регламента.

3.5. Допуск к информационному ресурсу предоставляется исключительно после ознакомления с локальными актами ООО МИП «ДНК-ДИАГНОСТИКА» и прохождения обучения (инструктажа) по вопросам обеспечения информационной безопасности.

3.6. Доступ пользователей к программным функциям технических средств ИСПДн должен осуществляться в соответствии с правилами разграничения доступа и с использованием учетных записей при успешном прохождении процедуры идентификации и аутентификации.

3.7. Средства, реализующие управление доступом, должны обеспечивать:

3.7.1. Ограничение неуспешных попыток входа (доступа) в количестве 5 раз за период времени в 5, а также обеспечивать блокирование устройства, с которого предпринимаются попытки доступа, и (или) учетной записи пользователя при превышении пользователем установленного ограничения.

4. МЕТОДЫ УПРАВЛЕНИЯ ДОСТУПОМ

4.1. В ИСПДн должен быть реализован ролевой метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе ролей субъектов доступа.

4.2. Список ролей определяется в отношении каждой ИСПДн с учетом особенностей функционирования ИСПДн и должностных обязанностей (функций) сотрудников ООО МИП «ДНК-ДИАГНОСТИКА» при эксплуатации ИСПДн и ее системы защиты персональных данных.

4.3. При этом в обязательном порядке должны быть выделены роли, осуществляющие функции по:

– управлению функциями безопасности и средствами защиты информации;

– управлению (администрированию) базами данных, прикладным программным обеспечением, телекоммуникационным оборудованием, рабочими станциями и серверами;

– обработке персональных данных;

– обслуживанию помещений, в которых размещаются технические средства ИСПДн (уборке, обслуживанию и ремонту инженерных систем и т.п.);

– обслуживанию, ремонту, настройке и контролю работы обеспечивающих функционирование ИСПДн технических средств и систем.

4.4. Каждой роли должны быть определены минимально необходимые права и привилегии, необходимые для обеспечения функционирования ИСПДн.

4.5. Каждому сотруднику при предоставлении доступа в ИСПДн должна быть определена одна из определенных ролей.

4.6. Сведения о ролях и их полномочиях детализируются в рамках локального акта ООО МИП «ДНК-ДИАГНОСТИКА», утверждающего систему разграничения доступа.

4.7. Полномочия пользователей могут уточняться Ответственным, исходя из должностных обязанностей (функций), возложенных на пользователя.

5. ИДЕНТИФИКАЦИЯ ОБЪЕКТОВ ДОСТУПА

5.1. Ответственный, исходя из должностных обязанностей (функций), возложенных на пользователей, должен идентифицировать (определить) объекты доступа, в отношении которых реализуется управление доступом.

5.2. В качестве объектов доступа следует рассматривать:

5.2.1. Из числа технических средств:

– автоматизированные рабочие места пользователей;

– серверное оборудование;

– оборудование, обеспечивающее функционирование ИСПДн (сервер синхронизации времени, оборудование локальной вычислительной сети, источники бесперебойного питания и т.п.);

5.2.2. Из числа объектов файловой системы:

– файлы и каталоги системного программного обеспечения;

– пользовательский каталог;

– запускаемые и исполняемые модули прикладного программного обеспечения;

– конфигурационные файлы прикладного программного обеспечения;

– запускаемые и исполняемые модули программного обеспечения средств защиты информации;

– конфигурационные файлы программного обеспечения средств защиты информации;

– файлы журналов регистрации событий безопасности;

– контейнеры (файлы), в которых хранится аутентификационная информация (или ее образы) пользователей.

5.3. Подробный состав объектов доступа в отношении каждой ИСПДн детализируется в рамках локального акта ООО МИП «ДНК-ДИАГНОСТИКА», утверждающего систему разграничения доступа.

6. ТИПЫ ДОСТУПА

6.1. В рамках управления доступа должны рассматриваться следующие типы доступа:

– физический доступ к техническим средствам;

– доступ к объектам файловой системы.

6.2. В качестве разрешенных к выполнению пользователю или запускаемому от его имени процессу при доступе к объектам файловой системы должны рассматриваться следующие операции:

– чтение (r);

– запись (w);

– удаление (d);

– выполнение (e).

7. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ ДОСТУПА

7.1. Формирование запроса

7.1.1. Предоставление доступа к ИСПДн осуществляется на основании заявок. Формирование заявки осуществляет либо сам сотрудник, которому необходимо предоставить доступ, либо руководитель сотрудника. Работа с заявками осуществляется в соответствии с установленным ООО МИП «ДНК-ДИАГНОСТИКА» порядком. При этом в заявке в обязательном порядке должен быть указан информационный ресурс, к которому необходим доступ, уровень доступа к нему, период, на который требуется предоставление доступа, и обоснование необходимости предоставления доступа.

7.1.2. Все заявки на предоставление доступа должны храниться Ответственным и могут впоследствии использоваться для:

– контроля правомерности предоставления доступа при разборе инцидентов информационной безопасности и конфликтных ситуаций;

– проверки корректности предоставления доступа к информационным ресурсам.

7.2. Согласование предоставления доступа

7.2.1. Все сформированные заявки на доступ подлежат согласованию.

7.2.2. Согласование производится с:

– руководителем подразделения (если заявка сформирована сотрудником

подразделения);

– лицами, согласование доступа с которыми предусмотрено в рамках локальных актов ООО МИП «ДНК-ДИАГНОСТИКА».

7.2.3. Ответственный в процессе согласования должен выполнить:

– верификацию пользователя (проверку личности пользователя, его должностных (функциональных) обязанностей);

– оценку обоснованности доступа к информационному ресурсу и запрашиваемого уровня доступа.

7.3. Ознакомление с документацией

7.3.1. Перед предоставлением доступа в обязательном порядке следует ознакомить лиц, которым предоставляется доступ, с локальными актами ООО МИП «ДНК-ДИАГНОСТИКА» в области обеспечения безопасности персональных данных.

7.3.2. Ознакомление должно производиться сотрудником ООО МИП «ДНК-ДИАГНОСТИКА», на которого возложены обязанности (функции) по обеспечению безопасности персональных данных. Факты ознакомления должны фиксироваться в листах ознакомления и (или) соответствующих журналах.

7.4. Предоставление доступа

7.4.1. Процесс предоставления доступа включает:

– создание Ответственным учетной записи пользователя. Формирование реквизитов учетной записи (идентификатора и начальной аутентификационной информации (пароля)) осуществляется в соответствии с Регламентом идентификации и аутентификации в информационных системах персональных данных;

– настройку Ответственным средств защиты информации;

– настройку Ответственным программного обеспечения автоматизированного рабочего места и (или) сервера.

7.4.2. Предоставление доступа пользователю должно осуществляться в течение 2-х рабочих дней со дня согласования заявки.

7.5. Дополнительные сведения

7.5.1. Доступ пользователям к информационным ресурсам может быть предоставлен без оформления заявки в случае письменного указания руководства ООО МИП «ДНК-ДИАГНОСТИКА».

7.5.2. Доступ сотрудников федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, иных государственных органов, органов прокуратуры и других правоохранительных органов, осуществляющих контрольные мероприятия и обладающих соответствующими полномочиями, осуществляется в соответствии с порядком, установленным законодательством Российской Федерации.

8. ПОРЯДОК ПРЕКРАЩЕНИЯ ДОСТУПА

8.1. Доступ к ИСПДн должен быть незамедлительно прекращен:

– при истечении срока предоставления доступа;

– при прекращении полномочий пользователя;

– по указанию руководства ООО МИП «ДНК-ДИАГНОСТИКА»;

– по указанию сотрудника ООО МИП «ДНК-ДИАГНОСТИКА», на которого возложены обязанности (функции) по обеспечению безопасности персональных данных;

– в случаях обнаружения факта компрометации учетной записи пользователя.

9. ЗАЩИТА УДАЛЕННОГО ДОСТУПА

9.1. Процесс предоставления защищенного удаленного доступа включает:

– установление видов доступа, разрешенных для удаленного доступа к объектам доступа ИСПДн в соответствии с установленными методами, типами и правилами разграничения доступа;

– ограничение на использование удаленного доступа в соответствии с задачами (функциями) ИСПДн, для решения которых такой доступ необходим, и предоставление удаленного доступа для каждого разрешенного вида удаленного доступа;

– предоставление удаленного доступа только тем пользователям, которым он необходим для выполнения установленных должностных обязанностей (функций);

– мониторинг и контроль удаленного доступа на предмет выявления несанкционированного удаленного доступа к объектам доступа ИСПДн;

– контроль удаленного доступа пользователей (процессов запускаемых от имени пользователей) к объектам доступа ИСПДн до начала информационного взаимодействия с ИСПДн.

10. УПРАВЛЕНИЕ ИНФОРМАЦИОННЫМИ ПОТОКАМИ МЕЖДУ УСТРОЙСТВАМИ, СЕГМЕНТАМИ ИСПДН, А ТАКЖЕ МЕЖДУ ИСПДН

10.1. В ИСПДн должно осуществляться управление информационными потоками при передаче информации между устройствами, сегментами в рамках ИСПДн, включающее:

– фильтрацию информационных потоков в соответствии с правилами управления потоками;

– разрешение передачи информации в ИСПДн только по маршруту, установленному ООО МИП «ДНК-ДИАГНОСТИКА»;

– изменение (перенаправление) маршрута передачи информации в случаях, установленных ООО МИП «ДНК-ДИАГНОСТИКА»;

– запись во временное хранилище информации для анализа и принятия решения о возможности ее дальнейшей передачи в случаях, установленных ООО МИП «ДНК-ДИАГНОСТИКА».

10.2. Управление информационными потоками должно обеспечивать разрешенный (установленный ООО МИП «ДНК-ДИАГНОСТИКА») маршрут прохождения информации между пользователями, устройствами, сегментами в рамках ИСПДн, а также между ИСПДн или при взаимодействии с сетью «Интернет» (или другими информационно-телекоммуникационными сетями международного информационного обмена) на основе правил управления информационными потоками, включающих контроль конфигурации ИСПДн, источника и получателя передаваемой информации, структуры передаваемой информации, характеристик информационных потоков и (или) канала связи (без анализа

содержания информации). Управление информационными потоками должно блокировать передачу защищаемой информации через сеть «Интернет» (или другие информационно-телекоммуникационные сети международного информационного обмена) по незащищенным линиям связи, сетевые запросы и трафик, несанкционированно исходящие из ИСПДн и (или) входящие в ИСПДн.

11. УПРАВЛЕНИЕ ВЗАИМОДЕЙСТВИЕМ С ВНЕШНИМИ ИНФОРМАЦИОННЫМИ СИСТЕМАМИ

11.1. Процесс обеспечения управления взаимодействием с внешними информационными системами включает:

– предоставление доступа к ИСПДн только авторизованным (уполномоченным) пользователям в соответствии с установленными методами, типами и правилами разграничения доступа;

– определение типов прикладного программного обеспечения ИСПДн, к которым разрешен доступ авторизованным (уполномоченным) пользователям из внешних информационных систем;

– определение системных учетных записей, используемых в рамках данного взаимодействия;

– определение порядка предоставления доступа к ИСПДн авторизованными (уполномоченным) пользователями из внешних информационных систем;

– определение порядка обработки, хранения и передачи персональных данных с использованием внешних информационных систем.

12. ОТВЕТСТВЕННОСТЬ

12.1. Ответственный несет персональную ответственность за ненадлежащее исполнение или неисполнение положений настоящего Регламента.

ПРИЛОЖЕНИЕ № 3
к приказу ООО МИП «ДНК-ДИАГНОСТИКА»
от «10» 08 2026 г. № 07

Регламент регистрации событий безопасности
в информационных системах персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий Регламент разработан с целью установления ООО МИП «ДНК-ДИАГНОСТИКА»(далее – ООО МИП «ДНК-ДИАГНОСТИКА») общих правил, требований и процедур регистрации событий безопасности в информационных системах персональных данных ООО МИП «ДНК-ДИАГНОСТИКА» (далее – ИСПДн).

1.2. Настоящий документ не применяется в отношении ИСПДн, включенных в перечень объектов, подлежащих защите в ООО МИП «ДНК-ДИАГНОСТИКА» в соответствии с требованиями приказа Федеральной службы по техническому и экспортному контролю от 11 апреля 2025 г. № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений», утвержденный локальным актом ООО МИП «ДНК-ДИАГНОСТИКА».

1.3. Меры защиты персональных данных, реализация которых описана в рамках настоящего Регламента, представлены в таблице 1.

Таблица 1 – Меры защиты персональных данных, реализация которых описана в рамках настоящего Регламента

Условное обозначение и номер меры	Меры защиты персональных данных
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения
РСБ.7	Защита информации о событиях безопасности

1.4. Состав мер определен на основании уровня защищенности персональных данных и структурно-функциональных характеристик ИСПДн.

1.5. Регламент предназначен для специалистов по защите персональных данных.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. Специалист по защите персональных данных (Ответственный) – сотрудник ООО МИП «ДНК-ДИАГНОСТИКА», выполняющий непосредственные функции по защите персональных данных, в том числе по управлению системой защиты персональных данных,

по управлению конфигурацией ИСПДн и ее системой защиты, по выявлению компьютерных инцидентов и реагированию на них.

3. РЕГИСТРАЦИЯ И МОНИТОРИНГ СОБЫТИЙ БЕЗОПАСНОСТИ

3.1. Общие положения

3.1.1. Сбор, запись и хранение информации о событиях безопасности осуществляется с целью выявления инцидентов информационной безопасности и реагирования на них.

3.1.2. Сбор, запись и хранение событий безопасности должны осуществляться на всех компонентах ИСПДн (рабочие места пользователей, серверы, телекоммуникационное оборудование). Требования к составу и содержанию информации о событиях безопасности представлены в пункте 3.2 настоящего Регламента.

3.1.3. Доступ к функциям управления механизмами регистрации (аудита) должен быть доступен только Ответственному.

3.1.4. Доступ к записям аудита должен быть доступен только Ответственному.

3.1.5. Защита информации о событиях безопасности (записях регистрации (аудита)) должна обеспечиваться применением мер защиты персональных данных от неправомерного доступа, уничтожения или модифицирования. В том числе должна обеспечиваться защита средств ведения регистрации (аудита) и настроек механизмов регистрации событий.

3.1.6. Зарегистрированные события безопасности должны храниться не менее чем 1 год.

3.2. Требования к составу регистрируемых событий безопасности

3.2.1. Регистрации подлежат события, представленные в таблице 2.

Таблица 2 – Состав и содержание информации о событиях безопасности

№ п/п	Событие	Минимальный состав информации о событии
1.	Вход (выход), а также попытки входа субъектов доступа (пользователей) в операционную систему	Дата и время входа (выхода) в операционную систему (из операционной системы); Результат попытки входа (успешный или неуспешный); Идентификатор (логин), предъявленный при попытке доступа
2.	Изменение полномочий субъектов доступа и статуса объектов доступа, в том числе создание, модификация, удаление учетных записей	Дата и время создания или модификации или удаления учетной записи или статуса объекта доступа; Результат операции (успешный или неуспешный); Идентификатор (логин) субъекта доступа (пользователя), выполнившего операцию (создание или модификация или удаление учетной записи / изменении статуса объекта доступа)
3.	Подключение съемных машинных носителей информации и вывод информации на носители информации	Дата и время подключения съемного машинного носителя информации и вывода информации на носители информации; Логическое имя (имя устройства и (или) ID) съемного машинного носителя информации; Идентификатор субъекта доступа, осуществляющего вывод информации на носитель информации
4.	Запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации	Дата и время запуска; Имя (идентификатор) программы (процесса, задания); Идентификатор субъекта доступа (пользователя, устройства),

№ п/п	Событие	Минимальный состав информации о событии
		запросившего программу (процесс, задание); Результат запуска (успешный, неуспешный)
5.	Попытки доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам	Дата и время попытки доступа к защищаемому файлу; Результат попытки доступа (успешный, неуспешный); Идентификатор субъекта доступа (пользователя, устройства); Спецификация защищаемого файла (логическое имя, тип)
6.	Попытки доступа программных средств к защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, записям, полям записей)	Дата и время попытки доступа к защищаемому объекту; Результата попытки доступа (успешный, неуспешный); Идентификатор субъекта доступа (пользователя, устройства); Спецификацию защищаемого объекта доступа (логическое имя (номер))
7.	Попытка удаленного доступа	Дата и время попытки удаленного доступа; Результат попытки удаленного доступа (успешный, неуспешный); Идентификатор субъекта доступа (пользователя, устройства); Используемый протокол доступа; Используемый интерфейс доступа

4. ОТВЕТСТВЕННОСТЬ

4.1. Ответственный несет персональную ответственность за ненадлежащее исполнение или неисполнение положений настоящего Регламента.

ПРИЛОЖЕНИЕ № 4
к приказу ООО МИП «ДНК-ДИАГНОСТИКА»
от «10» 08 2026 г. № 07

Регламент антивирусной защиты
в информационных системах персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий Регламент разработан с целью установления ООО МИП «ДНК-ДИАГНОСТИКА» (далее – ООО МИП «ДНК-ДИАГНОСТИКА») порядка организации защиты от угроз, связанных с внедрением вредоносных компьютерных программ (вирусов) из информационно-телекоммуникационных сетей, в том числе сетей международного информационного обмена (сетей связи общего пользования), и съемных машинных носителей персональных данных в информационных системах персональных данных ООО МИП «ДНК-ДИАГНОСТИКА» (далее – ИСПДн).

1.2. Настоящий документ не применяется в отношении ИСПДн, включенных в перечень объектов, подлежащих защите в ООО МИП «ДНК-ДИАГНОСТИКА» в соответствии с требованиями приказа Федеральной службы по техническому и экспортному контролю от 11 апреля 2025 г. № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений», утвержденный локальным актом ООО МИП «ДНК-ДИАГНОСТИКА».

1.3. Меры защиты персональных данных, реализация которых описана в рамках настоящего Регламента, представлены в таблице 1.

Таблица 1 – Меры защиты персональных данных, реализация которых описана в рамках настоящего Регламента

Условное обозначение и номер меры	Меры защиты персональных данных
АВЗ.1	Реализация антивирусной защиты
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)

1.4. Состав мер определен на основании уровня защищенности персональных данных и структурно-функциональных характеристик ИСПДн.

1.5. Регламент предназначен для специалистов по защите персональных данных.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. Антивирусная защита – защита информации и компонентов информационной системы персональных данных от вредоносных компьютерных программ (вирусов) (обнаружение вредоносных компьютерных программ (вирусов), блокирование, изолирование «зараженных» объектов, удаление вредоносных компьютерных программ (вирусов) из «зараженных» объектов).

2.2. Безопасность информации – состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность.

2.3. Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на информацию или ресурсы информационной системы персональных данных.

2.4. Компьютерный вирус – программа, способная создавать свои копии (необязательно совпадающие с оригиналом) и внедрять их в файлы, системные области компьютера, компьютерных сетей, а также осуществлять иные деструктивные действия. При этом копии сохраняют способность дальнейшего распространения. Компьютерный вирус относится к вредоносным программам.

2.5. Сигнатура – характерные признаки компьютерной вредоносной программы (вируса), используемые для ее обнаружения.

2.6. Специалист по защите персональных данных (Ответственный) – сотрудник ООО МИП «ДНК-ДИАГНОСТИКА», выполняющий непосредственные функции по защите персональных данных, в том числе по управлению системой защиты персональных данных, по управлению конфигурацией ИСПДн и ее системой защиты, по выявлению компьютерных инцидентов и реагированию на них.

2.7. Угроза безопасности информации – совокупность условий и факторов, определяющих потенциальную или реально существующую опасность нарушения безопасности информации.

2.8. Управление доступом – ограничение и контроль доступа субъектов доступа к объектам доступа в информационной системе персональных данных в соответствии с установленными правилами разграничения доступа.

3. ТРЕБОВАНИЯ К АНТИВИРУСНОЙ ЗАЩИТЕ

3.1. Для реализации антивирусной защиты на всех компонентах ИСПДн должны применяться средства антивирусной защиты.

3.2. Антивирусная защита должна быть реализована:

– на автоматизированных рабочих местах пользователей (в том числе привилегированных пользователей);

– на серверах.

3.3. Установка (инсталляция), настройка (конфигурирование), обновление модулей средств антивирусной защиты, удаление должны осуществляться только Ответственным.

3.4. Управление параметрами настройки функций безопасности средств антивирусной защиты должно быть доступно только Ответственному.

3.5. Средства антивирусной защиты должны постоянно находиться в активном состоянии и обеспечивать антивирусную защиту в режиме реального времени.

3.6. Автоматическое обновление модулей средств антивирусной защиты должно быть запрещено.

3.7. Обновление модулей средств антивирусной защиты должно производиться Ответственным.

4. ТРЕБОВАНИЯ К ПАРАМЕТРАМ НАСТРОЕК СРЕДСТВ АНТИВИРУСНОЙ ЗАЩИТЫ

4.1. Периодичность поиска вредоносных компьютерных программ (вирусов) средствами антивирусной защиты должно обеспечиваться в соответствии с таблицей 2.

Таблица 2 – Периодичность поиска вирусов

№ п/п	Объект проверки	Частота проверки
1.	Системная память	Не реже одного раза в сутки
2.	Объекты (файлы), загружаемые при старте операционной системы	Не реже одного раза в сутки
3.	Объекты (файлы), поступающие по каналам передачи данных	Каждый раз перед открытием (запуском) объекта (файла)
4.	Файлы инсталляции программного обеспечения	Каждый раз перед установкой (инсталляцией)
5.	Файлы обновлений программного обеспечения	Каждый раз перед обновлением программного обеспечения
6.	Машинные носители информации, встроенные в портативные или стационарные технические средства	Не реже одного раза в неделю
7.	Съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные носители)	Каждый раз при подключении

4.2. Антивирусная проверка должна осуществляться современными методами обнаружения вредоносных компьютерных программ (вирусов), в том числе включать:

– сигнатурный метод – метод, основанный на поиске в объектах (файлах) сигнатур известных компьютерных вирусов;

– метод обнаружения изменений – метод, основанный на предварительном запоминании характеристик всех областей диска, которые могут подвергаться нападению компьютерными вирусами, и их периодической проверке на изменения;

– методы резидентных сторожей – метод, основанный на отслеживании всех подозрительных действий, выполняемых другими программами;

– методы эвристического анализа (эвристического сканирования).

4.3. Средства антивирусной защиты при обнаружении вредоносной компьютерной программы (вируса) должны выполнять следующие действия:

– зафиксировать в журнале регистрации событий факт обнаружения вредоносной компьютерной программы (вируса);

– удалить зараженный объект (файла) либо переместить его в карантин;

– уведомить в масштабе времени, близком к реальному, об обнаружении вредоносной компьютерной программы (вируса).

4.4. Средства антивирусной защиты должны обеспечивать регистрацию событий, связанных с функционированием, включая:

– проведение проверок объектов на наличие вредоносных компьютерных программ (вирусов);

– отказ работоспособности средства антивирусной защиты и его компонентов;

– обнаружение вредоносной компьютерной программы (вируса);

– изменение конфигурации средства антивирусной защиты;

– обновление модулей средства антивирусной защиты и базы данных признаков вредоносных компьютерных программ (вирусов).

4.5. Журналы регистрации событий средств антивирусной защиты должны храниться не менее 1 года и должны быть доступны для оперативного анализа в течение 1 месяца после регистрации событий.

5. ТРЕБОВАНИЯ К ОБНОВЛЕНИЮ БАЗЫ ДАННЫХ ПРИЗНАКОВ ВРЕДОНОСНЫХ КОМПЬЮТЕРНЫХ ПРОГРАММ (ВИРУСОВ)

5.1. Ответственный должен обеспечить обновление базы данных признаков вредоносных компьютерных программ (вирусов) средств антивирусной защиты по факту их выпуска производителем средства антивирусной защиты.

5.2. Базы данных признаков вредоносных компьютерных программ (вирусов) должны быть получены из доверенных источников. В качестве доверенных источников следует рассматривать официальные сайты производителей используемых средств защиты информации.

5.3. Ответственный должен периодически проводить мероприятия по контролю обновления баз данных признаков вредоносных компьютерных программ (вирусов). Мероприятия должны быть включены в ежегодный план мероприятий по защите персональных данных.

6. ДЕЙСТВИЯ ПРИ ОБНАРУЖЕНИИ ВРЕДОНОСНЫХ КОМПЬЮТЕРНЫХ ПРОГРАММ (ВИРУСОВ)

6.1. При обнаружении вредоносных компьютерных программ (вирусов), Ответственный должен принять меры по предотвращению наступления негативных последствий заражения. Меры могут включать:

– остановку эксплуатации зараженного компонента ИСПДн и (или) изоляцию его от остальных компонентов;

– удаление вредоносной программы;

– установление причин и источника заражения;

– инициацию и проведение служебной проверки по факту заражения вредоносной компьютерной программой (вирусом);

– принятие мер по минимизации возможности подобных заражений в дальнейшем;

– проведение полной антивирусной проверки всех компонентов ИСПДн.

6.2. Возобновление работы с компонентом ИСПДн, подвергшимся заражению, осуществляется только после окончания работ по удалению вредоносных программ и проведения антивирусной проверки прочих объектов (файлов).

7. ОТВЕТСТВЕННОСТЬ

7.1. Ответственный несет персональную ответственность за ненадлежащее исполнение или неисполнение положений настоящего Регламента.

ПРИЛОЖЕНИЕ № 5
к приказу ООО МИП «ДНК-ДИАГНОСТИКА»
от «10» 08 2026 г. № 07

Регламент контроля (анализа) защищенности
в информационных системах персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий Регламент разработан с целью установления ООО МИП «ДНК-ДИАГНОСТИКА» (далее – ООО МИП «ДНК-ДИАГНОСТИКА») общих правил, требований и процедур контроля (анализа) защищенности в информационных системах персональных данных ООО МИП «ДНК-ДИАГНОСТИКА» (далее – ИСПДн).

1.2. Настоящий документ не применяется в отношении ИСПДн, включенных в перечень объектов, подлежащих защите в ООО МИП «ДНК-ДИАГНОСТИКА» в соответствии с требованиями приказа Федеральной службы по техническому и экспортному контролю от 11 апреля 2025 г. № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений», утвержденный локальным актом ООО МИП «ДНК-ДИАГНОСТИКА».

1.3. Меры защиты персональных данных, реализация которых описана в рамках настоящего Регламента, представлены в таблице 1.

Таблица 1 – Меры защиты персональных данных, реализация которых описана в рамках настоящего Регламента

Условное обозначение и номер меры	Меры защиты персональных данных
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации

1.4. Состав мер определен на основании уровня защищенности персональных данных и структурно-функциональных характеристик ИСПДн.

1.5. Регламент предназначен для специалистов по защите персональных данных.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. Специалист по защите персональных данных (Ответственный) – сотрудник ООО МИП «ДНК-ДИАГНОСТИКА», выполняющий непосредственные функции по защите персональных данных, в том числе по управлению системой защиты персональных данных, по управлению конфигурацией ИСПДн и ее системой защиты, по выявлению компьютерных инцидентов и реагированию на них.

3. КОНТРОЛЬ УСТАНОВКИ ОБНОВЛЕНИЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

3.1. Мероприятия по контролю установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации, должны

проводиться на периодической основе и должны быть включены в ежегодный план мероприятий по защите персональных данных. В ходе проведения данного мероприятия должны осуществляться:

3.1.1. Проверка использования последних версий общесистемного, прикладного и специального программного (микропрограммного) обеспечения, включая программное обеспечение средств защиты информации (проверка соответствия версий: используемой и представленной на официальном сайте (портале) производителя (разработчика));

3.1.2. Проверка наличия отметок об установке (применении) обновлений в эксплуатационной документации (техническом паспорте);

3.1.3. Документирование результатов контроля.

4. КОНТРОЛЬ ПРАВИЛ ГЕНЕРАЦИИ И СМЕНЫ ПАРОЛЕЙ ПОЛЬЗОВАТЕЛЕЙ, ЗАВЕДЕНИЯ И УДАЛЕНИЯ УЧЕТНЫХ ЗАПИСЕЙ ПОЛЬЗОВАТЕЛЕЙ, РЕАЛИЗАЦИИ ПРАВИЛ РАЗГРАНИЧЕНИЯ ДОСТУПА, ПОЛНОМОЧИЙ ПОЛЬЗОВАТЕЛЕЙ В ИСПДН

4.1. Мероприятия по контролю правил генерации и смены паролей, заведения и удаления учетных записей пользователя, реализации правил разграничения доступа, полномочий пользователя в ИСПДн должны проводиться на периодической основе и должны быть включены в ежегодный план мероприятий по защите персональных данных. В ходе проведения данного мероприятия должны осуществляться:

4.1.1. Проверка соблюдения правил генерации и смены паролей пользователями;

4.1.2. Проверка соблюдения правил заведения и удаления учетных записей пользователей, предусмотренных Регламентом управления доступом в информационных системах персональных данных;

4.1.3. Проверка реализации правил разграничения доступа в соответствии с Регламентом управления доступом в информационных системах персональных данных и локальным актом ООО МИП «ДНК-ДИАГНОСТИКА», утверждающим систему разграничения доступа в ИСПДн;

4.1.4. Принятие мер, направленных на устранение выявленных недостатков.

5. ОТВЕТСТВЕННОСТЬ

5.1. Ответственный несет персональную ответственность за ненадлежащее исполнение или неисполнение положений настоящего Регламента.

ПРИЛОЖЕНИЕ № 6
к приказу ООО МИП «ДНК-ДИАГНОСТИКА»
от «10» 08 2026 г. № 04

Регламент защиты технических средств информационных систем персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий Регламент разработан с целью установления ООО МИП «ДНК-ДИАГНОСТИКА» (далее – ООО МИП «ДНК-ДИАГНОСТИКА») общих правил, требований и процедур защиты технических средств информационных систем персональных данных ООО МИП «ДНК-ДИАГНОСТИКА» (далее – ИСПДн) и персональных данных.

1.2. Настоящий документ не применяется в отношении ИСПДн, включенных в перечень объектов, подлежащих защите в ООО МИП «ДНК-ДИАГНОСТИКА» в соответствии с требованиями приказа Федеральной службы по техническому и экспортному контролю от 11 апреля 2025 г. № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений», утвержденный локальным актом ООО МИП «ДНК-ДИАГНОСТИКА».

1.3. Меры защиты персональных данных, реализация которых описана в рамках настоящего Регламента, представлены в таблице 1.

Таблица 1 – Меры защиты персональных данных, реализация которых описана в рамках настоящего Регламента

Условное обозначение и номер меры	Меры защиты персональных данных
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр

1.4. Состав мер определен на основании уровня защищенности персональных данных и структурно-функциональных характеристик ИСПДн.

1.5. Регламент предназначен для специалистов по защите персональных данных.

2. УПРАВЛЕНИЕ ФИЗИЧЕСКИМ ДОСТУПОМ К ТЕХНИЧЕСКИМ СРЕДСТВАМ, СРЕДСТВАМ ЗАЩИТЫ ИНФОРМАЦИИ, СРЕДСТВАМ ОБЕСПЕЧЕНИЯ

ФУНКЦИОНИРОВАНИЯ, А ТАКЖЕ В ПОМЕЩЕНИЯ И СООРУЖЕНИЯ, В КОТОРЫХ ОНИ УСТАНОВЛЕНЫ

2.1. Управление физическим доступом предусматривает:

– определение перечня помещений, в которых размещены ИСПДн. Перечень утверждается локальным актом ООО МИП «ДНК-ДИАГНОСТИКА»;

– определение порядка доступа сотрудников ООО МИП «ДНК-ДИАГНОСТИКА» в помещения, в которых осуществляется обработка персональных данных и размещены ИСПДн. Порядок утверждается локальным актом ООО МИП «ДНК-ДИАГНОСТИКА»;

– санкционирование физического доступа;

– учет доступа.

2.2. Управление физическим доступом может достигаться:

– оснащением входных дверей помещений, в которых расположены технические средства и устройства ИСПДн, замками;

– постоянным закрытием входных дверей помещений, в которых расположены технические средства и устройства ИСПДн, на замок и их открытием только для санкционированного прохода;

– внедрением контрольно-пропускного и внутриобъектового режима (доступ посетителей на территорию ООО МИП «ДНК-ДИАГНОСТИКА» осуществляется только при наличии пропуска и документа, удостоверяющего личность);

– организацией доступа к информационным ресурсам по заявке, согласованной в соответствии с пропускным внутриобъектовым режимом;

– предоставлением доступа в помещения, в которых размещены серверные компоненты ИСПДн и обеспечивающие их функционирование устройства, строго определенному кругу лиц, осуществляющему их техническое обслуживание и сопровождение;

– ограничением нахождения посетителей и других лиц имеющих право разового доступа на территорию ООО МИП «ДНК-ДИАГНОСТИКА». Нахождение таких лиц допускается только в присутствии лиц, имеющих право постоянного доступа на территорию ООО МИП «ДНК-ДИАГНОСТИКА»;

– ознакомлением лиц, имеющих право постоянного доступа в помещения, в которых размещены ИСПДн, с локальными актами ООО МИП «ДНК-ДИАГНОСТИКА» в области обеспечения безопасности персональных данных;

– предоставлением доступа в помещения, в которых размещены ИСПДн, только тем лицам, которым указанный доступ необходим в рамках исполнения должностных обязанностей или обязанностей, предусмотренных договорами (соглашениями);

– фиксированием факта разового доступа лиц в помещения, в которых размещены ИСПДн.

3. РАЗМЕЩЕНИЕ УСТРОЙСТВ ВЫВОДА (ОТОБРАЖЕНИЯ) ИНФОРМАЦИИ

3.1. В качестве устройств вывода (отображения) информации рассматриваются:

– мониторы автоматизированных рабочих мест пользователей;

– мониторы консолей управления технических средств (серверов,

телекоммуникационного оборудования и иных технических средств);

– печатающие устройства.

3.2. При размещении данных устройств вывода (отображения) информации следует исключать возможность несанкционированного просмотра выводимой на них информации как из-за пределов помещения, в которых размещено устройство, так и в пределах этих помещений. С этой целью не следует размещать устройства вывода (отображения, печати) информации:

– напротив оконных проемов;

– напротив входных дверей;

– напротив технологических отверстий;

– в коридорах, холлах;

– в иных местах, доступных для несанкционированного просмотра.

4. ОТВЕТСТВЕННОСТЬ

4.1. Ответственный несет персональную ответственность за ненадлежащее исполнение или неисполнение положений настоящего Регламента.

ПРИЛОЖЕНИЕ № 7
к приказу ООО МИП «ДНК-ДИАГНОСТИКА»
от «10» 09 2026 г. № 07

Регламент защиты информационных систем персональных данных, их средств, систем связи и передачи данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий Регламент разработан с целью установления ООО МИП «ДНК-ДИАГНОСТИКА»(далее – ООО МИП «ДНК-ДИАГНОСТИКА») общих правил, требований и процедур защиты информационных систем персональных данных ООО МИП «ДНК-ДИАГНОСТИКА» (далее – ИСПДн), их средств, систем связи и передачи данных.

1.2. Настоящий документ не применяется в отношении ИСПДн, включенных в перечень объектов, подлежащих защите в ООО МИП «ДНК-ДИАГНОСТИКА» в соответствии с требованиями приказа Федеральной службы по техническому и экспортному контролю от 11 апреля 2025 г. № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений», утвержденный локальным актом ООО МИП «ДНК-ДИАГНОСТИКА».

1.3. Меры защиты персональных данных, реализация которых описана в рамках настоящего Регламента, представлены в таблице 1.

Таблица 1 – Меры защиты персональных данных, реализация которых описана в рамках настоящего Регламента

Условное обозначение и номер меры	Меры защиты персональных данных
ЗИС.3	Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при их передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи

1.4. Состав мер определен на основании уровня защищенности персональных данных и структурно-функциональных характеристик ИСПДн.

1.5. Регламент предназначен для специалистов по защите персональных данных.

2. ЗАЩИТА ИНФОРМАЦИИ ПРИ ЕЕ ПЕРЕДАЧЕ ПО КАНАЛАМ СВЯЗИ, ИМЕЮЩИМ ВЫХОД ЗА ПРЕДЕЛЫ КОНТРОЛИРУЕМОЙ ЗОНЫ

2.1. При передаче информации по каналам связи, выходящим за пределы контролируемой зоны, должна быть обеспечена защита информации от раскрытия, модификации и навязывания (ввода ложной информации).

2.2. Защита информации при ее передаче по каналам связи должна обеспечиваться одним или комбинацией из следующих способов:

– защита каналов связи от несанкционированного физического доступа (подключения) к ним;

– применение средств криптографической защиты информации.

2.3. Для защиты информации криптографическими методами должны использоваться программные или программно-аппаратные средства, прошедшие оценку соответствия в форме обязательной сертификации.

3. УПРАВЛЕНИЕ СЕТЕВЫМИ ПОТОКАМИ

3.1. В ИСПДн должно осуществляться управление сетевыми потоками при передаче информации между устройствами, сегментами, включающее:

– фильтрацию сетевых потоков в соответствии с правилами управления потоками;

– разрешение передачи информации только по разрешенному маршруту;

– изменение (перенаправление) маршрута передачи информации (в установленных ООО МИП «ДНК-ДИАГНОСТИКА» случаях);

– запись во временное хранилище информации для анализа и принятия решения о возможности ее дальнейшей передачи (в установленных ООО МИП «ДНК-ДИАГНОСТИКА» случаях).

3.2. Управление сетевыми потоками должно обеспечивать разрешенный маршрут прохождения информации между устройствами, сегментами ИСПДн, а также между ИСПДн или при взаимодействии с информационно-телекоммуникационными сетями провайдеров, предоставляющих услуги связи или сетями связи общего пользования на основе правил управления сетевыми потоками.

4. ОТВЕТСТВЕННОСТЬ

4.1. Ответственный несет персональную ответственность за ненадлежащее исполнение или неисполнение положений настоящего Регламента.