СОГЛАСОВАНО:
Общим собранием трудового коллектива
МБДОУ Приволенский д/с Аленка»
Протокол от 6.03.2023_г.

УТВЕРЖДЕНО:
Заведующим
МБДОУ Приволенский д/с Аленка»
_____ Гулакова С.В.
Приказ от 6.03.2023г. № 44

Муниципальное бюджетное дошкольное образовательное учреждение Приволенский детский сад «Аленка»
(МБДОУ Приволенский д/с «Аленка»)

Положение
о порядке организации и проведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

1. Общие положения

1.1. Положение об организации и проведении работ по обеспечению безопасности персональных данных при их автоматизированной обработке в информационных системах персональных данных (далее - Положение) разработано в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ "О персональных данных", Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", Приказом ФСТЭК России от 11.02.2013 № 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах", Приказом ФСТЭК России от 18.02.2013 № 21 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных", методическими рекомендациями ФСТЭК России и ФСБ России в целях обеспечения безопасности персональных данных (далее - ПДн) при их обработке в информационных системах персональных данных (далее - ИСПДн).

1.2. Положение определяет порядок работы персонала в ИСПДн в части обеспечения безопасности ПДн при их обработке, порядок разбирательства и составления заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, разработку и принятие мер по предотвращению возможных опасных последствий таких нарушений, порядок приостановки предоставления ПДн в случае обнаружения нарушений порядка их предоставления, порядок обучения персонала практике работы в ИСПДн, порядок проверки электронного журнала обращений к ИСПДн согласно приложению № 7 к Положению, порядок контроля соблюдения условий использования средств защиты информации, предусмотренные эксплуатационной и технической документацией, правила обновления общесистемного и прикладного программного обеспечения, правила организации антивирусной защиты и парольной защиты ИСПДн, порядок охраны и допуска посторонних лиц в помещения ограниченного доступа.

2. Порядок работы персонала ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн. Настоящий порядок определяет действия персонала ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн.

2.1. Допуск пользователей для работы на компьютерах ИСПДн осуществляется на основании приказа и в соответствии со списком лиц, допущенных к работе в ИСПДн. С целью обеспечения ответственности за ведение, нормальное функционирование и контроль работы средств защиты информации в ИСПДн, назначается ответственный за выполнение работ по обеспечению безопасности ПДн при их обработке в ИСПДн (администратор безопасности); с целью

контроля выполнения необходимых мероприятий по обеспечению безопасности - ответственный за организацию обработки ПДн.

2.2. Пользователь имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн. При этом для хранения информации, содержащей ПДн, разрешается использовать только машинные носители информации, учтенные в Журнале учета машинных носителей согласно приложению № 2 к Положению.

2.3. Пользователь несет ответственность за правильность включения и выключения средств вычислительной техники (СВТ), входа в систему и все действия при работе в ИСПДн.

2.4. Вход пользователя в систему может осуществляться по выдаваемому ему электронному идентификатору или по персональному паролю.

2.5. Запись информации, содержащей ПДн, осуществляется пользователем на съемные машинные носители информации, соответствующим образом учтенные в Журнале учета машинных носителей согласно приложению № 2 к Положению.

2.6. При работе со съемными машинными носителями информации пользователь каждый раз перед началом работы обязан проверить их на отсутствие вирусов с использованием штатных антивирусных программ, установленных на компьютерах ИСПДн. В случае обнаружения вирусов пользователь обязан немедленно прекратить их использование и действовать в соответствии с требованиями данного Положения.

2.7. Каждый сотрудник, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки ПДн и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИСПДн, несет персональную ответственность за свои действия и обязан:

- строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн; - знать и строго выполнять правила работы со средствами защиты информации, установленными на компьютерах ИСПДн;

- хранить в тайне свой пароль (пароли) (в соответствии с пунктами 8.5, 8.6 данного Положения и с установленной периодичностью менять свой пароль (пароли);- хранить свое индивидуальное устройство идентификации (ключ) и другие реквизиты в сейфе (металлическом шкафу);

- выполнять требования Положения по организации антивирусной защиты в полном объеме.

Немедленно известить ответственного за эксплуатацию ИСПДн либо ответственного за выполнение работ по обеспечению безопасности персональных данных в случае утери индивидуального устройства идентификации (ключа) или при подозрении компрометации личных ключей и паролей, а также при обнаружении:

- нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на составляющих узлах и блоках СВТ или иных фактов совершения в его отсутствие попыток несанкционированного доступа (далее - НСД) к данным, защищаемым СВТ;

- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ИСПДн;

- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию СВТ, выхода из строя или неустойчивого функционирования узлов СВТ или периферийных устройств (сканера, принтера и т.п.), а также перебоев в системе электроснабжения;

- некорректного функционирования установленных на компьютеры технических средств защиты;

- непредусмотренных отводов кабелей и подключенных устройств.

Пользователю категорически запрещается: - использовать компоненты программного и аппаратного обеспечения СВТ в неслужебных целях;

- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИСПДн или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные архивом дистрибутивов установленного программного обеспечения;

- осуществлять обработку ПДн в присутствии посторонних (не допущенных к данной информации) лиц;

- записывать и хранить конфиденциальную информацию (содержащую сведения ограниченного распространения) на неучтенных машинных носителях информации (гибких магнитных дисках и т.п.);

- оставлять включенным без присмотра компьютер, не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);

- оставлять без личного присмотра на рабочем месте или где бы то ни было свое персональное устройство идентификации, машинные носители и распечатки, содержащие защищаемую информацию (сведения ограниченного распространения);

- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации;

- размещать средства ИСПДн так, чтобы с них существовала возможность визуального считывания информации.

2.8. Ответственный за выполнение работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (далее - Администратор безопасности) обязан:

- знать состав основных и вспомогательных технических систем и средств (далее - ОТСС и ВТСС), установленных и смонтированных в ИСПДн, перечень используемого программного обеспечения (далее - ПО) в ИСПДн;

- контролировать целостность печатей (пломб, защитных наклеек) на периферийном оборудовании, защищенных СВТ и других устройствах;

- производить необходимые настройки подсистемы управления доступом установленных в ИСПДн СЗИ от НСД и сопровождать их в процессе эксплуатации, при этом:

- реализовывать полномочия доступа (чтение, запись) для каждого пользователя к элементам защищаемых информационных ресурсов (файлам, каталогам, принтеру и т.д.);

- вводить описания пользователей ИСПДн в информационную базу СЗИ от НСД;

- своевременно удалять описания пользователей из базы данных СЗИ при изменении списка допущенных к работе лиц;

- контролировать доступ лиц в помещение в соответствии со списком сотрудников, допущенных к работе в ИСПДн;

- проводить инструктаж сотрудников - пользователей компьютеров по правилам работы с используемыми техническими средствами и системами защиты информации;

- вести журналы согласно приложениям № 1, № 2, № 3, № 4, № 5, № 6, № 7, № 8, № 9, № 10 к Положению;

- контролировать своевременное (не реже чем один раз в течение 360 дней) проведение смены паролей для доступа пользователей к компьютерам и ресурсам ИСПДн;

- обеспечивать постоянный контроль выполнения сотрудниками установленного комплекса мероприятий по обеспечению безопасности информации в ИСПДн;

- осуществлять контроль порядка создания, учета, хранения и использования резервных и архивных копий массивов данных;

- настраивать и сопровождать подсистемы регистрации и учета действий пользователей при работе в ИСПДн;

- вводить в базу данных СЗИ от несанкционированного доступа описания событий, подлежащих регистрации в системном журнале согласно приложению № 10 к Положению;

- проводить анализ системного журнала для выявления попыток несанкционированного доступа к защищаемым ресурсам не реже одного раза в 10 дней;

- организовывать печать файлов пользователей на принтере и осуществлять контроль соблюдения установленных правил и параметров регистрации и учета бумажных носителей информации. Сопровождать подсистемы обеспечения целостности информации в ИСПДн;

- периодически тестировать функции СЗИ от НСД, особенно при изменении программной среды и полномочий исполнителей; - восстанавливать программную среду, программные средства и настройки СЗИ при сбоях;

- вести две копии программных средств СЗИ от НСД и контролировать их работоспособность;

- контролировать отсутствие на магнитных носителях остаточной информации по окончании работы пользователей;

- периодически обновлять антивирусные средства (базы данных), контролировать соблюдение пользователями порядка и правил проведения антивирусного тестирования:

- проводить работу по выявлению возможных каналов вмешательства в процесс функционирования ИСПДн и осуществления несанкционированного доступа к информации и техническим средствам вычислительной техники;

- сопровождать подсистему защиты информации от утечки за счет побочных электромагнитных излучений и наводок, контролировать соблюдение требований по размещению и использованию технических средств ИСПДн;

- контролировать соответствие документально утвержденного состава аппаратной и программной части ИСПДн реальным конфигурациям ИСПДн, вести учет изменений аппаратно-программной конфигурации;

- обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации технического обслуживания ИСПДн и отправке его в ремонт (контролировать затирание конфиденциальной информации на магнитных носителях с составлением соответствующего акта);

- присутствовать (участвовать) в работах по внесению изменений в аппаратно-программную конфигурацию ИСПДн;

- вести Журнал учета нештатных ситуаций, фактов вскрытия и опечатывания СВТ согласно приложению № 5 к Положению, выполнения профилактических работ, установки и модификации аппаратных и программных средств СВТ;

- поддерживать установленный порядок проведения антивирусного контроля согласно требованиям настоящего Положения, в случае отказа средств и систем защиты информации принимать меры по их восстановлению;

- докладывать ответственному за защиту информации, ответственному за эксплуатацию ИСПДн о неправомерных действиях пользователей, приводящих к нарушению требований по защите информации;

- вести документацию на ИСПДн в соответствии с требованиями нормативных документов.

2.9. Администратор безопасности, а также ответственный за организацию обработки персональных данных имеют право:

- требовать от сотрудников - пользователей ИСПДн соблюдения установленной технологии обработки информации и выполнения инструкций по обеспечению безопасности и защите информации в ИСПДн;

- инициировать проведение служебных проверок по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, модификации, порчи защищаемой информации и технических компонентов ИСПДн;

- требовать прекращения обработки информации в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации;

- участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа.

3. Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных, защищаемой информации и средств защиты информации

3.1. Настоящий порядок определяет организацию резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации.

3.2. К использованию для создания резервной копии в ИСПДн допускаются только зарегистрированные в журнале учета носители.

3.3. Администратор безопасности ежеквартально осуществляет резервное копирование конфиденциальной информации.

3.4. Носители информации (ЖМД, CD, USB-накопитель, другие), предназначенные для создания резервной копии и хранения конфиденциальной информации, выдаются установленным порядком руководителем, ответственным за защиту информации, и (или) администратором. По окончании процедуры резервного копирования электронные носители конфиденциальной информации сдаются на хранение администратору безопасности или руководителю, или ответственному за защиту информации.

3.5. Перед резервным копированием пользователь или администратор безопасности обязан проверить электронный носитель (ЖМД, CD, USB-накопитель) на отсутствие вирусов.

3.6. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль в соответствии с разделом 7 настоящего Положения.

3.7. Запрещается запись посторонней информации на электронные носители (ЖМД, CD, USB-накопитель и другие) резервной копии.

3.8. Порядок создания резервной копии:

- вставить в компьютер зарегистрированный электронный носитель (ЖМД, CD, USB-накопитель, другие) для резервного копирования;
- выбрать необходимый каталог (файл) для создания резервного архива;
- при использовании систем управления базами данных необходимо создать файл с резервной копией защищаемой информации с помощью встроенных средств системы;
- выполнить процедуру создания резервной копии;
- произвести копирование на отчуждаемый носитель;
- произвести отключение отчуждаемого носителя и, создав необходимые записи в журналах, убрать носитель в хранилище, указанного в журнале учета хранилищ, согласно приложению № 3 к Положению.

3.9. Хранение отчуждаемого носителя с резервной копией защищаемой информации осуществляется в специальном металлическом хранилище совместно с ключевой и аутентифицирующей информацией.

3.10. При восстановлении работоспособности программного обеспечения сначала осуществляется резервное копирование защищаемой информации, затем производится полная деинсталляция некорректно работающего программного обеспечения.

3.11. Восстановление программного обеспечения производится путем его инсталляции с использованием эталонных дистрибутивов, хранение которых осуществляется администратором безопасности в специальном хранилище.

3.12. При необходимости ремонта технических средств с них удаляются опечатывающие пломбы и по согласованию с администратором безопасности, ответственным за защиту информации, при условии проведенной аттестации информационной системы, представителем организации, проводившей аттестацию, оборудование передается в сервисный центр производителя. Ремонт носителей защищаемой информации не допускается. Неисправные носители с защищаемой информацией подлежат уничтожению в соответствии с порядком уничтожения носителей защищаемой информации. Работа с использованием неисправных технических средств запрещается.

3.13. При работе на компьютерах ИСПДн рекомендуется использовать источники бесперебойного питания с целью предотвращения повреждения технических средств и (или) защищаемой информации в результате сбоев в сети электропитания.

3.14. При восстановлении работоспособности средств защиты информации следует выполнить их настройку в соответствии с требованиями безопасности информации, изложенными в техническом задании на создание системы защиты персональных данных. Настройку данных средств должен выполнять сотрудник организации, имеющей лицензию на деятельность по технической защите конфиденциальной информации.

3.15. Восстановление средств защиты информации производится с использованием эталонных сертифицированных дистрибутивов, которые хранятся в хранилище. После успешной настройки средств защиты информации необходимо выполнить резервное копирование настроек данных средств с помощью встроенных в них функций на зарегистрированный носитель.

3.16. Ответственность за проведение резервного копирования в ИСПДн в соответствии с требованиями настоящего Положения возлагается на администратора безопасности.

3.17. Ответственность за проведение мероприятий по восстановлению работоспособности технических средств и программного обеспечения баз данных возлагается на администратора безопасности.

3.18. Ответственность за проведение мероприятий по восстановлению средств защиты информации (далее - СЗИ) возлагается на администратора безопасности.

4. Порядок контроля защиты информации в ИСПДн и приостановки предоставления ПДн в случае обнаружения нарушений порядка их предоставления. Порядок разбирательства и составления заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации и принятие мер по предотвращению возможных опасных последствий

4.1. Контроль защиты информации в ИСПДн - комплекс организационных и технических мероприятий, которые организуются и осуществляются в целях предупреждения и пресечения возможности получения посторонними лицами охраняемых сведений, выявления и предотвращения утечки информации по техническим каналам, исключения или существенного затруднения несанкционированного доступа к информации, хищения технических средств и носителей информации, предотвращения специальных программно-технических воздействий, вызывающих нарушение характеристик безопасности информации или работоспособности систем информатизации.

4.2. Основными задачами контроля являются:

- проверка организации выполнения мероприятий по защите информации в подразделениях, учета требований по защите информации в разрабатываемых плановых и распорядительных документах;
- выявление демаскирующих признаков объектов ИСПДн;
- уточнение зон перехвата обрабатываемой на объектах информации, возможных каналов утечки информации, несанкционированного доступа к ней и программно-технических воздействий на информацию;
- проверка выполнения установленных норм и требований по защите информации от утечки по техническим каналам, оценка достаточности и эффективности мероприятий по защите информации;
- проверка выполнения требований по защите ИСПДн от несанкционированного доступа;
- проверка выполнения требований по антивирусной защите автоматизированных систем и автоматизированных рабочих мест;
- проверка знаний работников по вопросам защиты информации и их соответствия требованиям уровня подготовки для конкретного рабочего места;
- оперативное принятие мер по пресечению нарушений требований (норм) защиты информации в ИСПДн;
- разработка предложений по устранению (ослаблению) демаскирующих признаков и технических каналов утечки информации.

4.3. Контроль защиты информации проводится с учетом реальных условий по всем физическим полям, по которым возможен перехват информации, циркулирующей в ИСПДн, и осуществляется по объектовому принципу, при котором на объекте одновременно проверяются все вопросы защиты информации. Перечень каналов утечки устанавливается в соответствии с моделью угроз.

4.4. В ходе контроля проверяются:

- соответствие принятых мер по обеспечению безопасности персональных данных (далее - ОБ ПДн);
- своевременность и полнота выполнения требований настоящего Положения и других руководящих документов ОБ ПДн;
- полнота выявления демаскирующих признаков охраняемых сведений об объектах защиты и возможных технических каналов утечки информации, несанкционированного доступа к ней и программно-технических воздействий на информацию;

- эффективность применения организационных и технических мероприятий по защите информации;

- устранение ранее выявленных недостатков.

Кроме того, могут проводиться необходимые измерения и расчеты приглашенными для этих целей специалистами организации, имеющей соответствующие лицензии ФСТЭК России.

4.5. Основными видами технического контроля являются визуально-оптический контроль, контроль эффективности защиты информации от утечки по техническим каналам, контроль несанкционированного доступа к информации и программно-технических воздействий на информацию.

4.6. Полученные в ходе ведения контроля результаты обрабатываются и анализируются в целях определения достаточности и эффективности предписанных мер защиты информации и выявления нарушений. При обнаружении нарушений норм и требований по защите информации администратор безопасности докладывает руководителю для принятия ими решения о прекращении обработки информации и проведения соответствующих организационных и технических мер по устранению нарушения. Результаты контроля защиты информации оформляются актами либо в соответствующих журналах учета результатов контроля.

4.7. Невыполнение предписанных мероприятий по защите ПДн считается предпосылкой к утечке информации (далее - предпосылка).

По каждой предпосылке для выяснения обстоятельств и причин невыполнения установленных требований по указанию главного врача или ответственного за организацию обработки персональных данных проводится расследование.

Для проведения расследования назначается комиссия с привлечением администратора безопасности. Комиссия обязана установить, имела ли место утечка сведений, обстоятельства, ей сопутствующие, установить лиц, виновных в нарушении предписанных мероприятий по защите информации, установить причины и условия, способствовавшие нарушению, и выработать рекомендации по их устранению. После окончания расследования руководитель принимает решение о наказании виновных лиц и необходимых мероприятиях по устранению недостатков.

4.8. Ведение контроля защиты информации осуществляется путем проведения периодических, плановых и внезапных проверок объектов защиты. Периодические, плановые и внезапные проверки объектов организации проводятся, как правило, силами администратора безопасности и (или) ответственного за защиту информации, в соответствии с утвержденным планом или по согласованию с руководителем.

4.9. Одной из форм контроля защиты информации является обследование объектов ИСПДн. Оно проводится не реже одного раза в год рабочей группой в составе администратора безопасности, ответственного за защиту информации, ответственного за эксплуатацию объекта. Для обследования ИСПДн может привлекаться организация, имеющая лицензию ФСТЭК России на деятельность по технической защите информации.

4.10. Обследование ИСПДн проводится с целью определения соответствия помещений, технических и программных средств требованиям по защите информации, установленным в Аттестате соответствия (если проводилась аттестация), и (или) требованиям по безопасности персональных данных.

4.11. В ходе обследования проверяется:

- соответствие текущих условий функционирования обследуемого объекта ИСПДн условиям, сложившимся на момент проверки;

- соблюдение организационно-технических требований помещений, в которых располагается ИСПДн;

- сохранность печатей, пломб на технических средствах передачи и обработки информации, а также на устройствах их защиты, отсутствие повреждений экранов корпусов аппаратуры, оболочек кабелей и их соединений с шинами заземления;

- соответствие выполняемых на объекте ИСПДн мероприятий по защите информации данным, изложенным в настоящем Положении;

- выполнение требований по защите информационных систем от несанкционированного доступа;

- выполнение требований по антивирусной защите.

4.12. Для выявления радиоэлектронных устройств и проводов неизвестного назначения, преднамеренного нарушения защитных свойств оборудования, а также не предусмотренных правилами эксплуатации отводов от оборудования и соединительных линий, проложенных в выделенных и защищаемых помещениях, а также других нарушений и способов возникновения каналов утечки информации необходимо:

- тщательно осмотреть мебель, сувениры (особенно иностранного производства), оборудование, установленное в этом помещении, осветительную аппаратуру, ниши отопительных батарей, шторы, оконные проемы;
- вскрыть и осмотреть розетки, выключатели осветительной сети, люки вентиляции и каналы скрытой проводки;
- проверить качество установки стеклопакетов оконных проемов;
- провести аппаратурную проверку помещения на отсутствие возможно внедренных электронных устройств перехвата информации (при наличии соответствующей аппаратуры), при необходимости для проведения данных видов работ могут привлекаться организации, имеющие соответствующие лицензии ФСБ России.

4.13. Государственный контроль состояния защиты информации осуществляется Федеральной службой по техническому и экспортному контролю России и Федеральной службой безопасности России в рамках их полномочий в соответствии с действующим законодательством Российской Федерации. Доступ представителей указанных федеральных органов исполнительной власти на объекты для проведения проверки, а также к работам и документам в объеме, необходимом для осуществления контроля, обеспечивается в установленном порядке по предъявлении служебного удостоверения сотрудника, а также документа установленной формы на право проведения проверки.

5. Порядок обучения персонала практике работы в ИСПДн в части обеспечения безопасности персональных данных

5.1. Перед началом работы в ИСПДн пользователи должны ознакомиться с инструкциями по использованию программных и технических средств, по использованию средств защиты информации под роспись.

5.2. Пользователи должны продемонстрировать администратору безопасности и (или) ответственному за защиту информации наличие необходимых знаний и умений для выполнения требований настоящего Положения. Администратор безопасности должен вести журнал учета проверок знаний и навыков пользователей согласно приложению № 8 к Положению.

5.3. Пользователи, демонстрирующие недостаточные знания и умения для обеспечения безопасности персональных данных в соответствии с требованиями настоящего Положения, к работе в ИСПДн не допускаются.

5.4. Ответственным за организацию обучения и оказание методической помощи является администратор безопасности.

5.5. Для проведения занятий, семинаров и совещаний могут привлекаться специалисты по программному и техническому обеспечению, а также специалисты органов по аттестации объектов ИСПДн, организаций-лицензиатов ФСТЭК России и ФСБ России.

5.6. К работе в ИСПДн допускаются только сотрудники, прошедшие первичный инструктаж ОБ в ИСПДн и показавшие твердые теоретические знания и практические навыки, о чем делается соответствующая запись в Журнале учета допуска к работе в ИСПДн согласно приложению № 6 к Положению.

5.7. Администратор безопасности должен иметь профильное образование (либо дипломы о повышении квалификации) в области защиты информации. Рекомендуется прохождение администратором специализированных курсов по администрированию средств защиты информации, используемых в ИСПДн.

6. Порядок проверки электронного журнала обращений к ИСПДн

6.1. Настоящий раздел Положения определяет порядок проверки электронных журналов обращений к ресурсам ИСПДн.

6.2. Проверка электронного журнала обращений проводится с целью выявления несанкционированного доступа к защищаемой информации в ИСПДн.

6.3. Право проверки электронного журнала обращений имеют:

- ответственный за организацию обработки персональных данных;
- ответственный за выполнение работ по обеспечению безопасности ПДн при их обработке в ИСПДн;
- главный врач.

6.4. На технических средствах ИСПДн, на которых установлены специализированные средства защиты информации (далее - СЗИ), проверка электронного журнала производится в соответствии с прилагаемым к указанным СЗИ Руководством.

6.5. Если в ходе периодических, плановых или внезапных проверок ИСПДн выявлены случай НСД к информации конфиденциального характера, то проводится расследование согласно пункту 4.7 данного Положения.

6.6. Проверке подлежат все электронные журналы ИСПДн.

6.7. Проверка должна проводиться не реже чем один раз в неделю с целью своевременного выявления фактов нарушения требований настоящего Положения.

6.8. Факты проверок электронных журналов отражаются в специальном журнале проверок. После каждой проверки Администратор безопасности делает соответствующую отметку в журнале и ставит свою роспись.

7. Правила антивирусной защиты

7.1. Настоящие правила определяют требования к организации защиты объекта ИСПДн от разрушающего воздействия вредоносного программного обеспечения (ПО), компьютерных вирусов и устанавливают ответственность руководителя и сотрудников, эксплуатирующих и сопровождающих компьютеры в составе ИСПДн, за их выполнение. Настоящие правила распространяются на все объекты ИСПДн.

7.2. К использованию на компьютерах допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств.

7.3. Установка и начальная настройка средств антивирусного контроля на компьютерах осуществляется администратором безопасности.

7.4. Администратор безопасности осуществляет периодическое обновление антивирусных пакетов и контроль их работоспособности.

7.5. Ярлык (ссылка) для запуска антивирусной программы должен быть доступен всем пользователям информационной системы.

7.6. Еженедельно в начале работы после загрузки компьютера в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов компьютеров.

Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных носителях (магнитных дисках, лентах, CD). Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

Настройки средств антивирусной защиты должны быть выполнены в соответствии с требованиями безопасности персональных данных определенного для данной ИСПДн класса. Настройку средств антивирусной защиты выполняет администратор безопасности.

7.7. Файлы, помещаемые в электронный архив на магнитных носителях, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

7.8. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера администратором безопасности должна быть выполнена антивирусная проверка ИСПДн.

7.9. На компьютеры запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации.

7.10. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь самостоятельно (или вместе с администратором безопасности) должен провести внеочередной антивирусный контроль компьютера.

В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан:

- приостановить обработку данных в ИСПДн;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов администратора безопасности, а также смежные подразделения, использующие эти файлы в работе;
- совместно с владельцем зараженных вирусом файлов провести анализ возможности, дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов.

7.11. Ответственность за организацию антивирусного контроля в ИСПДн в соответствии с требованиями настоящего Положения возлагается на ответственного за защиту информации.

7.12. Ответственность за проведение мероприятий антивирусной защиты в конкретной ИСПДн и соблюдение требований настоящего Положения возлагается на администратора безопасности и всех пользователей данной ИСПДн.

8. Правила парольной защиты

8.1. Данные правила регламентируют организационно-технические мероприятия по обеспечению процессов генерации, смены и прекращения действия паролей в ИСПДн, а также контроль действий пользователей при работе с паролями.

8.2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль действий пользователей при работе с паролями возлагается на администратора безопасности.

8.3. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями ОВТ самостоятельно с учетом следующих требований:

- пароль должен быть не менее 6 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем или нижнем регистрах, цифры и/или специальные символы (@, #, $, &, *, % и т.п.);
- символы паролей для рабочих станций, на которых установлено средство защиты информации от несанкционированного доступа, должны вводиться в режиме латинской раскладки клавиатуры;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);
- при смене пароля новое значение должно отличаться от предыдущих;
- пользователь не имеет права сообщать личный пароль другим лицам.

Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

8.4. В случае возникновения нештатных ситуаций, форс-мажорных обстоятельств, технологической необходимости использования имен и паролей сотрудников (исполнителей) в их отсутствие, сотрудники обязаны сразу же после смены своих паролей их новые значения (вместе с именами соответствующих учетных записей) в запечатанном конверте или опечатанном пенале передавать на хранение руководителю структурного подразделения. Запечатанные конверты (пеналы) с паролями исполнителей должны храниться в недоступном месте у руководителя структурного подразделения.

8.5. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в течение 360 дней.

8.6. Внеплановая смена личного пароля или удаление учетной записи пользователя ИСПДн в случае прекращения его полномочий должна производиться администратором безопасности (либо новым постоянным пользователем) немедленно после окончания последнего сеанса работы данного пользователя с системой на основании указания начальника отдела.

8.7. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри предприятия и другие обстоятельства) администратора безопасности.

8.8. В случае компрометации личного пароля пользователя ИСПДн должны быть немедленно предприняты меры по восстановлению парольной защиты.

8.9. Контроль действий пользователей при работе с паролями, соблюдение порядка их смены, хранения и использования возлагается на администратора безопасности.

9. Правила обновления общесистемного и прикладного программного обеспечения, технического обслуживания ИСПДн

9.1. Настоящие правила регламентируют обеспечение безопасности информации при проведении обновления, модификации общесистемного и прикладного программного обеспечения, технического обслуживания и при возникновении нештатных ситуаций в работе ИСПДн.

9.2. Все изменения конфигураций технических и программных средств ИСПДн должны производиться только на основании заявок ответственного за эксплуатацию конкретного ИСПДн.

9.3. Право внесения изменений в конфигурацию аппаратно-программных средств, защищенных ИСПДн предоставляется:

- в отношении системных и прикладных программных средств - администратору безопасности по согласованию (в случае, если проводилась аттестация) с органом по аттестации, проводившим аттестацию данной ИСПДн;
- в отношении аппаратных средств, а также в отношении программно-аппаратных средств защиты - администратору безопасности по согласованию (в случае, если проводилась аттестация) с органом по аттестации, проводившим аттестацию данной ИСПДн.

9.4. Изменение конфигурации аппаратно-программных средств ИСПДн кем-либо, кроме перечисленных в п. 9.3 уполномоченных сотрудников и подразделений, запрещено.

9.5. Процедура внесения изменений в конфигурацию системных и прикладных программных средств ИСПДн инициируется заявкой ответственного за эксплуатацию ИСПДн.

9.6. В заявке могут указываться следующие виды необходимых изменений в составе аппаратных и программных средств ИСПДн:

- установка (развертывание) на компьютер(ы) программных средств, необходимых для решения определенной задачи (добавление возможности решения данной задачи в данной ИСПДн);
- обновление (замена) на компьютере (ах) программных средств, необходимых для решения определенной задачи (обновление версий, используемых для решения определенной задачи программ);
- удаление с компьютера программных средств, использовавшихся для решения определенной задачи (исключение возможности решения данной задачи на данном компьютере).

9.7. Также в заявке указывается условное наименование ИСПДн. Наименования задач указываются в соответствии с перечнем задач архива дистрибутивов установленного программного обеспечения, которые можно решать с использованием указанного компьютера.

9.8. Заявку ответственного за эксплуатацию ИСПДн, в которой требуется произвести изменения конфигурации, рассматривает ответственный за организацию обработки персональных данных в Министерстве, визирует ее, утверждая тем самым производственную необходимость проведения указанных в заявке изменений, после чего заявка передается администратору безопасности для непосредственного исполнения работ по внесению изменений в конфигурацию компьютера, указанного в заявке ИСПДн.

9.9. Подготовка обновления, модификации общесистемного и прикладного программного обеспечения ИСПДн, тестирование, стендовые испытания (при необходимости) и передача исходных текстов, документации и дистрибутивных носителей программ в архив дистрибутивов

установленного программного обеспечения, внесение необходимых изменений в настройки средств защиты от НСД и средств контроля целостности файлов на компьютерах (обновление) и удаление системных и прикладных программных средств производится администратором безопасности по согласованию с органом по аттестации (в случае, если проводилась аттестация), проводившим аттестацию данной ИСПДн. Работы производятся в присутствии ответственного за эксплуатацию данной ИСПДн.

9.10. Установка или обновление подсистем ИСПДн должны проводиться в строгом соответствии с технологией проведения модификаций программных комплексов данных подсистем.

9.11. Установка и обновление ПО (системного, тестового и т.п.) на компьютерах производится только с оригинальных лицензионных дистрибутивных носителей; прикладного ПО - с эталонных копий программных средств, полученных из архива дистрибутивов установленного программного обеспечения.

9.12. Все добавляемые программные и аппаратные компоненты должны быть предварительно проверены на работоспособность, а также отсутствие опасных функций.

9.13. После установки (обновления) ПО администратор безопасности должен произвести требуемые настройки средств управления доступом к компонентам компьютера и проверить работоспособность ПО и правильность их настройки и произвести соответствующую запись в Журнале учета нештатных ситуаций в ИСПДн, выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн согласно приложению № 5 к Положению, делает отметку о выполнении (на обратной стороне заявки) и в Техническом паспорте.

9.14. Формат записей Журнала учета нештатных ситуаций ИСПДн, выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн устанавливается главным врачом.

9.15. При возникновении ситуаций, требующих передачи технических средств в сервисный центр с целью ремонта, ответственный за эксплуатацию ИСПДн докладывает об этом ответственному за защиту информации, который в свою очередь связывается с сотрудниками органа по аттестации (в случае, если проводилась аттестация) и в дальнейшем действует согласно их инструкциям. В данном случае администратор безопасности обязан предпринять необходимые меры для затирания защищаемой информации, которая хранилась на дисках компьютера. Оригиналы заявок (документов), на основании которых производились изменения в составе программных средств компьютеров с отметками о внесении изменений в состав программных средств, должны храниться вместе с техническим паспортом на ИСПДн и Журналом учета нештатных ситуаций ИСПДн, выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн у ответственного за защиту информации.

9.16. Копии заявок могут храниться у администратора безопасности:

- для восстановления конфигурации ИСПДн после аварий;
- для контроля правомерности установки на ИСПДн средств для решения соответствующих задач при разборе конфликтных ситуаций;
- для проверки правильности установки и настройки средств защиты ИСПДн.

9.17. Факт уничтожения данных, находившихся на диске компьютера, оформляется актом за подписью администратора безопасности и сотрудника, ответственного за эксплуатацию данной ИСПДн.

9.18. С целью соблюдения принципа персональной ответственности за свои действия каждому сотруднику, допущенному к работе на компьютерах конкретной ИСПДн, должно быть сопоставлено персональное уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать на данном компьютере.

9.19. Использование несколькими сотрудниками при работе в ИСПДн одного и того же имени пользователя ("группового имени") запрещено.

9.20. Процедура регистрации (создания учетной записи) пользователя и предоставления ему (или изменения его) прав доступа к ресурсам ИСПДн инициируется заявкой ответственного за эксплуатацию данной ИСПДн, в которой указывается:

- содержание запрашиваемых изменений (регистрация нового пользователя ИСПДн, удаление учетной записи пользователя, расширение или сужение полномочий и прав доступа к ресурсам ИСПДн ранее зарегистрированного пользователя);

- должность (с полным наименованием отдела), фамилия, имя и отчество сотрудника;

- имя пользователя (учетной записи) данного сотрудника;

- полномочия, которых необходимо лишить пользователя или которые необходимо добавить пользователю (путем указания решаемых пользователем задач в ИСПДн).

9.21. Заявку рассматривает ответственный за организацию обработки персональных данных, визируя ее, утверждая тем самым производственную необходимость допуска (изменения прав доступа) данного сотрудника к необходимым для решения им указанных в заявке задач ресурсам ИСПДн. Затем подписывает задание администратору безопасности на внесение необходимых изменений в списки пользователей соответствующих подсистем ИСПДн.

9.22. На основании задания, в соответствии с документацией на средства защиты от несанкционированного доступа, администратор безопасности производит необходимые операции по созданию (удалению) учетной записи пользователя, присвоению ему начального значения пароля (возможно также регистрацию персонального идентификатора), заявленных прав доступа к ресурсам ИСПДн и другие необходимые действия, указанные в задании. Для всех пользователей должен быть установлен режим принудительного запроса смены пароля не реже одного раза в течение 360 дней.

9.23. После внесения изменений в списки пользователей администратор безопасности должен обеспечить настройки средств защиты, соответствующие требованиям безопасности указанной ИСПДн. По окончании внесения изменений в списки пользователей в заявке делается отметка о выполнении задания за подписью исполнителя - администратор безопасности.

9.24. Сотруднику, зарегистрированному в качестве нового пользователя ИСПДн, сообщается имя соответствующего ему пользователя и может выдаваться персональный идентификатор (для работы в режиме усиленной аутентификации) и начальное(-ые) значение(-ия) пароля(-ей), которое(-ые) он обязан сменить при первом же входе в систему.

9.25. Исполненные заявка и задание (за подписью администратора безопасности) передаются руководителю на хранение, которые могут впоследствии использоваться:

- для восстановления полномочий пользователей после аварий ИСПДн;

- для контроля правомерности наличия у конкретного пользователя прав доступа к тем или иным ресурсам ИСПДн при разборе конфликтных ситуаций;

- для проверки сотрудниками контролирующих органов правильности настройки средств разграничения доступа к ресурсам ИСПДн.

10. Порядок контроля соблюдения условий использования средств защиты информации, в том числе криптографических

10.1. Данный раздел Положения определяет порядок контроля соблюдения условий использования средств защиты информации (далее - СЗИ).

10.2. Технические средства защиты информации являются важным компонентом ОБ ПДн.

10.3. Порядок работы с техническими СЗИ определен в соответствующих руководствах по настройке и использованию СЗИ обязательных для исполнения, как сотрудниками, обрабатывающими конфиденциальную информацию, так и администратором безопасности ИСПДн.

10.4. Право проверки соблюдения условий использования средств защиты информации имеют:

- главный врач;

- ответственный за организацию обработки персональных данных;

- ответственный за выполнение работ по обеспечению безопасности персональных данных.

10.5. Пользователю ИСПДн категорически запрещается:

- обрабатывать конфиденциальную информацию с отключенными СЗИ;

- менять настройки СЗИ.

10.6. Администратору безопасности запрещается менять настройки программно-аппаратных СЗИ, предустановленные специалистом организации, имеющей лицензию на деятельность по технической защите информации, без согласования с этой организацией.

10.7. Если в ходе периодических, плановых или внезапных проверок ИСПДн выявлено нарушение требования п. 10.5, то проводится расследование согласно пункту 4.7 данного Положения.

10.8. Криптографические СЗИ должны использоваться в соответствии с технической и эксплуатационной документацией на них, а также в соответствии с правилами пользования ими.

11. Порядок охраны и допуска посторонних лиц в защищаемые помещения

11.1. Настоящее Положение устанавливает порядок охраны защищаемых помещений ИСПДн.

11.2. Вскрытие и закрытие помещений осуществляется сотрудниками, работающими в данных помещениях.

Список сотрудников, имеющих право вскрывать помещения, утверждается главным врачом.

11.3. При отсутствии сотрудников, ответственных за вскрытие помещений, данные помещения могут быть вскрыты комиссией, созданной на основании распоряжения, о чем составляется акт.

11.4. При закрытии помещений сотрудники, ответственные за помещения, проверяют закрытие окон, выключают освещение, бытовые приборы, оргтехнику и проверяют противопожарное состояние помещения, а документы и носители информации, на которых содержится конфиденциальная информация, убираются для хранения в опечатываемый сейф (металлический шкаф).

11.5. Руководитель, ответственный за защиту информации, и администратор безопасности организуют проверку ИСПДн на предмет несанкционированного доступа к конфиденциальной информации и наличие документов и машинных носителей информации.

Если обнаружено вторжение в защищаемое помещение, то необходимо действовать в порядке, указанном в пункте 4.7 настоящего Положения.

11.6. В соответствии с требованиями данного Положения при обработке защищаемой информации в ИСПДн исключить неконтролируемое пребывание посторонних лиц в пределах границ контролируемой зоны ИСПДн, определенных соответствующим приказом.

12. Порядок стирания защищаемой информации и уничтожения носителей защищаемой информации

12.1. В обязательном порядке уничтожению подлежат поврежденные, выводимые из эксплуатации носители, содержащие защищаемую информацию, использование которых не предполагается в дальнейшем. Стиранию подлежат носители, содержащие защищаемую информацию, которые выводятся из эксплуатации в составе ИСПДн. Не допускаются стирание неисправных носителей и передача их в сервисный центр для ремонта. Такие носители должны уничтожаться в соответствии с настоящим Порядком.

12.2. Стирание должно производиться по технологии, предусмотренной для данного типа носителя, с применением сертифицированных средств гарантированного уничтожения информации (допускается задействовать механизмы затирания встроенные в сертифицированные средства защиты информации).

12.3. Уничтожение носителей производится путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления информации (перед уничтожением, если носитель исправен, должно быть произведено гарантирование стирания информации на носителе). Непосредственные действия по уничтожению конкретного типа носителя должны исключать возможность восстановления информации.

12.4. Бумажные и прочие сгораемые носители (конверты с неиспользуемыми более паролями) уничтожают путем сжигания или с помощью любых бумагорезательных машин.

12.5. По факту уничтожения или стирания носителей составляется акт, в журналах учета делаются соответствующие записи.

12.6. Процедуры стирания и уничтожения осуществляются комиссией, в которую входят: ответственный за эксплуатацию ИСПДн, ответственный за защиту информации, администратор безопасности.

13. Заключительные положения

13.1. Требования настоящего Положения обязательны для всех сотрудников, обрабатывающих конфиденциальную информацию (персональные данные).

13.2. Нарушение требований настоящего Положения влечет за собой ответственность в соответствии с законодательством Российской Федерации.

Приложение 1 к Положению

Журнал
поэкземплярного учета криптосредств, эксплуатационной и технической документации к ним, ключевых документов

	Наименование криптосредства эксплуатационной и технической документации к ним, ключевых документов	Регистрационные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о выдаче	
				От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя криптосредств	Дата и расписка в получении
	2	3	4	5	6	7	8

Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
Ф.И.О. пользователя криптосредств, производившего подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Номера аппаратных средств, в которые установлены или к которым подключены криптосредства	Дата изъятия (уничтожения)	Ф.И.О. пользователя СКЗИ, производившего изъятие (уничтожение)	Номер акта или расписка об уничтожении	
9	10	11	12	13	14	15

Приложение 2 к Положению

Журнал
учета машинных носителей информации

N п/п	Регистрационный (учетный) номер носителя	Вид носителя	Тип носителя и его емкость	Дата поступления	Расписка в получении (Ф.И.О., подпись, дата)	Расписка в обратном приеме (Ф.И.О., подпись, дата)	Место хранения	Дата и номер акта об уничтожении	Примечание
1	2	3	4	5	6	7	8	9	10

Приложение 3 к Положению

Журнал
учета хранилищ

N п/п	Регистрационный (учетный) номер хранилища	Вид хранилища	Дата постановки на учет	Фамилия и подпись принявшего (ответственного), дата	Место расположения (номер помещения)	Дата и номер акта о выводе из эксплуатации	Примечание
	2	3	4	5	6	7	8

Приложение 4 к Положению

Журнал
периодического тестирования средств защиты информации

N п/п	Наименование средства защиты информации от НСД или криптосредства	Регистрационные номера СЗИ от НСД или криптосредства	Дата тестирования	Фамилия и подпись ответственного пользователя, проводившего тестирование	Наименование теста, используемые средства для проведения теста	Результат тестирования (успешный/неуспешный), комментарий	Дата очередного тестирования
	2	3	4	5	6	7	8

Приложение 5 к Положению

Журнал
учета нештатных ситуаций ИСПДн, выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн

N п/п	Дата	Краткое описание выполненной работы (нештатной ситуации)	Ф.И.О. исполнителей и их подписи	Ф.И.О. ответственного за эксплуатацию ПЭВМ, подпись	Подпись специалиста по защите информации	Примечание (ссылка на заявку)
1	2	3	4	5	6	7

Приложение 6 к Положению

Журнал
учета пользователей, допущенных к информационным системам персональных данных

N п/п	Дата	Фамилия, имя, отчество пользователя	Наименование ИСПДн	Подпись пользователя об ознакомлении с Положением и требованиями по безопасности	Подпись администратора безопасности о готовности пользователя к работе в ИСПДн	Примечание
1	2	3	4	5	6	7

Приложение 7 к Положению

Журнал
проверок электронных журналов

N п/п	Дата проверки	Наименование ИСПДн, компьютера, технического средства	Наименование проверяемого журнала	Выявленные нарушения требований безопасности, нештатные ситуации	Подпись администратора безопасности	Примечание
1	2	3	4	5	6	7

Приложение 8 к Положению

Журнал
проверок знаний и навыков пользователей

N п/п	Ф.И.О. должность, пользователя	Дата проведения проверки	Подпись пользователя	Отметка о результатах проведения проверок	Подпись администратора безопасности	Примечание
1	2	3	7	8	9	10

Приложение 9 к Положению

Журнал
регистрации письменных запросов

№ п/п	Вх. N письма	Дата получения запроса	Ф.И.О. гражданина	Сведения о документе, удостоверяющем личность			Отметка о предоставлении доступа к ПДн (отказе в доступе)	Исх. номер и дата письма с ответом на запрос	Ф.И.О., должность, роспись сотрудника, выдавшего ответ	Примечание
				Номер, серия	Дата выдачи	Кем выдан				
1	2	3	4	5	6	7	8	9	10	11

Приложение 10 к Положению

Журнал
регистрации ПДн

N п/п	Исх. N пакета	Дата отправки	Ф.И.О. ответственного сотрудника	Сведения о передаваемых ПДн			Наименование организации получателя	Вх. N пакета	Ф.И.О., должность, роспись сотрудника, принявшего пакет	Примечание
				Количество уникальных записей	Категория ПДн	Цель передачи				
1	2	3	4	5	6	7	8	9	10	11