УТВЕРЖДЕНО
Приказом ГФУ «Инженерные защиты
Чебоксарского водохранилища РМЭ»
от «16» февраля 2017 г. № 18-п

П О Л О Ж Е Н И Е
по организации и проведению работ по обеспечении безопасности персональных данных при их обработке в информационной системе персональных данных ГФУ «Инженерные защиты Чебоксарского водохранилища РМЭ»

Настоящее Положение разработано в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ "О персональных данных", нормативными документами ФСТЭК и ФСБ России, с целью обеспечения защиты прав и свобод граждан при обработке их персональных данных в информационных системах персональных данных.

Для целей настоящего Положения применяются следующие термины и определения:

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

Оператор Персональных данных - ГФУ «Инженерные защиты Чебоксарского водохранилища по РМЭ» (далее - Учреждение) - орган организующий и осуществляющий обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

Технические средства информационной системы персональных данных - средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах;

Пользователь информационной системы персональных данных - лицо, участвующее в функционировании информационной

системы персональных данных или использующее результаты ее функционирования;

Правила разграничения доступа к информационным системам персональных данных - совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа;

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

Распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

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

Несанкционированный доступ (несанкционированные действия) к информационным системам персональных данных - доступ к информации или действия с информацией, нарушающие правила разграничения доступа, в том числе с использованием штатных средств, предоставляемых информационными системами персональных данных.

Защита информации – комплекс организационно-технических мероприятий, направленных на предотвращение потери, искажения и несанкционированного доступа к данным, при этом предусматривается:

разграничение полномочий доступа к данным (C, U, D, R, P, S и др.);

авторизация, контроль и учет действий с данными (регистрация событий);

контроль копирования, печати, обмена данными по каналам связи;

межсетевое экранирование и защита от вирусов;

учет внешних носителей данных;

резервное копирование / восстановление данных;

раздельное хранение носителей данных с резервными копиями;

контроль доступа в помещения и к компьютерам;

применение устройств идентификации пользователей для доступа.

1. Общие положения

Настоящим Положением определяется структура и составляющие безопасности информации в информационной системе персональных данных Учреждения.

Обеспечение безопасности персональных данных (ПДн) при их обработке в автоматизированных системах (информационных системах персональных данных – ИСПДн) достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иные несанкционированные действия.

Мероприятия по обеспечению безопасности ПДн формулируются в зависимости от класса ИСПДн с учетом возможного возникновение угроз безопасности жизненно важным интересам личности, общества и государства.

При обеспечении безопасности ПДн проводятся мероприятия, направленные на:

предотвращение несанкционированного доступа (НСД) к ПДн и (или) передачи их лицам, организациям не имеющим права доступа к такой информации;

своевременного обнаружения фактов НСД к ПДн;

недопущения воздействия на технические средства автоматизированной обработки ПДн, в результате которого может быть нарушено их функционирование;

оперативного резервирования информации в ИСПДн;

возможности незамедлительного восстановления ПДн, модифицированных или уничтоженных вследствие НСД к ним;

постоянного контроля за обеспечением уровня защищенности ПДн.

Обеспечение безопасности ПДн осуществляется путем выполнения комплекса организационных и технических мероприятий, реализуемых в рамках создаваемой системы защиты персональных данных (СЗПДн), в соответствии с утвержденными Требованиями по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных ГФУ «Инженерные защиты Чебоксарского водохранилища по РМЭ» (приложение № 1).

Структура, состав и основные функции СЗПДн определяются исходя из класса ИСПДн. СЗПДн включает организационные меры и технические средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки ПДн), а также используемые в информационной системе информационные технологии.

Под организацией обеспечения безопасности ПДн при их обработке в ИСПДн понимается формирование совокупности осуществляемых на всех стадиях жизненного цикла ИСПДн согласованных по целям, задачам, месту и времени мероприятий, направленных на предотвращение (нейтрализацию) и парирование угроз безопасности ПДн в ИСПДн, на восстановление нормального функционирования ИСПДн после нейтрализации угрозы, с целью минимизации как непосредственного, так и опосредованного ущерба от возможной реализации таких угроз. Обеспечение безопасности ПДн при их обработке в автоматизированных ИСПДн должно проводиться путем выполнения комплекса организационных и технических мероприятий (применения технических средств), в рамках системы (подсистемы) защиты персональных данных, развертываемой в ИСПДн в процессе ее создания или модернизации.

Порядок организации обеспечения безопасности ПДн в ИСПДн предусматривает:

оценку обстановки;

обоснование требований по обеспечению безопасности ПДн и формулирование задач защиты ПДн;

разработку замысла обеспечения безопасности ПДн;

выбор целесообразных способов (мер и средств) защиты ПДн в соответствии с задачами и замыслом защиты;

решение вопросов управления обеспечением безопасности ПДн в динамике изменения обстановки и контроля эффективности защиты;

обеспечение реализации принятого замысла защиты; планирование мероприятий по защите ПДн;

организацию и проведение работ по созданию СЗПДн в рамках разработки (модернизации) ИСПДн, в том числе с привлечением специализированных сторонних организаций к разработке и развертыванию СЗПДн или ее элементов в ИСПДн, решение основных задач взаимодействия, определение их задач и функций на различных стадиях создания и эксплуатации ИСПДн;

разработку документов, регламентирующих вопросы организации обеспечения безопасности ПДн и эксплуатации СЗПДн в ИСПДн.

Мероприятия по обеспечению безопасности персональных данных при их обработке в ИСПДн включают в себя:

а) определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;

б) разработку на основе модели угроз системы защиты ПДн, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты ПДн, предусмотренных для соответствующего класса информационных систем;

в) проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

г) установку и ввод в эксплуатацию разрешенных лицензионных средств защиты информации в соответствии с эксплуатационной и технической документацией;

д) обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

е) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

ж) учет лиц, допущенных к работе с ПДн в информационной системе;

з) контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

и) разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности ПДн или другим нарушениям, приводящим к снижению уровня защищенности ПДн, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

к) описание системы защиты персональных данных.

Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

Для обеспечения безопасности ПДн при их обработке в информационных системах осуществляется защита речевой информации и информации, обрабатываемой техническими средствами, а также информации, представленной в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, магнитно-оптической и иной основе.

По структуре ИСПДн, на которые направлена реализация мероприятий по защите, выделяются следующие классы угроз:

угрозы безопасности ПДн, обрабатываемых в ИСПДн, на базе автоматизированного рабочего места;

угрозы безопасности ПДн, обрабатываемых в ИСПДн на базе локальных информационных систем.

Для обеспечения безопасности ПДн при их обработке в информационных системах проводятся:

обследование и оформление документа о классе информационной системы Учреждения (КЗ), определение способов и состава средств защиты информации (СЗИ), в том числе разработка модели угроз, проектирование;

ввод в эксплуатацию – закупка и инсталляция сертифицированных СЗИ, обучение персонала, издание приказов о допуске персонала и регламентах обработки конфиденциальной информации.

2. Цели обеспечения информационной безопасности

4.1 Стратегической целью обеспечения безопасности информации в ИСПДн является защита интересов субъектов информационных отношений. Данная цель достигается посредством постоянного поддержания следующих свойств информации в процессе ее обработки, хранения и передачи:

целостности информации;

доступности обрабатываемой информации для зарегистрированных пользователей;

конфиденциальности информации;

3. Объект защиты.

Объектом защиты является информационная система персональных данных Учреждения:

а) Информационные ресурсы:

- персональные данные (исходная информация, информационные базы данных);
- инструментальная информация (программное обеспечение), с помощью которой обрабатывается, хранится и передается информация ПДн;

б) Технические информационные системы и средства Учреждения, в которых обрабатывается, хранится и передается информация ПДн;

в) помещения объектов Учреждения, а в которых размещаются информационные ресурсы, и обрабатывается конфиденциальная информация;

г) Технические системы жизнеобеспечения, электропитания, проводного вещания, часофикации, охранной и пожарной сигнализации, обеспечивающие или размещаемые совместно с оборудованием ИСПДн;.

Критичными свойствами объекта защиты являются:

а) возможность разрушения или повреждения информационных систем персональных данных в результате пожара, затопления, аварии инженерных систем жизнеобеспечения;

б) возможность прекращения или нарушения нормального функционирования ИСПДн в результате повреждения отдельных их элементов;

в) несанкционированная доступность информации, выражающаяся в возможности:

- непосредственного доступа к информации, находящейся на первичном или вторичном носителе, в транспортной среде передачи; воздействия на носитель или транспортную среду с целью перлюстрации, отчуждения, копирования, изменения, подмены и уничтожения информации;

-прямого или косвенного доступа к оборудованию ИСПДн; и транспортной среде передачи с целью получения доступа к информации (несанкционированный доступ).

4. Субъекты информационных отношений

4.1 Субъектами информационных отношений являются сотрудники.

4.2 Перечисленные субъекты информационных отношений заинтересованы в обеспечении:

конфиденциальности (сохранения в тайне) информации, в соответствии с требованиями российского законодательства;

достоверности (полноты, точности, адекватности, целостности) информации;

своевременного доступа (за приемлемое для них время) к необходимой им информации;

разграничения ответственности за нарушения законных прав (интересов) других субъектов информационных отношений и установленных правил обращения с информацией;

возможности осуществления непрерывного контроля и управления процессами обработки и передачи информации.

5. Возможные угрозы и участки вторжения

5.1. Общая классификация угроз.

1. Угрозы конфиденциальности данных и программ. Реализуются при несанкционированном доступе к программам, данным, каналам связи, при перехвате электромагнитных излучений, при анализе трафика.

2. Угрозы целостности данных, программ, аппаратуры. Реализуются при несанкционированном уничтожении, модификации данных, порождении фальсифицированных данных, задержке и нарушении маршрутизации данных в каналах связи.

3. Угрозы доступности данных. Реализуются при создании условий, когда законный пользователь или процесс не получает своевременного доступа к данным или ресурсам системы, каналам связи.

4. Угрозы отказа от выполнения транзакций. Реализуются при создании условий легальному пользователю для отказа от выполненной операции по передаче или приему информации.

6. Порядок проведения контрольных мероприятий и действий по его результатам контроля

Контроль заключается в проверке выполнения требований нормативных документов по защите информации, а также в оценке

обоснованности и эффективности принятых мер. Контроль может проводиться Учреждением или на договорной основе сторонними организациями, при наличии лицензии на деятельность по технической защите конфиденциальной информации.

Решение основных вопросов обеспечения защиты ПДн предусматривает подготовку кадров, выделение необходимых финансовых и материальных средств, закупку программного и аппаратного обеспечения.

Приложения:

Приложение №1. Требования по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных ГФУ «Инженерные защиты Чебоксарского водохранилища РМЭ».

Приложение №2. Схема подключений информационно-вычислительной сети (ЛВС) ГФУ «Инженерные защиты Чебоксарского водохранилища РМЭ».

Приложение №3. Сведения о сетевом программном обеспечении информационно-вычислительной сети (ЛВС) ГФУ «Инженерные защиты Чебоксарского водохранилища РМЭ».

Приложение №4. Сведения о базах данных информационно-вычислительной сети в сегменте общей сети ГФУ «Инженерные защиты Чебоксарского водохранилища РМЭ».

Приложение №5. Сведения о клиентском прикладном программном обеспечении информационно-вычислительной сети (ЛВС) ГФУ «Инженерные защиты Чебоксарского водохранилища РМЭ».

Приложение №6. Сведения о программно-технических средствах защиты информационно-вычислительной сети (ЛВС) ГФУ «Инженерные защиты Чебоксарского водохранилища РМЭ».

Приложение №7. Сведения о пользователях систем общего пользования (СОП) ГФУ «Инженерные защиты Чебоксарского водохранилища РМЭ».

Приложение №8. Инструкция по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных ГФУ «Инженерные защиты Чебоксарского водохранилища РМЭ».

Приложение №9. Рекомендации по использованию программных и аппаратных средств защиты информации и обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

ПРИЛОЖЕНИЕ № 1
к Положению по организации и проведению
работ по обеспечении безопасности
персональных данных при их обработке
в информационной системе персональных
данных ГФУ «Инженерные защиты
Чебоксарского водохранилища РМЭ»

Т Р Е Б О В А Н И Я

по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных ГФУ «Инженерные защиты Чебоксарского водохранилища РМЭ»

При организации и осуществлении защиты персональных данных (ПДн) необходимо руководствоваться требованиями нормативных и методических документов по защите информации в автоматизированных системах (информационных системах персональных данных – ИСПДн), учитывая при этом, что ПДн, в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» отнесены к конфиденциальной информации.

При проведении мероприятий по защите ПДн учитывается, что информационные ресурсы подвержены потенциальным внешним и внутренним угрозам, ведущим к потерям конфиденциальности, доступности и целостности информационных ресурсов.

Источники угрозы:

люди (недобросовестные внешние и внутренние пользователи информационных ресурсов);

аварии (ошибки пользователя, ошибки администратора);

отказ аппаратного обеспечения, ошибки программного обеспечения, отказы индустриального оборудования)

природные факторы (стихийные бедствия, астрофизические явления, биологические явления).

Угрозы увеличивают риски безопасности, представляющие собой:

неавторизированный доступ в сеть;

неавторизированное раскрытие информации;

неавторизированную модификацию данных или программного обеспечения;

разрушение функций сети (недоступность данных и сервисов).

Наличие рисков безопасности требуют введения мер безопасности.

Меры безопасности должны гарантировать:

конфиденциальность;

целостность;

доступность информации;

физическую безопасность информации;

контроль доступа к информации.

Информационная безопасность предусматривает:

процедурную (административную и организационную безопасность);

безопасность персонала;

физическую безопасность;

безопасность системы (операции, HW, SW);

безопасность коммуникаций.

Обеспечение безопасности ПДн при их обработке в ИСПДн достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иные несанкционированные действия.

Мероприятия по обеспечению безопасности ПДн проводятся в зависимости от класса ИСПДн с учетом возможного возникновение угроз безопасности жизненно важным интересам субъектам персональных данных.

При обеспечении безопасности ПДн проводятся мероприятия, направленные на:

предотвращение несанкционированного доступа (НСД) к ПДн и (или) передачи их лицам, организациям, не имеющим права доступа к такой информации;

своевременное обнаружение фактов НСД к ПДн;

недопущение воздействия на технические средства автоматизированной обработки ПДн, в результате которого может быть нарушено их функционирование;

оперативного резервирования информации в ИСПДн;

возможность незамедлительного восстановления ПДн, модифицированных или уничтоженных вследствие НСД к ним;

постоянный контроль за обеспечением уровня защищенности ПДн.

Обеспечение безопасности ПДн осуществляется путем выполнения комплекса организационных и технических мероприятий, реализуемых в рамках создаваемой системы защиты персональных данных (СЗПДн).

Структура, состав и основные функции СЗПДн определяются исходя из класса ИСПДн, используемых в учреждении.

СЗПДн включает организационные меры и технические средства защиты, а также используемые в информационной системе информационные технологии.

Под организацией обеспечения безопасности ПДн при их обработке в ИСПДн понимается формирование совокупности осуществляемых на всех стадиях жизненного цикла ИСПДн согласованных по цели, задачам, месту и времени мероприятий, направленных на предотвращение (нейтрализацию) и парирование угроз безопасности ПДн в ИСПДн, на восстановление нормального функционирования ИСПДн после нейтрализации угрозы, с целью минимизации как непосредственного, так и опосредованного ущерба от возможной реализации таких угроз. Обеспечение безопасности ПДн при их обработке в автоматизированных ИСПДн проводится путем выполнения комплекса организационных и технических мероприятий (применения технических средств), в рамках системы (подсистемы) защиты персональных данных, развертываемой в ИСПДн в процессе ее создания или модернизации.

Порядок организации обеспечения безопасности ПДн в ИСПДн предусматривает:

оценку обстановки;

обоснование требований по обеспечению безопасности ПДн и формулирование задач защиты ПДн;

разработку замысла обеспечения безопасности ПДн; выбор целесообразных способов (мер и средств) защиты ПДн в соответствии с задачами и замыслом защиты;

решение вопросов управления обеспечением безопасности ПДн в динамике изменения обстановки и контроля эффективности защиты;

обеспечение реализации принятого замысла защиты;

планирование мероприятий по защите ПДн;

организацию и проведение работ по созданию системы защиты персональных данных (СЗПДн) в рамках разработки (модернизации) ИСПДн, в том числе с привлечением специализированных сторонних организаций к разработке и развертыванию СЗПДн или ее элементов в ИСПДн, решение основных задач взаимодействия, определение их задач и функций на различных стадиях создания и эксплуатации ИСПДн;

разработку документов, регламентирующих вопросы организации обеспечения безопасности ПДн и эксплуатации СЗПДн в ИСПДн.

В интересах технического обеспечения безопасности ПДн при их обработке в ИСПДн в зависимости от класса информационной системы должны быть реализованы мероприятия по защите от НСД к ПДн при их обработке в ИСПДн.

В состав мероприятий по защите ПДн при их обработке в ИСПДн от НСД и неправомерных действий входят следующие мероприятия:

защита от НСД при однопользовательском режиме обработки ПДн;

антивирусная защита.

Мероприятия по защите ПДн реализуются в рамках подсистем: управления доступом, регистрации и учета, обеспечения целостности, криптографической защиты, антивирусной защиты.

Меры безопасности ПДн должны гарантировать:

конфиденциальность;

целостность;

доступность информации;

Мероприятия по обеспечению безопасности предусматривают:

управление доступом;

регистрацию и учет;

обеспечение целостности;

контроль отсутствия недекларированных возможностей;

антивирусную защиту;

обеспечение безопасного межсетевого взаимодействия;

анализ защищенности.

Подсистема управления доступом, регистрации и учета должна реализовываться на базе программных средств блокирования несанкционированных действий, сигнализации и регистрации. Это специальные, не входящие в ядро какой-либо операционной системы программные и программно-аппаратные средства защиты самих операционных систем, электронных баз данных и прикладных программ. Они выполняют функции защиты самостоятельно или в комплексе с другими средствами защиты и направлены на исключение или затруднение выполнения опасных для действий пользователя или нарушителя.

Средства диагностики должны осуществлять тестирование файловой системы и баз данных, постоянный сбор информации о функционировании элементов подсистемы обеспечения безопасности информации.

Средства уничтожения предназначены для уничтожения остаточных данных и должны предусматривать аварийное уничтожение данных в случае угрозы несанкционированного доступа (НСД), которая не может быть блокирована системой.

Подсистема обеспечения целостности должна быть реализована операционными системами и системами управления базами данных. Средства повышения достоверности и обеспечения целостности передаваемых данных и надежности транзакций, встраиваемые в операционные системы и системы управления базами данных, основаны на расчете контрольных сумм, уведомлении о сбое в передаче пакета сообщения, повторе передачи не принятого пакета.

Подсистема контроля отсутствия недекларированных возможностей должна реализовываться на базе систем управления

базами данных, средств защиты информации, антивирусных средств защиты информации.

Для разработки и осуществления мероприятий по обеспечению безопасности персональных данных при их обработке в информационной системе Учреждением или уполномоченным лицом назначается структурное подразделение или должностное лицо (работник), ответственные за обеспечение безопасности персональных данных.

Лица, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения служебных (трудовых) обязанностей должны допускаться к соответствующим персональным данным на основании утвержденных Перечней должностных лиц, допущенных к работе с персональными данными.

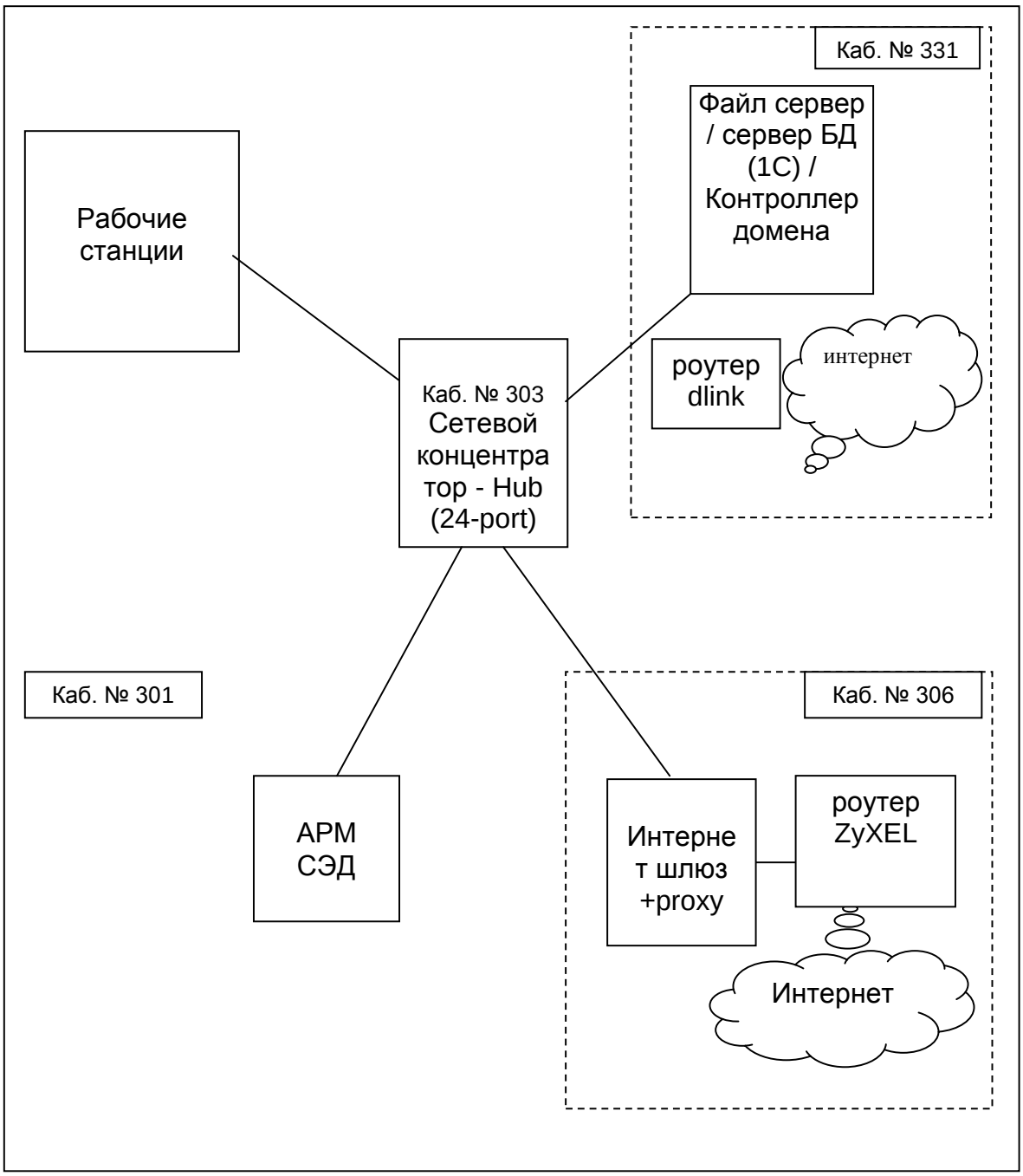
Запросы пользователей информационной системы на получение персональных данных, включая лиц, указанных в утвержденных Перечнях должностных лиц, а также факты предоставления персональных данных по этим запросам должны регистрироваться автоматизированными средствами информационной системы в электронном журнале обращений. Содержание электронного журнала обращений периодически проверяется соответствующими должностными лицами (работниками) Учреждения или уполномоченного лица.

При обнаружении нарушений порядка предоставления персональных данных Учреждения или уполномоченные лица должны незамедлительно приостановить предоставление персональных данных пользователям информационной системы до выявления причин нарушений и устранения этих причин.

При хранении материальных носителей информации с персональными данными (или другой конфиденциальной информацией) должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются Учреждением отдельно.

ПРИЛОЖЕНИЕ № 2
к Положению по организации и проведению
работ по обеспечении безопасности
персональных данных при их обработке
в информационной системе персональных
данных ГФУ «Инженерные защиты
Чебоксарского водохранилища РМЭ»

Схема подключений информационно-вычислительной сети (ЛВС) ГФУ «Инженерные защиты Чебоксарского водохранилища по РМЭ»



Пояснительная записка

1. ЛВС находится в пределах одного здания и занимает один этаж.
2. Количество узлов – 1.
3. Топология – звезда, тип Ethernet 100Base – TX.
4. Участники сети являются источниками и потребителями информации.
5. Сеть – 192.168.100.0, маска подсети 255.255.255.0.
6. Сеть использует стек протоколов TCP/IP.
7. Телекоммуникационные каналы предоставляются согласно договору с провайдером «Волгателеком».
8. Скоростные характеристики: ЛВС – 100 Мбит/с; Интернет (ADSL) – без ограничений скорости.
9. Администрирование и перечень работ определяется администратором информационной безопасности Учреждения.
10. Участники сети, которым необходим доступ в Интернет для выполнения служебных обязанностей, допускаются с разрешения директора Учреждения и имеют свободный доступ в глобальную сеть (с соблюдением требований ограничения доступа).

ПРИЛОЖЕНИЕ № 3
к Положению по организации и проведению
работ по обеспечении безопасности
персональных данных при их обработке
в информационной системе персональных
данных ГФУ «Инженерные защиты
Чебоксарского водохранилища РМЭ»

Сведения о технических средствах информационно-вычислительной сети ГФУ «Инженерные защиты Чебоксарского водохранилища РМЭ»

№	Коммутационное оборудование	Количество, предназначение	Где установлено	Кто устанавливал (договор)	Кто сопровождает (договор)	Страна производитель
1	Сервер	1 шт., хранение БД, файлов; обеспечение пользователей домена	каб. №331	Администратор информационной безопасности Учреждения	Администратор информационной безопасности Учреждения, сервисные центры поставщиков СВТ и ОТ.	Китай
2	Роутер dlink	1 шт. Доступ в интернет (Седна)	каб. №331	Администратор информационной безопасности Учреждения	Администратор информационной безопасности Учреждения, сервисные центры поставщиков СВТ и ОТ.	Китай
3	Сетевой концентратор (Hub)	1 шт., коммутация	каб. №303	Администратор информационно	Администратор информационной	Китай

№	Коммутационное оборудование	Количество, предназначение	Где установлено	Кто устанавливал (договор)	Кто сопровождает (договор)	Страна производитель
		сети		й безопасности Учреждения	безопасности Учреждения, сервисные центры поставщиков СВТ и ОТ.	
4	Роутер zyxel	1 шт., обеспечение доступа к глобальной сети (Ростелеком)	каб. №306	Администратор информационной безопасности Учреждения	Администратор информационной безопасности Учреждения, сервисные центры поставщиков СВТ и ОТ.	Китай
5	Рабочие станции пользователей	21 шт., обработка информации	каб. №301, 302, 303, 304, 305, 306, 307, 320,321,330	Администратор информационной безопасности Учреждения	Администратор информационной безопасностиУчреждения, сервисные центры поставщиков СВТ и ОТ.	Китай
6	Принтеры	8 шт., распечатка документов	каб. №301, 302, 303, 304, 306, 307, 330	Администратор информационной безопасности Учреждения	Администратор информационной безопасности Учреждения, сервисные центры поставщиков СВТ и ОТ.	Китай
7	МФУ HP LaserJet M1522 MFP Series PCL 6	1 шт., распечатка, сканирование и тиражирование	каб. №301	Администратор информационной безопасности Учреждения	Администратор информационной безопасности Учреждения, сервисные центры	Китай

№	Коммутационное оборудование	Количество, предназначение	Где установлено	Кто устанавливал (договор)	Кто сопровождает (договор)	Страна производитель
		документов			поставщиков СВТ и ОТ.	
8	Ксерокс Xerox Workcentre 7132	1 шт., тиражирование документов, печать А3	каб. №306	Администратор информационной безопасности Учреждения	Администратор информационной безопасности Учреждения, сервисные центры поставщиков СВТ и ОТ.	Китай
9	МФУ HP LaserJet Pro MFP 176n	1 шт., распечатка, сканирование и тиражирование документов	каб. №321	Администратор информационной безопасности Учреждения	Администратор информационной безопасности Учреждения, сервисные центры поставщиков СВТ и ОТ.	Китай
10	Копир Canon FC128	1 шт., тиражирование документов,	каб. №304	Администратор информационной безопасности Учреждения	Администратор информационной безопасности Учреждения, сервисные центры поставщиков СВТ и ОТ.	Китай

Пояснительная записка

1. Технические средства (далее - ТС) приобретаются согласно Федеральному закону от 5 апреля 2013 г. N 44-ФЗ "О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд".

2. Ввод в эксплуатацию, ремонт производится поставщиком ТС, подключение ТС к сети осуществляется администратором информационной безопасности Учреждения.

3. Оценка полноты переданного представителями фирмы-производителя, разработчика, продавца эксплуатационной документации на ТС осуществляется администратором информационной безопасности Учреждения.

4. Внесение изменений в телекоммуникационную схему ЛВС производится администратором информационной безопасности Учреждения.

5. ТС проверяется администратором информационной безопасности Учреждения.

6. На этапах установки и настройки, обеспечением безопасности информации занимаются специалисты организации, имеющей лицензию ФСТЭК на техническую защиту конфиденциальной информации.

ПРИЛОЖЕНИЕ № 4
к Положению по организации и проведению
работ по обеспечении безопасности
персональных данных при их обработке
в информационной системе персональных
данных ГФУ «Инженерные защиты
Чебоксарского водохранилища РМЭ»

Сведения о сетевом программном обеспечении
Информационно-вычислительной сети (ЛВС) ГФУ «Инженерные защиты Чебоксарского водохранилища РМЭ»

№	Программное обеспечение	Производитель, страна	Назначение	Кто устанавливал программное обеспечение	Кто сопровождает программное обеспечение	Примечание
1	Microsoft Windows Server 2008 R2	США, Microsoft	Операционная система	Администратор информационной безопасности Учреждения	Администратор информационной безопасности Учреждения	
2	Microsoft Windows 10 pro	США, Microsoft	Операционная система	Администратор информационной безопасности Учреждения	Администратор информационной безопасности Учреждения	
3	Microsoft Windows XP Professional Russian Service Pack 3	США, Microsoft	Сетевые клиенты к серверу	Администратор информационной безопасности Учреждения	Администратор информационной безопасности Учреждения	
4	1С: свод отчетов	Россия, 1С	Сетевые клиенты к серверу	Администратор информационной безопасности	Администратор информационной безопасности	

№	Программное обеспечение	Производитель, страна	Назначение	Кто устанавливал программное обеспечение	Кто сопровождает программное обеспечение	Примечание
				Учреждения	Учреждения	
5	Антивирус DR. Web 11	РФ, Доктор Веб	Антивирусная программа	Администратор информационной безопасности Учреждения	Администратор информационной безопасности Учреждения	
6	1С бухгалтерия 1С зарплата	Россия, 1С	Сетевые клиенты к серверу	Администратор информационной безопасности Учреждения	Администратор информационной безопасности Учреждения	

Пояснительная записка

1. Программное обеспечение (далее ПО) приобретается согласно Федеральному закону от 5 апреля 2013 г. N 44-ФЗ "О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд".

2. Оценка полноты переданного представителями фирмы-производителя, разработчика, продавца эксплуатационной документации на ТС производится администратором информационной безопасности Учреждения.

3. Настройка ПО производится администратором информационной безопасности Учреждения.

4. При появлении новых версий ПО, изменения в ПО вносятся администратором информационной безопасности Учреждения.

5. Предоставление информационных ресурсов производится согласно группам пользователей ОС Windows 2008 Server.

6. В сети используются протоколы из стека протоколов TCP/IP.

7. Сеть – 192.168.100.0, маска подсети 255.255.255.0.

8. Изменения в программное обеспечение может вносить только администратором информационной безопасности Учреждения.

ПРИЛОЖЕНИЕ № 5
к Положению по организации и проведению
работ по обеспечении безопасности
персональных данных при их обработке
в информационной системе персональных
данных ГФУ «Инженерные защиты
Чебоксарского водохранилища РМЭ»

Сведения о базах данных информационно-вычислительной сети в сегменте общей сети ГФУ «Инженерные защиты Чебоксарского водохранилища РМЭ»

№ п/п	Программное обеспечение, где установлено	Разработчик	Кто устанавливал программное обеспечение (№ договора)	Кто сопровождает программное обеспечение (№ договора)	Субъекты доступа, способ разграничения доступа к информации	Категория обрабатываемой информации
1	БД 1С 8.1 Бухгалтерия (на сервере в каб. № 331)	Компания «1 С»	ООО «Все для главбуха» (Договор № 09-36 от 01.01.2009)	ООО «Бизнес решения»	Сотрудники финансово-экономического отдела, бухгалтерии по личному паролю, с разграничением доступа, ОС.	Конфиденциальная: Бухгалтерский учет, персональные данные
2	БД 1С 8.1 Зарплата и кадры (на сервере в каб. № 331)	Компания «1 С»	ООО «Все для главбуха» (Договор № 09-36 от 01.01.2009)	ООО «Бизнес решения»	Сотрудники отдела правового обеспечения, делопроизводства и кадров и Сотрудники финансово-экономического отдела, бухгалтерии по личному паролю, с разграничением доступа, ОС.	Конфиденциальная: Бухгалтерский учет, зарплата, персональные данные

Пояснительная записка

1. Закупка программных средств (баз данных) выполняется в соответствии с Федеральным законом от 5 апреля 2013 г. N 44-ФЗ "О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд". Установка и эксплуатация базы данных (далее - БД) выполняется администратором информационной безопасности Учреждения.

2. Эксплуатационная документация входит в комплект поставки программных средств.

3. Работы по сопровождению выполняются администратором информационной безопасности Учреждения (или сторонней организацией по договору) в соответствии с распоряжениями руководства.

4. Регламентные работы по сопровождению задач выполняются на основании договоров с организациями-поставщиками программных средств.

5. Разграничение доступа пользователей к БД осуществляется в соответствии должностными обязанностями с помощью индивидуального пароля.

6. Описание структур БД входит в комплект документации по эксплуатации программных продуктов.

7. Технологические процессы по организации работ с БД реализуются в зависимости от вида БД:

информационно-правовая система (пользователями БД являются пользователи сети Учреждения);

работы с БД, связанные с профессиональной деятельностью: «1С–предприятие» – финансово-экономическим отделом, бухгалтерией, отделом правового обеспечения, делопроизводства и кадров;

установку и обновление БД выполняет фирма-поставщик программных продуктов;

8. Обязанности лиц, ответственных за защиту информации, эксплуатацию технических и программных средств отражены в должностных регламентах и инструкциях специалистов.

9. Обеспечение неизменности технических и программных средств осуществляется администратором информационной безопасности Учреждения в соответствии с должностными инструкциями.

_____

ПРИЛОЖЕНИЕ № 6
к Положению по организации и проведению
работ по обеспечении безопасности
персональных данных при их обработке
в информационной системе персональных
данных ГФУ «Инженерные защиты
Чебоксарского водохранилища РМЭ»

Сведения о клиентском прикладном программном обеспечении информационно-вычислительной сети (ЛВС) ГФУ «Инженерные защиты Чебоксарского водохранилища РМЭ»

№ п/п	Наименование прикладного программного обеспечения	Производитель, страна	Назначение	Кто устанавливал программное обеспечение	Кто сопровождает программное обеспечение	Примечание
1	Windows XP Professional Edition Rus SP3	США, Microsoft	Операционная система	Администратор информационной безопасности Учреждения	Администратор информационной безопасности Учреждения	
2	Microsoft Windows 10 pro	США, Microsoft	Операционная система	Администратор информационной безопасности Учреждения	Администратор информационной безопасности Учреждения	
2	Microsoft Office 2003 Professional RUS SP3	США, Microsoft	Офисный пакет приложений для работы с документами	Администратор информационной безопасности Учреждения	Администратор информационной безопасности Учреждения	
3	DR. Web 11	РФ	Антивирусная программа	Администратор информационной	Администратор информационной	

№ п/п	Наименование прикладного программного обеспечения	Производитель, страна	Назначение	Кто устанавливал программное обеспечение	Кто сопровождает программное обеспечение	Примечание
				безопасности Учреждения	безопасности Учреждения	
5	Microsoft Office 2007 Professional RUS	США, Microsoft	Офисный пакет приложений для работы с документами	Администратор информационной безопасности Учреждения	Администратор информационной безопасности Учреждения	

Пояснительная записка

1. Программное обеспечение (ПО) приобретается согласно Федеральному закону от 5 апреля 2013 г. N 44-ФЗ "О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд".

2. Оценка полноты переданного представителями фирмы-производителя, разработчика, документации на ПО производится администратором информационной безопасности Учреждения.

3. При появлении новых версий ПО изменения в ПО вносятся администратором информационной безопасности Учреждения.

4. Изменения в программное обеспечение может вносить только администратор информационной безопасности Учреждения.

5. Настройка ПО производится администратором информационной безопасности Учреждения.

ПРИЛОЖЕНИЕ № 7
к Положению по организации и проведению
работ по обеспечении безопасности
персональных данных при их обработке
в информационной системе персональных
данных ГФУ «Инженерные защиты
Чебоксарского водохранилища РМЭ»

Сведения о программно-технических средствах защиты информационно-вычислительной сети (ЛВС) ГФУ «Инженерные защиты Чебоксарского водохранилища РМЭ»

№ п/п	Средства защиты информации	Сертификат безопасности информации	Где установлено	Разработчик СЗИ	Высшая категория защищаемой информации	Кто устанавливал	Кто сопровождает	Примечание
1	Парольная защита сетевой ОС Windows Server 2008 R2	Да	Сервер ГФУ	США, Microsoft	Рабочие документы, БД 1С	Администратор информационной безопасности Учреждения	Администратор информационной безопасности Учреждения	
2	Парольная защита клиентской ОС Windows XP Professional	Да	Рабочие станции пользователей в кабинетах	США, Microsoft	Рабочие документы	Администратор информационной безопасности Учреждения	Администратор информационной безопасности Учреждения	
3	DR. Web 11	Да	Сервера, рабочие станции пользовате	РФ	Рабочие документы, персональные данные	Администратор информационной безопасности Учреждения	Администратор информационной безопасности Учреждения	

№ п/п	Средства защиты информации	Сертификат безопасности информации	Где установлено	Разработчик СЗИ	Высшая категория защищаемой информации	Кто устанавливал	Кто сопровождает	Примечание
			лей					
4	Парольная защита клиентской ОС Windows 10 Professional	Да	Рабочие станции пользователей в кабинетах	США, Microsoft	Рабочие документы	Администратор информационной безопасности Учреждения	Администратор информационной безопасности Учреждения	
5	СКЗИ КриптоПро CSP	Да	Рабочие станции пользователей в кабинетах	Россия, Крипто-Про	Электронная цифровая подпись	Администратор информационной безопасности Учреждения	Администратор информационной безопасности Учреждения	

Пояснительная записка

1. Средства защиты информации (далее – СЗИ) приобретаются согласно Федеральному закону от 5 апреля 2013 г. N 44-ФЗ "О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд".

2. Настройка СЗИ производится администратором информационной безопасности Учреждения.

3. Разграничение доступа пользователей производится с помощью стандартных средств ОС Windows 2008 Server.

4. Изменения в СЗИ производятся только администратором информационной безопасности Учреждения.

ПРИЛОЖЕНИЕ № 8
к Положению по организации и проведению
работ по обеспечении безопасности
персональных данных при их обработке
в информационной системе персональных
данных ГФУ «Инженерные защиты
Чебоксарского водохранилища РМЭ»

Сведения о пользователях систем общего пользования ГФУ «Инженерные защиты Чебоксарского водохранилища РМЭ»

№	Подразделение	Количество допущенных сотрудников	Маршрут физического подключения к СОП	Кто осуществлял подключение	Доступные сервисы	Кто сопровождает пользователей	Примечание
1	Производственно-технический отдел	8	Сетевой концентратор, Шлюз доступа к Интернет, WIFI роутер, телефонная линия, провайдер «Волгателеком»	«Волгателеком»	HTTP, HTTPS, DNS, FTP, POP3, SMTP	Администратор информационной безопасности Учреждения	

№	Подразделение	Количество допущенных сотрудников	Маршрут физического подключения к СОП	Кто осуществлял подключение	Доступные сервисы	Кто сопровождает пользователей	Примечание
2	Финансово-экономический отдел, бухгалтерия	8	Сетевой концентратор, Шлюз доступа к Интернет, WIFI роутер, телефонная линия, провайдер «Волгателеком» «Седна»	«Волгателеком» «Седна»	HTTP, HTTPS, FTP, POP3, SMTP	Администратор информационной безопасности Учреждения	
3	Приемная	1	Сетевой концентратор, Шлюз доступа к Интернет, WIFI роутер, телефонная линия, провайдер «Волгателеком»	«Волгателеком»	HTTP, HTTPS, FTP, POP3, SMTP	Администратор информационной безопасности Учреждения	
4	Главный инженер	1	Сетевой концентратор, Шлюз доступа к Интернет, WIFI роутер, телефонная линия, провайдер «Волгателеком»	«Волгателеком»	HTTP, HTTPS, FTP, POP3, SMTP	Администратор информационной безопасности Учреждения	

№	Подразделение	Количество допущенных сотрудников	Маршрут физического подключения к СОП	Кто осуществлял подключение	Доступные сервисы	Кто сопровождает пользователей	Примечание
5	Ведущий специалист по кадрам	1	Сетевой концентратор, Шлюз доступа к Интернет, WIFI роутер, телефонная линия, провайдер «Волгателеком»	«Волгателеком»	HTTP, HTTPS, FTP, POP3, SMTP	Администратор информационной безопасности Учреждения	
6	Заместитель директора	1	Сетевой концентратор, Шлюз доступа к Интернет, WIFI роутер, телефонная линия, провайдер «Волгателеком»	«Волгателеком»	HTTP, HTTPS, FTP, POP3, SMTP	Администратор информационной безопасности Учреждения	
7	Директор	1	Сетевой концентратор, Шлюз доступа к Интернет, WIFI роутер, телефонная линия, провайдер «Волгателеком»	«Волгателеком»	HTTP, HTTPS, FTP, POP3, SMTP	Администратор информационной безопасности Учреждения	

Приложение № 9
к Положению по организации и проведению
работ по обеспечении безопасности
персональных данных при их обработке
в информационной системе персональных
данных ГФУ «Инженерные защиты
Чебоксарского водохранилища РМЭ»

И Н С Т Р У К Ц И Я

по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных ГФУ «Инженерные защиты Чебоксарского водохранилища по РМЭ»

1. Общие положения:

1.1. Целью настоящей инструкции является регулирование совместной работы сотрудников (далее – пользователей), распределения сетевых ресурсов коллективного пользования и поддержания необходимого уровня защиты информации, ее сохранности и соблюдения прав доступа к информации, установленных ее собственником, в том числе и соблюдения конфиденциальности личной информации.

1.2. По уровню ответственности и правам доступа к ЛВС Учреждения (далее СЕТИ) пользователи разделяются на следующие категории: администраторы безопасности и пользователи.

1.3. **Пользователь компьютера**, подключенного к СЕТИ - лицо за которым закреплена ответственность за данный компьютер. Пользователь компьютера должен принимать все необходимые меры по защите информации на компьютере и контролю за соблюдением прав доступа к информации.

1.3.1. В случае появления у пользователя сведений или подозрений о фактах несанкционированного удаленного доступа к информации, размещенной на контролируемом им компьютере, пользователь должен немедленно сообщить об этом системному администратору.

1.4. **Администратор информационной безопасности** - лицо, обслуживающее сервер, следящее за бесперебойным функционированием СЕТИ и отвечающее за обеспечение безопасности информации в СЕТИ. Администратор информационной безопасности:

обеспечивает сетевую безопасность (защиту от несанкционированного доступа к информации, просмотра или изменения системных файлов и данных);

обеспечивает безопасность межсетевого взаимодействия;

обеспечивает соблюдение требований безопасности при обработке персональных данных;

составляет инструкции по работе с сетевым обеспечением, защите информации и доводит их до сведения пользователей;

ведет журнал системной информации, оформляет иную техническую документацию;

принимает исчерпывающие меры по сохранению данных, в том числе в случае возникновения неполадок в сети, на сервере, в отдельных компьютерах, в том числе обеспечивает своевременное копирование и резервирование данных;

самостоятельно устраняет неполадки в работе оборудования и программного обеспечения сети, сервера, персональных компьютеров;

в случае невозможности устранения неполадок в работе компьютеров, сервера, сети своими силами - обращается к техническому персоналу сторонних организаций, в соответствии с заключенными договорами Учреждения. При этом активно участвует в восстановлении работоспособности указанных систем;

организует доступ к локальной и глобальной сетям;

контролирует использование сетевых ресурсов и дискового пространства, выявляет ошибки пользователей и неполадки сетевого программного обеспечения. Проводит разъяснительную работу. Сообщает своему непосредственному руководителю о случаях злоупотребления сетью и принятых мерах;

обеспечивает почтовое обслуживание, регистрирует пользователей, назначает идентификаторы и пароли, своевременно обновляет данные;

обучает пользователей работе в сети, ведению архивов;

консультирует пользователей по вопросам пользования компьютерами, программами, сетью.

1.4.1. Администратор информационной безопасности информирует пользователей о всех плановых профилактических работах, которые могут привести к частичной или полной неработоспособности СЕТИ на ограниченное время, а также об изменениях предоставляемых сервисов и ограничениях, накладываемых на доступ к ресурсам СЕТИ.

1.4.2. Администратор информационной безопасности дает разрешение на подключение компьютера к СЕТИ. Самовольное подключение является серьезнейшим нарушением правил пользования СЕТЬЮ. Администратор информационной безопасности имеет право отключить компьютер пользователя от СЕТИ в том случае, если с данного компьютера производился несанкционированный доступ к информации, и в случаях других серьезных нарушений настоящей инструкции.

1.4. Все п**ользователи сети** Учреждения должны ознакомиться с настоящей инструкцией.

2. Пользователи СЕТИ обязаны:

2.1. Соблюдать правила работы в СЕТИ, оговоренные настоящей инструкцией.

2.2. Немедленно сообщать администратору информационной безопасности об обнаруженных проблемах в использовании предоставленных ресурсов, а также о фактах нарушения настоящей инструкции кем-либо. Системные администраторы, при необходимости, должны провести расследование указанных фактов, доложить о результатах расследования непосредственному руководителю и принять соответствующие меры.

2.3. Не разглашать известную им конфиденциальную информацию (логины, пароли), необходимую для безопасной работы в СЕТИ, и доступную им информацию по персональным данным. Передача персональных данных возможна и осуществляется только в соответствии с требованиями утвержденного Положения о порядке работы с персональными данными государственных гражданских служащих и работников Учреждения.

2.4. Немедленно отключать от СЕТИ компьютер, который подозревается в заражении вирусом. Компьютер не должен подключаться к СЕТИ до тех пор, пока администратор информационной безопасности не удостоверятся в удалении вируса. По факту заражения вирусом проводится служебное расследование.

2.5. Обеспечивать беспрепятственный доступ администратору информационной безопасности к сетевому оборудованию и компьютерам пользователей.

2.6. Выполнять предписания администратора информационной безопасности, направленные на обеспечение безопасности СЕТИ.

3. Пользователи СЕТИ имеют право:

3.1. Использовать в работе предоставленные им сетевые ресурсы в оговоренных в настоящей инструкцией рамках. При этом администратор информационной безопасности вправе ограничивать доступ к некоторым сетевым ресурсам вплоть до их полной блокировки, изменять распределение трафика и проводить другие меры, направленные на повышение эффективности использования сетевых ресурсов.

3.2. Обращаться за помощью к администратору информационной безопасности при решении задач использования ресурсов СЕТИ.

3.3. Вносить предложения по улучшению работы с ресурсами сети.

4. Пользователям СЕТИ запрещается:

4.1. Разрешать посторонним лицам, не включенным в соответствующие Перечни должностных лиц Учреждения, пользоваться вверенным им компьютером.

4.2. Использовать сетевые программы, не предназначенные для выполнения прямых служебных обязанностей без согласования с системными администраторами.

4.3. Самостоятельно устанавливать или удалять установленные системным администратором сетевые программы на компьютерах,

подключенных к СЕТИ, изменять настройки операционной системы и приложений, влияющие на работу сетевого оборудования и сетевых ресурсов.

4.4. Повреждать, уничтожать или фальсифицировать информацию, не принадлежащую пользователю.

4.5. Вскрывать компьютеры, сетевое и периферийное оборудование; подключать к компьютеру дополнительное оборудование без согласования с администратором информационной безопасности.

4.6. Самовольно подключать компьютер к СЕТИ, а также изменять IP-адрес компьютера, выданный системным администратором. Передача данных в сеть с использованием других IP-адресов в качестве адреса отправителя является распространением ложной информации и создает угрозу безопасности информации на других компьютерах.

4.7. Работать с каналоемкими ресурсами (real video, real audio, chat и др.) без согласования с администратором информационной безопасности. При сильной перегрузке канала вследствие использования каналоемких ресурсов текущий сеанс пользователя, вызвавшего перегрузку, будет приостановлен.

4.8. Использовать иные формы доступа к сети Интернет, за исключением разрешенных администратором информационной безопасности: обходить установленный администратором информационной безопасности брандмауэр при соединении с сетью Интернет с помощью модемов, программ для сетевого туннелирования и других средств.

4.11. Осуществлять попыток несанкционированного доступа к ресурсам СЕТИ, проведение или участие в сетевых атаках и сетевом взломе.

4.12. Использовать СЕТЬ в коммерческих целях.

При работе с электронной почтой:

4.13. Открывать или запускать приложения, полученные по электронной почте от неизвестного источника и (или) не затребованные пользователем.

4.14. Осуществлять массовую рассылку не согласованных предварительно электронных писем. Под массовой рассылкой подразумевается как рассылка множеству получателей, так и множественная рассылка одному получателю (спам).

4.15. Использовать несуществующие обратные адреса при отправке электронных писем.

5. Общие ресурсы сети

5.1. Дисковое пространство серверов Учреждения используется исключительно для хранения информации общего пользования и баз данных.

6. Персональные данные.

6.1. Персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации

физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

6.2. Лица, получающие доступ к персональным данным, должны обеспечивать конфиденциальность таких данных.

6.3. Обеспечение конфиденциальности персональных данных не требуется:

в случае обезличивания персональных данных;

в отношении общедоступных персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес, абонентский номер, сведения о профессии и иные персональные данные, предоставленные субъектом персональных данных.

6.4. При резервном копировании персональных данных обеспечивается учет носителей информации с резервными или рабочими копиями информации. Машинные носители (CD, DVD-диски, др. носители) с данными должны сдаваться в конце рабочего дня ответственному лицу (администратору). При их хранении и использовании должны обеспечиваться меры защиты от несанкционированного доступа и обеспечение сохранности носителей информации.

7. Ответственность

7.1. Пользователь отвечает за информацию, хранящуюся на его персональном компьютере.

7.2. Пользователь несет личную ответственность за весь информационный обмен между его персональным компьютером и другими компьютерами в СЕТИ и за ее пределами.

7.3. Администратор информационной безопасности отвечает за бесперебойное функционирование вверенного ему участка СЕТИ, качество предоставляемых пользователям сервисов, регламентируемую работу системы защиты информации.

7.4. Нарушение данной инструкции, повлекшее уничтожение, блокирование, модификацию либо копирование охраняемых законом данных, нарушение работы компьютеров пользователей, системы или СЕТИ компьютеров, может повлечь административную или уголовную ответственность в соответствии с действующим законодательством Российской Федерации.

Приложение 10
к Положению по организации и проведению
работ по обеспечении безопасности
персональных данных при их обработке
в информационной системе персональных
данных ГФУ «Инженерные защиты
Чебоксарского водохранилища РМЭ»

Р Е К О М Е Н Д А Ц И И

по использованию программных и аппаратных средств защиты информации и обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

Мероприятия по защите ПДн при их обработке в ИСПДн от несанкционированного доступа и неправомерных действий включают в себя:

управление доступом;
регистрацию и учет;
обеспечение целостности;
контроль отсутствия недекларированных возможностей;
антивирусную защиту;
обеспечение безопасного межсетевого взаимодействия ИСПДн;
анализ защищенности;
обнаружение вторжений.

Для выполнения вышеназванных требований, необходимо наличие следующих средств защиты:

средство защиты от Несанкционированного Доступа;
межсетевой экран;
антивирус;

При выборе того или иного средства, основными критериями отбора являются:

наличие сертификатов ФСТЭК, ФСБ
обеспечение необходимого уровня защиты;
производительность;
совместимость;
простота настройки и эксплуатации;
техническая поддержка;
цена.