ДЕПАРТАМЕНТ СЕМЬИ, СОЦИАЛЬНОЙ И ДЕМОГРАФИЧЕСКОЙ ПОЛИТИКИ БРЯНСКОЙ ОБЛАСТИ
ГОСУДАРСТВЕННОЕ КАЗЕННОЕ УЧРЕЖДЕНИЕ БРЯНСКОЙ ОБЛАСТИ
ОТДЕЛ СОЦИАЛЬНОЙ ЗАЩИТЫ НАСЕЛЕНИЯ
БРАСОВСКОГО РАЙОНА

Приказ

28.06.2023 года № 58

п. Локоть

Об утверждении Концепции
информационной безопасности
информационных систем
в государственном казенном учреждении
Брянской области «Отдел социальной
защиты населения Брасовского района»

В соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», со статьями 6,16 Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

ПРИКАЗЫВАЮ:

1.Утвердить прилагаемую Концепцию информационной безопасности информационных систем в государственном казенном учреждении Брянской области «Отдел социальной защиты населения Брасовского района» (далее — Концепция).

2. Ответственному за организацию обработки персональных данных (В.Н. Иваниковой) обеспечить ознакомление работников учреждения с Концепцией.

3. Хоченковой Т. А. обеспечить размещение Концепции на официальном сайте учреждения в информационно-телекоммуникационной сети «Интернет».

4. Местом хранения Концепции определить кабинет ответственного за организацию обработки персональных данных.

5. Приказ вступает в силу со дня его подписания.

6.Контроль за исполнением настоящего приказа возложить на ответственного за организацию обработки персональных данных-заместителя начальника отдела Иваникову В.Н.

Начальник А.В.Гуляева

Утверждена приказом
ГКУ «ОСЗН Брасовского района»

от 28 06 2023 № 58

КОНЦЕПЦИЯ
информационной безопасности информационных систем в государственном казенном учреждении Брянской области «Отдел социальной защиты населения Брасовского района»

1. Общие положения

1.1.Настоящая Концепция определяет основные цели и задачи, а также общую стратегию построения системы защиты персональных данных, используемых в информационных системах государственном казенном учреждении «Отдел социальной защиты населения Брасовского района» (далее – Учреждение).

1.2. Настоящая Концепция определяет основные требования и базовые подходы к реализации системы защиты персональных данных для достижения требуемого уровня безопасности информации.

1.3. Настоящая Концепция разработана в соответствии с системным подходом к обеспечению информационной безопасности. Системный подход предполагает проведение комплекса мероприятий, включающих исследование угроз информационной безопасности и разработку системы защиты персональных данных с позиции комплексного применения технических и организационных мер и средств защиты.

1.4. Под информационной безопасностью персональных данных понимается защищённость персональных данных и обрабатывающей их инфраструктуры от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, её владельцам (субъектам персональных данных) или инфраструктуре. Задачи информационной безопасности сводятся к минимизации ущерба от возможной реализации угроз безопасности персональных данных, а также к прогнозированию и предотвращению таких воздействий.

1.5. Настоящая Концепция является методологической основой для:

формирования и проведения единой политики в области обеспечения безопасности персональных данных в информационных системах Учреждения;

принятия управленческих решений и разработки практических мер для реализации политики безопасности персональных данных и выработки комплекса согласованных мер нормативно-правового, технологического и организационно-технического характера, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз персональных данных;

разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного

обеспечения безопасности персональных данных в информационных системах Учреждения.

2. Построение системы защиты персональных данных в Учреждении

2.1. Система защиты персональных данных представляет собой совокупность организационных и технических мероприятий для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также иных неправомерных действий с ними.

2.2. Безопасность персональных данных достигается путём исключения несанкционированного, в том числе случайного, доступа к ним, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

2.3.Структура, состав и основные функции системы защиты персональных данных определяются исходя из уровня защищённости и класса защищённости информационных систем Учреждения.

2.4. Система защиты персональных данных включает в себя 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 персональных данных), а также используемые в информационной системе информационные технологии.

2.5.Система защиты персональных данных призвана обеспечить:

конфиденциальность информации (защита от несанкционированного ознакомления);

целостность информации (актуальность и непротиворечивость информации, её защищённость от разрушения и несанкционированного изменения);

доступность информации (возможность за приемлемое время получить требуемую информационную услугу).

2.6. Организационные меры как составная часть системы защиты персональных данных включают в себя создание и поддержание правовой базы безопасности персональных данных и разработку (введение в действие) предусмотренных Политикой информационной безопасности информационных систем персональных данных Учреждения.

2.7.Технические средства защиты информации реализуются при помощи соответствующих программно-технических средств и методов защиты. Перечень необходимых мер и средств защиты информации определяется по результатам внутренней проверки обеспечения защиты персональных данных в информационных системах Учреждения.

3. Задачи системы защиты персональных данных в Учреждении

3.1. Основной целью системы защиты персональных данных в Учреждении является минимизация ущерба от возможной реализации угроз безопасности персональных данных.

3.2. Для достижения основной цели система защиты персональных данных информационных систем Учреждении должна обеспечивать эффективное решение следующих задач:

- защиту от вмешательства в процесс функционирования информационных систем посторонних лиц (возможность использования информационных систем Учреждения и доступ к её ресурсам должны иметь только зарегистрированные в установленном порядке пользователи);

- разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам информационных систем Учреждения (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям информационных систем Учреждения для выполнения своих должностных обязанностей), то есть защиту от несанкционированного доступа:

- к информации, циркулирующей в информационных системах Учреждения;

- средствам вычислительной техники информационных систем Учреждения;

аппаратным, программным и криптографическим средствам защиты, используемым в информационных системах Учреждения;

- регистрацию действий пользователей при использовании защищаемых ресурсов информационных систем Учреждения в системных журналах и периодический контроль корректности действий пользователей системы путём анализа содержимого этих журналов;

- контроль целостности (обеспечение неизменности) среды исполнения программ и её восстановление в случае нарушения;

- защиту от несанкционированной модификации и контроль целостности используемых в информационных системах Учреждения программных средств, а также защиту системы от внедрения несанкционированных программ;

- защиту персональных данных от утечки по техническим каналам при их обработке, хранении и передаче по каналам связи;

- защиту персональных данных, хранимых, обрабатываемых и передаваемых по каналам связи, от несанкционированного разглашения или искажения;

- обеспечение живучести криптографических средств защиты информации при компрометации части ключевой системы;

- своевременное выявление источников угроз безопасности персональных данных, причин и условий, способствующих нанесению ущерба субъектам персональных данных, создание механизма оперативного реагирования на угрозы безопасности персональных данных и негативные тенденции;

- создание условий для минимизации и локализации наносимого неправомерными действиями физических и юридических лиц ущерба, ослабления негативного влияния и ликвидация последствий нарушения безопасности персональных данных.

4. Объекты защиты персональных данных в Учреждении

4.1 Объектами защиты персональных данных в Учреждении являются информация, обрабатываемая в информационных системах Учреждения, и технические средства её обработки и защиты.

4.2. Перечень персональных данных, подлежащих защите, определяется в Перечне персональных данных, подлежащих защите в информационных системах Учреждения, утверждаемым приказом по Учреждению.

4.3. Объекты защиты персональных данных в Учреждении включают в себя:

обрабатываемую информацию;
технологическую информацию;
программно-технические средства обработки;
каналы информационного обмена;
помещения, в которых размещены компоненты информационных систем Учреждения.

5. Классификация пользователей информационных систем Учреждения

5.1. Пользователем информационных систем Учреждение является лицо, участвующее в функционировании информационной системы Учреждения или использующее результаты её функционирования.

5.2.Пользователи информационных систем Учреждения делятся на две основные категории:

1) администратор информационной безопасности;
2) пользователь информационной системы.

5.3. Категории пользователей определяются для каждой информационной системы Учреждение.

6. Основные принципы построения системы защиты персональных данных Учреждения

6.1. Построение системы защиты персональных данных в Учреждении и её функционирование должны осуществляться в соответствии со следующими основными принципами:

законность;
системность;
комплексность;
непрерывность;
своевременность;
преемственность и непрерывность совершенствования;
персональная ответственность;
минимизация полномочий;
взаимодействие и сотрудничество;

гибкость системы защиты;
открытость алгоритмов и механизмов защиты;
простота применения средств защиты;
научная обоснованность и техническая реализуемость;
специализация и профессионализм;
обязательность контроля.

6.2. Принцип законности предполагает осуществление защитных мероприятий и разработку системы защиты персональных данных в Учреждении в соответствии с требованиями законодательства в области защиты персональных данных и других нормативных актов по безопасности информации, утверждённых органами государственной власти в пределах их компетенции.

Пользователи информационных систем Учреждения должны быть осведомлены о порядке работы с защищаемой информацией и об ответственности за нарушение режима защиты персональных данных, установленного в Учреждении.

6.3. Системный подход к построению системы защиты персональных данных в Учреждении предполагает учёт всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности персональных данных.

При создании системы защиты персональных данных в Учреждении должны учитываться все слабые и наиболее уязвимые места системы обработки персональных данных, а также характер, возможные объекты и направления атак на систему со стороны нарушителей, пути проникновения в распределённые системы и несанкционированный доступ к информации. Система защиты персональных данных Учреждении должна строиться с учётом не только всех известных каналов проникновения и несанкционированного доступа к информации, но и с учётом возможности появления принципиально новых путей реализации угроз безопасности.

6.4. Комплексное использование методов и средств защиты персональных данных предполагает согласованное применение разнородных средств при построении целостной системы защиты персональных данных, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных её компонентов.

Защита персональных данных должна строиться эшелонировано. Для каждого канала утечки информации и для каждой угрозы безопасности должно существовать несколько защитных рубежей. Создание защитных рубежей осуществляется с учётом того, чтобы для их преодоления потенциальному злоумышленнику требовались профессиональные навыки в нескольких невзаимосвязанных областях.

Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами. Одним из наиболее укреплённых рубежей призваны быть средства криптографической защиты. Прикладной уровень защиты, учитывающий особенности предметной области, представляет внутренний рубеж защиты.

6.5. Принцип непрерывности подразумевает непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла информационных систем Учреждения.

Информационные системы должны находиться в защищённом состоянии на протяжении всего времени их функционирования. В соответствии с этим принципом должны приниматься меры по недопущению перехода информационной системы в незащищённое состояние. Большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная техническая и организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имён, паролей, ключей шифрования, переопределение полномочий и т.п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, для внедрения специальных программных и аппаратных «закладок» и других средств преодоления системы защиты после восстановления её функционирования.

6.6. Принцип своевременности предполагает упреждающий характер мер обеспечения безопасности персональных данных, то есть постановку задач по комплексной защите информационных систем Учреждения и реализацию мер обеспечения безопасности персональных данных на ранних стадиях разработки информационной системы в целом и её системы защиты информации, в частности.

Разработка системы защиты должна вестись параллельно с разработкой и развитием самой защищаемой системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счёте, создать более эффективные (как по затратам ресурсов, так и по стойкости) защищённые системы.

6.7. Принципы преемственности и непрерывности совершенствования мер и средств защиты информации обеспечиваются на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования информационной системы и её системы защиты с учётом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

6.8.Принцип персональной ответственности предполагает возложение ответственности за обеспечение безопасности персональных данных и системы их обработки на каждого сотрудника Учреждения в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей специалистов строится таким образом, чтобы в случае любого нарушения круг виновников был чётко известен или сведён к минимуму.

6.9.Принцип минимизации полномочий означает предоставление пользователям минимальных прав доступа в соответствии с производственной необходимостью, на основе принципа «всё, что не разрешено, запрещено».

Доступ к персональным данным должен предоставляться только в том случае и объёме, если это необходимо специалисту для выполнения его должностных обязанностей.

6.10.Принцип взаимодействия и сотрудничества предполагает создание благоприятной атмосферы в коллективах структурных подразделений, обеспечивающих деятельность информационных систем Учреждения, для снижения вероятности возникновения негативных действий, связанных с человеческим фактором.

6.11.Принцип гибкости системы защиты подразумевает возможность расширения, исключения или замены мер защиты информации на работающей информационной системе без нарушения процесса её нормального функционирования.

6.12. Принцип открытости алгоритмов и механизмов состоит в том, что защита не должна обеспечиваться только за счёт секретности структурной организации и алгоритмов функционирования её подсистем. Знание алгоритмов работы системы защиты не должно давать возможности её преодоления (даже автору). Однако, это вовсе не означает, что информация о конкретной системе защиты должна быть общедоступна.

6.13. Механизмы защиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных в установленном порядке пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций (ввод нескольких паролей и имен и т.д.).

6.14. Информационные технологии, технические и программные средства, средства и меры защиты информации должны быть реализованы на современном уровне развития науки и техники, научно обоснованы с точки зрения достижения заданного уровня безопасности информации и должны соответствовать установленным нормам и требованиям по безопасности персональных данных.

Система защиты персональных данных должна быть ориентирована на решения, возможные риски для которых и меры противодействия этим рискам прошли всестороннюю теоретическую и практическую проверку.

6.15. Принцип специализации и профессионализма предполагает привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности персональных данных, имеющих опыт практической работы и лицензию на право оказания услуг в этой области. Реализация административных мер и эксплуатация средств защиты должна осуществляться профессионально подготовленными специалистами Учреждения.

6.16. Принцип обязательности контроля предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности персональных данных на основе используемых систем и средств защиты информации при совершенствовании критериев и методов оценки эффективности этих систем и средств.

Контроль за деятельностью любого пользователя, каждого средства защиты и в отношении любого объекта защиты персональных данных в Учреждении должен осуществляться на основе применения средств оперативного контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

7. Меры и средства обеспечения требуемого уровня защищённости информационных систем Учреждения

7.1. Обеспечение требуемого уровня защищённости должности достигаться с использованием мер, методов и средств безопасности.

7.2. Все меры обеспечения безопасности информационных систем подразделяются на:

законодательные (правовые);

морально-этические;

организационные (административные);

физические;

технические (аппаратно-программные).

7.3. К законодательным (правовым) мерам обеспечения безопасности информационных систем относятся действующие в Российской Федерации нормативные акты, регламентирующие правила обращения с персональными данными, закрепляющие права и обязанности участников информационных отношений в процессе её обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию персональных данных и являющиеся сдерживающим фактором для потенциальных нарушителей.

Законодательные (правовые) меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями информационных систем.

7.4. К морально-этическим мерам обеспечения безопасности информационных систем относятся нормы поведения, которые традиционно сложились или складываются по мере распространения информационных технологий. Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в Учреждении и снижают вероятность возникновения негативных действий, связанных с человеческим фактором.

7.5. Организационные (административные) меры обеспечения безопасности информационных систем - это меры организационного характера, регламентирующие процессы функционирования информационных систем, использование ресурсов информационных систем, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

7.6. Организационные меры обеспечения безопасности должны предусматривать регламент информационных отношений, исключающих возможность несанкционированных действий в отношении объектов защиты; определять коалиционные и иерархические принципы и методы разграничения доступа к персональным данным; определять порядок работы с программно-математическими и техническими (аппаратными) средствами защиты и криптозащиты и других защитных механизмов; организовать меры противодействия несанкционированного доступа на этапах аутентификации, авторизации, идентификации, обеспечивающих гарантии реализации прав и ответственности субъектов информационных отношений.

7.7.Организационные меры должны состоять из порядка допуска сотрудников Учреждения к использованию ресурсов информационных систем Учреждения; инструкций (пользователя информационной системы,

администратора безопасности) и других документов, регламентирующих порядок функционирования информационных систем в Учреждения.

7.8. Физические меры обеспечения безопасности информационных систем основаны на применении разного рода механических, электро- или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации.

7.9.Физическая защита зданий, помещений, объектов и средств информатизации должна осуществляться путём установления соответствующих постов охраны, с помощью технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими проникновение в здание, помещения посторонних лиц, хищение информационных носителей, самих средств информатизации, исключающими нахождение внутри контролируемой (охраняемой) зоны технических средств разведки.

7.9. Технические (аппаратно-программные) меры обеспечения безопасности информационных систем основаны на использовании различных электронных устройств и специальных программ, входящих в состав информационных систем и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

7.10. В состав системы защиты персональных данных в Учреждении должны быть включены следующие средства:

средства защиты от несанкционированного доступа; средства идентификации (опознавания) и аутентификации (подтверждения подлинности) пользователей информационных систем;

средства разграничения доступа зарегистрированных пользователей системы к ресурсам информационных систем Учреждении; средства обеспечения и контроля целостности программных и информационных ресурсов;

средства оперативного контроля и регистрации событий безопасности; средства защиты от утечки информации по техническим каналам связи и по каналам побочных электромагнитных излучений и наводок;

криптографические и антивирусные средства защиты персональных данных;

программно-аппаратные средства защиты информации.

7.11. применение технических мер обеспечения безопасности информационных систем на основании основных принципов построения системы комплексной защиты информации предполагает, что выполнение перечисленных ниже требований обеспечено организационными (административными) мерами и используемыми физическими средствами защиты:

обеспечена физическая целостность всех компонентов информационных систем;

обеспечен учёт и хранение съёмных носителей информации и их обращение, исключающее хищение, подмену и уничтожение;

обеспечено резервирование технических средств, дублирование носителей информации;

обеспечена электромагнитная развязка между линиями связи и другими цепями вспомогательных технических средств и систем, выходящими за пределы контролируемой зоны, и информационными цепями;

обеспечено использование антивирусных средств защиты от вредоносного программного обеспечения и криптографических средств защиты информации;

обеспечено использование средств защиты информации, позволяющих вести собственные журналы регистрации событий параллельно со встроенными в информационными системами;

обеспечено использование межсетевого экранирования как при использовании программных, так и при использовании аппаратных межсетевых экранов;

каждый пользователь информационных систем имеет уникальное системное имя и минимально необходимые для выполнения ими своих функциональных обязанностей полномочия по доступу к ресурсам информационной системы;

разработка и отладка программ осуществляется за пределами информационных систем на выделенных персональных компьютерах; все изменения конфигурации технических и программных средств информационных систем производятся в строго установленном порядке (регистрируются и контролируются) только на основании распоряжений руководства Учреждения;

сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.) располагается в местах, недоступных для посторонних (специальных помещениях, шкафах, и т.п.);

пользователями информационных систем осуществляется непрерывное управление и административная поддержка функционирования средств защиты.

8. Модель угроз безопасности персональных данных при их обработке в информационных системах Учреждения

8.1.Для информационных систем Учреждение выделяются следующие основные категории угроз безопасности персональных данных:

угрозы от утечки по техническим каналам;
угрозы несанкционированного доступа к информации:

угрозы уничтожения, хищения аппаратных средств информационных систем, носителей информации путём физического доступа к элементам информационных систем;

угрозы хищения, несанкционированной модификации или блокирования информации путём несанкционированного доступа с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий);

угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования информационных систем и средств защиты персональных данных в её составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадёжности

элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера;

угрозы преднамеренных действий внутренних нарушителей;

угрозы несанкционированного доступа по каналам связи.

9. Контроль эффективности системы защиты персональных данных в Учреждении

9.1. Контроль эффективности системы защиты персональных данных должен осуществляться на периодической основе. В Учреждении целью контроля эффективности является своевременное выявление ненадлежащих режимов работы системы защиты персональных данных (отключение средств защиты, нарушение режимов защиты, несанкционированное изменение режима защиты и т.п.), а так же прогнозирование и превентивное реагирование на новые угрозы безопасности персональных данных.

9.2.Контроль эффективности системы защиты персональных данных может проводиться как администратором безопасности информационных систем Учреждения, так и привлекаемыми для этой цели компетентными организациями, имеющими лицензию на этот вид деятельности, а также Федеральной службой по техническому и экспортному контролю Российской Федерации и Федеральной службой безопасности Российской Федерации в пределах их компетенции.

9.3.Контроль может осуществляться администратором безопасности информационных систем Учреждение как с помощью штатных средств системы защиты персональных данных, так и с помощью специальных программных средств контроля.

9.4. Оценка эффективности системы защиты персональных данных проводится с использованием технических и программных средств контроля на предмет соответствия установленным требованиям.

10. Ответственность

10.1. Ответственным за разработку мер защиты персональных данных и контроль за обеспечением безопасности персональных данных является начальник Учреждения (далее – начальник).

10.2. .Начальник может делегировать часть полномочий по обеспечению безопасности персональных данных одному из своих сотрудников.

10.3..При взаимодействии со сторонними организациями в случаях, когда сотрудникам этих организаций предоставляется доступ к персональным данным, обрабатываемым в Учреждении, с этими организациями заключается соглашение о конфиденциальности либо соглашение о соблюдении режима безопасности персональных данных. Подготовка типовых вариантов указанных соглашений осуществляется Учреждением.

11. Ожидаемый эффект от реализации настоящей Концепции

11.1. Реализация настоящей Концепции позволит:

оценить состояние безопасности информации информационных систем Учреждения, выявить источники внутренних и внешних угроз информационной безопасности, определить приоритетные направления предотвращения, отражения и нейтрализации этих угроз;

разработать организационно-распорядительные документы применительно к информационных системам Учреждения;

провести организационно-режимные и технические мероприятия по обеспечению безопасности персональных данных в Учреждении;

обеспечить необходимый уровень безопасности объектов защиты персональных данных в Учреждении.

11.2. Осуществление этих мероприятий обеспечит создание единой и целостной системы информационной безопасности информационных систем персональных данных и создаст условия для её дальнейшего совершенствования.

ДЕПАРТАМЕНТ СЕМЬИ, СОЦИАЛЬНОЙ И ДЕМОГРАФИЧЕСКОЙ ПОЛИТИКИ БРЯНСКОЙ ОБЛАСТИ
ГОСУДАРСТВЕННОЕ КАЗЕННОЕ УЧРЕЖДЕНИЕ БРЯНСКОЙ ОБЛАСТИ
ОТДЕЛ СОЦИАЛЬНОЙ ЗАЩИТЫ НАСЕЛЕНИЯ
БРАСОВСКОГО РАЙОНА

Приказ

5 марта 2024 года № 22

рп. Локоть

О внесении изменения в приказ
от 28 июня 2023 года № 58
«Об утверждении Концпеции
информационной безопасности
информационных систем
в государственном казенном учреждении
Брянской области «Отдел социальной
защиты населения Брасовского района»

В связи с кадровыми изменениями

ПРИКАЗЫВАЮ:

1. Внести в приказ ГКУ «ОСЗН Брасовского района» от 28 июня 2023 года № 58 «Об утверждении Концпеции информационной безопасности информационных систем в государственном казенном учреждении Брянской области «Отдел социальной защиты населения Брасовского района» следующее изменение:

пункт 6 приказа изложить в следующей редакции:

«6. Контроль за исполнением настоящего приказа возложить на ответственного за организацию обработки персональных данных».

2. Контроль за исполнением приказа оставляю за собой.

Начальник отдела А.В.Гуляева