ПРИНЯТО:
Протокол № 1
от «29» 08 2022 г.
заседания педагогического совета
Майского филиала ГБПОУ КБАПК

УТВЕРЖДЕНО:
Приказом № 137-9
от «12» 09 2022г.
Директор филиала
_____А.М. Кунижев

ПОЛОЖЕНИЕ
Об информационной безопасности ИСПДн в
Майском филиале Государственного бюджетного
профессионального образовательного учреждения
«Кабардино-Балкарский агропромышленный
колледж им. Б.Г. Хамдохова»

1. Введение

1.1. Настоящее Положение об информационной безопасности информационной системы персональных данных (далее по тексту – ИСПДн) в Майском филиале Государственного бюджетного профессионального образовательного учреждения «Кабардино-Балкарский агропромышленный колледж им. Б.Г. Хамдохова»является официальным документом, в котором определена система взаимоувязанных понятий и принципов по обеспечению информационной безопасности реализуемых оператором ИСПДн.

1.2. Необходимость разработки Положения обусловлена стремительным расширением сферы применения новейших информационных технологий и процессов в Колледже, при обработке информации вообще, и персональных данных в частности.

1.3. Настоящее Положение определяет основные цели и задачи, а также общую стратегию построения системы защиты персональных данных (далее по тексту - СЗПДн). Положение определяет основные требования и базовые подходы к их реализации, для достижения требуемого уровня безопасности информации.

1.4. Положение разработано в соответствии с системным подходом к обеспечению информационной безопасности. Системный подход предполагает проведение комплекса мероприятий, включающих исследование угроз информационной безопасности и разработку системы защиты ПДн, с позиции комплексного применения технических и организационных мер и средств защиты.

1.5. Под информационной безопасностью персональных данных (далее по тексту - ПДн) понимается защищенность персональных данных и обрабатывающей их инфраструктуре от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам (субъектам ПДн) или инфраструктуре. Задачи информационной безопасности сводятся к минимизации ущерба от возможной реализации угроз безопасности ПДн, а также к прогнозированию и предотвращению таких воздействий.

1.6. Положение служит основой для разработки комплекса организационных и технических мер по обеспечению информационной безопасности Колледжа, а также нормативных и методических документов, обеспечивающих ее реализацию, и не предполагает подмены функций государственных органов власти Российской Федерации, отвечающих за обеспечение безопасности информационных технологий и защиту информации.

1.7. Положение является методологической основой для: 1.7.1. Формирования и проведения единой политики в области обеспечения безопасности ПДн в ИСПДн Колледжа;

1.7.2. Принятия управленческих решений и разработки практических мер по воплощению политики безопасности ПДн и выработки комплекса согласованных мер нормативно-правового, технологического и организационно-технического характера, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз ПДн;

1.7.3. Координации деятельности структурных подразделений Колледжа при проведении работ по развитию и эксплуатации ИСПДн с соблюдением требований обеспечения безопасности ПДн;

1.7.4. Разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения безопасности ПДн в ИСПДн Колледжа.

1.8. Область применения Положения распространяется на подразделения филиала колледжа, эксплуатирующие технические и программные средства ИСПДн, в которых осуществляется автоматизированная обработка ПДн.

1.9. Правовой базой для разработки настоящего Положения служат требования действующих в России законодательных и нормативных документов по обеспечению безопасности персональных данных.

2. Общие положения

2.1. Настоящее Положение определяет основные цели и задачи, а также общую стратегию построения системы защиты персональных данных (СЗПДн) филиала колледжа, в соответствии с Перечнем ИСПДн. Положение определяет основные требования и базовые подходы к их реализации, для достижения требуемого уровня безопасности информации.

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

2.3. Безопасность персональных данных 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 иных несанкционированных действий.

2.4. 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.

2.5. Эти меры призваны обеспечить:

2.5.1. Конфиденциальность информации (защита от несанкционированного ознакомления);

2.5.2. Целостность информации (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);

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

2.6. Организационные меры предусматривают создание и поддержание правовой базы безопасности ПДн и разработку (введение в действие) предусмотренных Политикой информационной безопасности ИСПДн следующих организационно- распорядительных документов:

2.6.1. План мероприятий по обеспечению защиты ПДн при их обработке в ИСПДн;

2.6.2. Порядок резервирования и восстановления работоспособности ТС и ПО, баз данных и СЗИ;

2.6.3. Должностная инструкция пользователя ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн.

2.7. Технические меры защиты реализуются при помощи соответствующих программно-технических средств и методов защиты.

2.8. Перечень необходимых мер защиты информации определяется по результатам внутренней проверки безопасности ИСПДн Колледжа.

3. Задачи СЗПДн

3.1. Основной целью СЗПДн является минимизация ущерба от возможной реализации угроз безопасности ПДн.

3.2. Для достижения основной цели система безопасности ПДн ИСПДн должна обеспечивать эффективное решение следующих задач:

3.2.1. Защиту от вмешательства в процесс функционирования ИСПДн посторонних лиц (возможность использования информационной системой и доступ к ее ресурсам должны иметь только зарегистрированные установленным порядком пользователи);

3.2.2. Разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам ИСПДн (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям ИСПДн для выполнения своих служебных обязанностей), то есть защиту от несанкционированного доступа:

- к информации, циркулирующей в ИСПДн;
- средствам вычислительной техники ИСПДн;
- аппаратным, программным и криптографическим средствам защиты, используемым в ИСПДн;

3.2.3. Контроль целостности (обеспечение неизменности) среды исполнения программ и ее восстановление в случае нарушения;

3.2.4. Защиту от несанкционированной модификации и контроль целостности используемых в ИСПДн программных средств, а также защиту системы от внедрения несанкционированных программ;

3.2.5. Защиту ПДн от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи;

3.2.6. Защиту ПДн, хранимой, обрабатываемой и передаваемой по каналам связи, от несанкционированного разглашения или искажения;

3.2.7. Своевременное выявление источников угроз безопасности ПДн, причин и условий, способствующих нанесению ущерба субъектам ПДн, создание механизма оперативного реагирования на угрозы безопасности ПДн и негативные тенденции;

3.2.8. Создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности ПДн.

4. Перечень информационных систем

4.1. В Колледже производится обработка персональных данных в информационных системах обработки персональных данных. Перечень ИСПДн определяется на основании приказа филиала колледжа.

5. Объекты защиты

5.1. Объектами защиты являются - информация, обрабатываемая в ИСПДн, и технические средства ее обработки и защиты. Перечень персональных данных, подлежащие защите, определен в Положении о персональных данных, подлежащих защите в ИСПД.

5.2. Объекты защиты включают:

5.2.1. Обрабатываемая информация.

5.2.2. Технологическая информация.

5.2.3. Программно-технические средства обработки.

5.2.4. Средства защиты ПДн.

5.2.5. Каналы информационного обмена.

5.2.6. Объекты и помещения, в которых размещены компоненты ИСПДн.

6. Классификация пользователей ИСПДн

6.1. Пользователем ИСПДн является лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования. Пользователем ИСПДн является любой сотрудник филиала колледжа, имеющий доступ к ИСПДн и ее ресурсам в соответствии с установленным порядком, в соответствии с его функциональными обязанностями.

6.2. Пользователи ИСПДн:

6.2.1. Оператор ИСПДн - сотрудники подразделений филиала колледжа, участвующие в процессе эксплуатации ИСПДн. Оператор ИСПДн - сотрудник обладает следующим уровнем доступа: - обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн; - располагает конфиденциальными данными, к которым имеет доступ.

6.3. Категории пользователей должны быть определены для каждой ИСПДн. Должно быть уточнено разделение сотрудников внутри категорий, в соответствии с типами пользователей определенными в Политике информационной безопасности.

7. Основные принципы построения системы комплексной защиты информации

7.1. Построение системы обеспечения безопасности ПДн ИСПДн Колледжа и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

7.2. Законность. Предполагает осуществление защитных мероприятий и разработку СЗПДн филиала колледжа в соответствии с действующим законодательством в области защиты ПДн и других нормативных актов по безопасности информации, утвержденных органами государственной власти и управления в пределах их компетенции. Пользователи и обслуживающий персонал ПДн ИСПДн Колледжа должны быть осведомлены о порядке работы с защищаемой информацией и об ответственности за защиты ПДн.

7.3. Системность. Системный подход к построению СЗПДн филиала колледжа предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности ПДн ИСПДн Колледжа. При создании системы защиты должны учитываться все слабые и наиболее уязвимые места системы обработки ПДн, а также характер, возможные объекты и направления атак на систему со стороны нарушителей (особенно высококвалифицированных злоумышленников), пути проникновения в распределенные системы и НСД к информации. Система защиты должна строиться с учетом не только всех известных каналов проникновения и НСД к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

7.4. Комплексность. Комплексное использование методов и средств защиты предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов. Создание защитных рубежей осуществляется с учетом 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 укрепленных рубежей призваны быть средства криптографической защиты, реализованные с использованием технологии VPN. Прикладной уровень защиты, учитывающий особенности предметной области, представляет внутренний рубеж защиты.

7.5. Непрерывность защиты ПДн. Защита ПДн - не разовое мероприятие и не простая совокупность проведенных мероприятий и установленных средств защиты, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла ИСПДн. ИСПДн должны находиться в защищенном состоянии на протяжении всего времени их функционирования. В соответствии с этим принципом должны приниматься меры по недопущению перехода ИСПДн в незащищенное состояние.

7.6. Своевременность. Предполагает упреждающий характер мер обеспечения безопасности ПДн, то есть постановку задач по комплексной защите ИСПДн и реализацию мер обеспечения безопасности ПДн на ранних стадиях разработки ИСПДн в целом и ее 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 счете, создать более эффективные (как по затратам ресурсов, так и по стойкости) защищенные системы.

7.7. Преемственность и совершенствование. Предполагают постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования ИСПДн и ее системы защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

7.8. Персональная ответственность. Предполагает возложение ответственности за обеспечение безопасности ПДн и системы их обработки на каждого сотрудника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей сотрудников строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

7.9. Доступ к ПДн должен предоставляться только в том случае и объеме, если это необходимо сотруднику для выполнения его должностных обязанностей.

7.10. Взаимодействие и сотрудничество. Предполагает создание благоприятной атмосферы в коллективах подразделений, обеспечивающих деятельность ИСПДн Колледжа, для снижения вероятности возникновения негативных действий, связанных с человеческим фактором. В такой обстановке сотрудники должны осознанно соблюдать установленные правила и оказывать содействие в деятельности подразделений технической защиты информации.

7.11. Гибкость системы защиты ПДн. Принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения возможности варьирования уровнем защищенности, средства защиты должны обладать определенной гибкостью. Особенно важным это свойство является в тех случаях, когда установку средств защиты необходимо осуществлять на работающую систему, не нарушая процесса ее нормального функционирования.

7.12. Открытость алгоритмов и механизмов защиты. Суть принципа открытости алгоритмов и механизмов защиты состоит в том, что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможности ее преодоления (даже авторам). Однако это не означает, что информация о конкретной системе защиты должна быть общедоступна.

7.13. Простота применения средств защиты. 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 установленным порядком пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций (ввод нескольких паролей и имен и т.д.). Должна достигаться автоматизация максимального числа действий пользователей ИСПДн.

7.14. Научная обоснованность и техническая реализуемость. 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 ПДн. СЗПДн должна быть ориентирована на решения, возможные риски для которых и меры противодействия этим рискам прошли всестороннюю теоретическую и практическую проверку.

7.15. Специализация и профессионализм. Предполагает привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности ПДн, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области.

7.16. Обязательность контроля. Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности ПДн 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 должен осуществляться на основе применения средств оперативного контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

8. Меры, методы и средства обеспечения требуемого уровня защищенности

8.1. Обеспечение требуемого уровня защищенности должности достигаться с использованием мер, методов и средств безопасности. Перечень выбранных мер обеспечения безопасности отражается в Плане внутреннего контроля по обеспечению защиты персональных данных. Все меры обеспечения безопасности ИСПДн подразделяются на:

8.1.1. Законодательные (правовые) меры защиты. К правовым мерам защиты относятся действующие в стране законы, указы и нормативные акты, регламентирующие правила обращения с ПДн, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования.а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию ПДн и являющиеся сдерживающим фактором для потенциальных нарушителей. Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом системы.

8.1.2. Морально-этические меры защиты. К морально-этическим мерам относятся нормы поведения, которые традиционно сложились или складываются по мере распространения ЭВМ

в стране или обществе. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормативные акты, однако, их несоблюдение ведет обычно к падению авторитета, престижа человека, группы лиц или организации. Морально-этические нормы бывают как неписаные (например, общепризнанные нормы честности, патриотизма и т.п.), так и писаные, то есть оформленные в некоторый свод (устав) правил или предписаний. Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективах подразделений. Морально-этические меры защиты снижают вероятность возникновения негативных действий, связанных с человеческим фактором.

8.1.3. Организационные и административные меры защиты. Организационные и административные меры защиты - это меры организационного характера, регламентирующие процессы функционирования ИСПДн, использование ресурсов ИСПДн, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с ИСПДн таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации. Главная цель административных мер, предпринимаемых на высшем управленческом уровне - сформировать Политику информационной безопасности ПДн (отражающую подходы к защите информации) и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел. Реализация Политики информационной безопасности ПДн в ИСПДн состоят из мер административного уровня и организационных (процедурных) мер защиты информации. К административному уровню относятся решения руководства, затрагивающие деятельность ИСПДн в целом. Эти решения закрепляются в Политике информационной безопасности. Политика верхнего уровня должна четко очертить сферу влияния и ограничения при определении целей безопасности ПДн, определить какими ресурсами (материальные, персонал) они будут достигнуты и найти разумный компромисс между приемлемым уровнем безопасности и функциональностью ИСПДн. На организационном уровне определяются процедуры и правила достижения целей и решения задач Политики информационной безопасности ПДн.

8.1.4. Физические меры защиты. Физические меры защиты 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. Физическая защита зданий, помещений, объектов и средств информатизации должна осуществляться путем 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.

8.1.5. Аппаратно-программные средства защиты ПДн. Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ, входящих в состав ИСПДн 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.).

8.2. Контроль эффективности СЗПДн должен осуществляется на периодической основе. Целью контроля эффективности является своевременное выявление ненадлежащих режимов работы СЗПДн (отключение средств защиты, нарушение режимов защиты,

несанкционированное изменение режима защиты и т.п.), а также прогнозирование и превентивное реагирование на новые угрозы безопасности ПДн.

8.3. Контроль может проводиться как администраторами безопасности ИСПДн (оперативный контроль в процессе информационного взаимодействия в ИСПДн), так и привлекаемыми для этой цели компетентными организациями, имеющими лицензию на этот вид деятельности, а также ФСТЭК России и ФСБ России в пределах их компетенции.

8.4. Контроль может осуществляться администратором безопасности как с помощью штатных средств системы защиты ПДн, так и с помощью специальных программных средств контроля.

8.5. Оценка эффективности мер защиты ПДн проводится с использованием технических и программных средств контроля на предмет соответствия установленным требованиям.

8.6. Ответственным за разработку мер и контроль над обеспечением безопасности персональных данных является руководитель Колледжа. Руководитель может делегировать часть полномочий по обеспечению безопасности персональных данных.

8.7. Сфера ответственности руководителя включает следующие направления обеспечения безопасности ПДн:

8.7.1. Планирование и реализация мер по обеспечению безопасности ПДн; 8.7.2. Анализ угроз безопасности ПДн;

8.7.3. Разработку, внедрение, контроль исполнения и поддержание в актуальном состоянии политик, руководств, концепций, процедур, регламентов, инструкций и других организационных документов по обеспечению безопасности;

8.7.4. Контроль защищенности ИТ инфраструктуры Колледжа от угроз ИБ путем;

8.7.5. Обучение и информирование пользователей ИСПДн, о порядке работы с ПДн и средствами защиты;

8.7.6. Предотвращение, выявление, реагирование и расследование нарушений безопасности ПДн.

9. Модель нарушителя безопасности

9.1. Под нарушителем в Колледже понимается лицо, которое в результате умышленных или неумышленных действий может нанести ущерб объектам защиты.

9.2. Нарушители подразделяются по признаку принадлежности к ИСПДн. Все нарушители делятся на две группы:

9.2.1. Внешние нарушители - физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн;

9.2.2. Внутренние нарушители - физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПДн.

9.3. Классификация нарушителей представлена в Модели угроз безопасности персональных данных каждой ИСПДн.

10. Модель угроз безопасности

10.1. Для ИСПДн Колледжа выделяются следующие основные категории угроз безопасности персональных данных:

10.1.1. Угрозы от утечки по техническим каналам.

10.1.2. Угрозы несанкционированного доступа к информации:

10.1.2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн.

10.1.2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно- математических воздействий).

10.1.2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз не антропогенного (сбоев аппаратуры из- за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.

10.1.2.4. Угрозы преднамеренных действий внутренних нарушителей.

10.1.2.5. Угрозы несанкционированного доступа по каналам связи.

10.2. Описание угроз, вероятность их реализации, опасность и актуальность представлены в Модели угроз безопасности персональных данных каждой ИСПДн. 11. Механизм реализации

11.1. Реализация должна осуществляться на основе перспективных программ и планов, которые составляются на основании и во исполнение:

- федеральных законов в области обеспечения информационной безопасности и защиты информации; - постановлений Правительства Российской Федерации;

- руководящих, организационно-распорядительных и методических документов ФСТЭК России;

- потребностей ИСПДн в средствах обеспечения безопасности информации.

12. Ожидаемый эффект от реализации

12.1. Реализация безопасности ПДн в ИСПДн позволит:

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

- разработать распорядительные и нормативно-методические документы применительно к ИСПДн;

- провести классификацию, аттестацию ИСПДн;

- провести организационно-режимные и технические мероприятия по обеспечению безопасности ПДн в ИСПДн;

- обеспечить необходимый уровень безопасности объектов защиты.

12.2. Осуществление этих мероприятий обеспечит создание единой, целостной и скоординированной системы информационной безопасности ИСПДн и создаст условия для ее дальнейшего совершенствования.