Национальный медицинский исследовательский центр
имени В. А. Алмазова
Федеральное государственное бюджетное учреждение
«НМИЦ им. В. А. Алмазова» Минздрава России

Политика информационной безопасности Информационных систем персональных данных ФГБУ «НМИЦ им В. А. Алмазова» Минздрава России

г. Москва
2023 г.

СОДЕРЖАНИЕ

1 ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

В настоящем документе использованы следующие сокращения:

ИБ – Информационная безопасность

ИС – Информационная система

СУИБ – Система управления информационной безопасностью

НТС ИТ – Научно-технический совет по информационным технологиям

СЗПД – Система защиты персональных данных

ИСПДн – Информационные системы персональных данных

2 ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Термины и определения, используемые в настоящей Политике и рекомендуемые к использованию в нормативных и организационно-распорядительных документах, созданных на её основе, приведены в Приложении № 1 «Термины и определения».

3 ВВЕДЕНИЕ

Настоящая Политика информационной безопасности (далее — Политика) ФГБУ «НМИЦ им. В. А. Алмазова» Минздрава России (далее — Центра) разработана в соответствии с требованиями Федерального закона «О персональных данных» от 27 июля 2006 г. № 152-ФЗ на основании:

«Методических рекомендаций для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости», утверждённых Директором Департамента информатизации Министерства здравоохранения и социального развития 23.12.2009 г. и согласованных с начальником 2 Управления ФСТЭК России 22.12.2009 г., и является официальным документом.

В Политике определены требования к персоналу ИСПДн, степень ответственности персонала, структура и необходимый уровень защищенности, статус и должностные обязанности сотрудников, ответственных за обеспечение безопасности персональных данных в ИСПДн Центра.

4 ОБЩИЕ ПОЛОЖЕНИЯ

При разработке настоящей Политики учтены требования и рекомендации следующих Целью настоящей Политики является обеспечение безопасности объектов защиты Центра от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности ПДн (УБПДн).

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.

Построение подсистемы информационной безопасности автоматизированной системы и ее функционирование осуществляется в соответствии с основными принципами:

Законность. Предполагает осуществление защитных мероприятий и разработку подсистемы информационной безопасности ИСПДн в соответствии с законодательством в области информации, информационных технологий и защиты информации, руководящими документами Минздрава России, ФСБ России и ФСТЭК России, а также в соответствии с внутренними документами Центра.

Системность. Системный подход к построению подсистемы информационной безопасности в ИСПДн предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности информации в ИСПДн.
При создании подсистемы информационной безопасности ИСПДн должны учитываться все слабые и наиболее уязвимые места системы поиска, сбора, хранения, обработки, предоставления, распространения ПДн, возможности появления принципиально новых путей реализации угроз информационной безопасности.

Комплексность. Комплексное использование методов и средств защиты АС предполагает согласованное применение разнородных средств при построении целостной подсистемы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов.

Непрерывность защиты. Защита ПДн — непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла АС, начиная с ранних стадий проектирования, разработки, испытания, внедрения и эксплуатации автоматизированных систем (подсистем).

Своевременность. Предполагает упреждающий характер мер обеспечения безопасности информации, то есть постановку задач по комплексной защите АС и реализацию мер обеспечения безопасности информации на ранних стадиях разработки АС в целом и ее подсистемы защиты информации.

В частности разработка подсистемы защиты ПДн должна вестись параллельно с разработкой и развитием самой информационной системы.

Преемственность и совершенствование. Предполагают постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования АС 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.

Разумная достаточность (экономическая целесообразность, сопоставимость возможного ущерба и затрат). Предполагает соответствие уровня затрат на обеспечение безопасности ПДн, ценности информационных ресурсов и величине возможного ущерба от их разглашения, утраты, утечки, уничтожения и искажения. Используемые меры и средства обеспечения безопасности информационных ресурсов не должны заметно ухудшать эргономические показатели работы АС, в которой эта информация циркулирует.

Важно правильно выбрать тот достаточный уровень защиты, при котором затраты, риск и размер возможного ущерба были бы сведены до минимума (задача анализа риска).

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

Принцип минимизации полномочий. Означает предоставление работникам Центра, привлекаемым специалистам минимальных прав доступа в соответствии со служебной или производственной необходимостью. Доступ к информации должен предоставляться только в объеме, необходимом работнику Центра (привлекаемому специалисту) для выполнения его должностных обязанностей.

Гибкость системы 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.

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). Это, однако, не означает, что информация о конкретной системе защиты должна быть общедоступна.

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.

Обязательность контроля. Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных политик (правил) обеспечения безопасности ПДн, на основе используемых систем и средств защиты информации, при совершенствовании критериев и методов оценки эффективности этих систем и средств. Контроль над 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.

Политика призвана обеспечить и постоянно поддерживать следующие свойства информации в ИСПДн:

Целостность и аутентичность информации, хранимой и обрабатываемой в ИСПДн.

Своевременное обнаружение и реагирование на УБПДн.

Конфиденциальность информации ограниченного доступа и служебной информации, хранимой и обрабатываемой СВТ.

Доступность хранимой и обрабатываемой информации для законных пользователей (устойчивого функционирования ИСПДн, при котором пользователи имеют возможность получения необходимой информации и результатов решения задач за приемлемое для них время).

Предоставить обзор требований к информационной безопасности ИСПДн и к отдельным ее компонентам.

Описать действия над существующими подсистемами и планируемые изменения в них с целью приведения к соответствию указанным требованиям.

Описать правила поведения и ответственность пользователей, имеющих доступ к ИСПДн.

5 НОРМАТИВНЫЕ ССЫЛКИ

Основными нормативно-правовыми и методическими документами, на которых базируется настоящая Политика, являются:

1. Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных» (далее — ФЗ «О персональных данных»), устанавливающий основные принципы и условия обработки ПДн, права, обязанности и ответственность участников отношений, связанных с обработкой ПДн.
2. «Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденное Постановлением Правительства РФ от 15.09.2008 г. № 687.
3. Постановления Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
4. Приказ ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
5. «Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных», утвержденные Постановлением Правительства РФ от 06.07.2008 г. № 512.

6 ОБЛАСТЬ ДЕЙСТВИЯ

Настоящий документ определяет политику информационной безопасности на объекте информатизации Центра. Положения документа распространяются на все информационные системы, средства коммуникаций и помещения объекта информатизации, и обязательны для исполнения всеми работниками Центра (штатными, временными, работающими по контракту и т. п.), а также всеми прочими лицами (подрядчиками, аудиторами и т. п.).

7 СИСТЕМА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Система защиты персональных данных (СЗПДн), строится на основании:

- положений законодательства Российской Федерации,
- нормативно-методических документов ФСБ России и ФСТЭК России,
- отчёта о результатах проведения внутренней проверки,
- перечня персональных данных, подлежащих защите,
- акта классификации информационных систем персональных данных,
- модели угроз безопасности персональных данных,
- положения о разграничении прав доступа к обрабатываемым ПДн.

На основании этих документов определяется необходимый уровень защищенности ПДн каждой ИСПДн Центра. На основании анализа актуальных угроз безопасности ПДн описанного в Модели угроз и Отчета о результатах проведения внутренней проверки, делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн. Выбранные необходимые мероприятия отражаются в Плане мероприятий по обеспечению защиты ПДн.

Для каждой ИСПДн должен быть составлен список используемых технических средств защиты, а так же программного обеспечения участвующего в обработке ПДн, на всех элементах ИСПДн:

- АРМ пользователей,
- сервера приложений,
- СУБД,
- граница ЛВС,

- каналов передачи в сети общего пользования и (или) международного обмена, если по ним передаются ПДн.

В зависимости от уровня защищенности ИСПДн и актуальных угроз, СЗПДн могут включать следующие технические средства:

- антивирусные средства для рабочих станций пользователей и серверов,
- средства межсетевого экранирования,
- средства криптографической защиты информации, при передаче защищаемой информации по каналам связи.

Так же, в список должны быть включены функции защиты, обеспечиваемые штатными средствами обработки ПДн операционными системами (ОС), прикладным ПО и специальными комплексами, реализующими средства защиты. Список функций защиты может включать:

- управление и разграничение прав доступа пользователей,
- регистрацию и учет действий с информацией,
- обеспечивать целостность данных,
- производить поиск обнаружения вторжений.

Список используемых технических средств отражается в «Плане мероприятий по обеспечению защиты персональных данных». Список используемых средств должен поддерживаться в актуальном состоянии. При изменении состава технических средств защиты или элементов ИСПДн, соответствующие изменения должны быть внесены в Список и утверждены директором Центра или лицом, ответственным за обеспечение защиты ПДн.

Настоящий документ определяет политику информационной безопасности на объекте информатизации Центра. Положения документа распространяются на все информационные системы, средства коммуникаций и помещения объекта

информатизации, и обязательны для исполнения всеми работниками Центра (штатными, временными, работающими по контракту и т. п.), а также всеми прочими лицами (подрядчиками, аудиторами и т. п.).

8 ТРЕБОВАНИЯ К ПОДСИСТЕМАМ СЗПДН

СЗПДн включают в себя следующие подсистемы:

- управления доступом, регистрации и учета,
- обеспечения целостности и доступности,
- антивирусной защиты,
- межсетевого экранирования,
- физической безопасности,
- анализа защищенности,
- обнаружения вторжений,
- криптографической защиты.

Подсистемы СЗПДн имеют различный функционал в зависимости от класса ИСПДн, определенного в Акте классификации информационной системы персональных данных.

8.1. Подсистемы управления доступом, регистрации и учета

Подсистема управления доступом, регистрации и учета предназначена для реализации следующих функций:

- идентификации и проверка подлинности субъектов доступа при входе в ИСПДн;
- идентификации терминалов, узлов сети, каналов связи, внешних устройств по логическим именам;
- идентификации программ, томов, каталогов, файлов, записей, полей записей по именам;

- регистрации входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее останова.
- регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам;
- регистрации попыток доступа программных средств к терминалам, каналам связи, программам, томам, каталогам, файлам, записям, полям записей.

Подсистема управления доступом может быть реализована с помощью штатных средств обработки ПДн (операционных систем, приложений и СУБД). Так же может быть внедрено специальное техническое средство или их комплекс средств, осуществляющих дополнительные меры по аутентификации и контролю. Например, применение единых хранилищ учетных записей пользователей и регистрационной информации, использование биометрических и технических (с помощью электронных пропусков) мер аутентификации и других.

Свободный доступ к информации не допускаются, за исключением случаев предоставления общедоступных сервисов, к которым предъявляются следующие требования:

- для свободного доступа может быть предоставлена исключительно, общедоступная распространяемая информация;
- контроль за правомерностью предоставления той или иной информации в общий доступ осуществляется администратором безопасности;
- свободный доступ к файлам может быть предоставлен только на чтение;
- серверные приложения должны быть сконфигурированы таким образом, чтобы ответные информационные сообщения при попытках внешнего подключения не содержали информации о версиях программных продуктов.

8.2. Подсистема обеспечения целостности и доступности

Подсистема обеспечения целостности и доступности ПДн, программных и аппаратных средств ИСПДн Центра предназначена для защиты от случайного или преднамеренного изменения или уничтожения и включают в себя реализацию следующих мер:

- на каждом автоматизированном рабочем месте должно быть установлено антивирусное программное обеспечение, включающее:
  — антивирусный сканер;
  — резидентный антивирусный монитор;
  — система антивирусной защиты электронной почты (там, где используется ЭП);
  — дисковый ревизор, осуществляющий контроль целостности критических файлов с использованием контрольных сумм (при необходимости);
  — сигнатуры антивирусных баз должны обновляться ежедневно, как правило, в автоматическом режиме;
  — должна проводиться регулярная проверка программ и данных в системах, поддерживающих критически важные информационные и технологические процессы. Наличие случайных файлов и несанкционированных исправлений должно быть расследовано;
  — запрещается использование неучтенных съемных накопителей (незарегистрированных или неизвестного происхождения). Все съемные накопители перед каждым подключением подлежат проверке на наличие вирусов;
- для администраторов должны быть доступны следующие данные (перечисленные ниже данные должны сохраняться в файлах системных журналов в автоматическом режиме с целью последующего анализа):
  а) идентификатор пользователя, который последний входил в систему;
  б) дата и время последнего входа и выхода из системы;

в) число неудачных попыток входа в систему.
— функции администратора, связанные с назначением прав и полномочий пользователей, не должны быть доступны пользователям и процессам;
— контроль целостности программных и информационных ресурсов должен обеспечиваться как минимум одним из следующих способов:
а) средствами подсчёта и анализа контрольных сумм;
б) средствами электронной цифровой подписи;
в) средствами сравнения критичных ресурсов с их эталонными копиями.
— не допускается работа пользователя (в т. ч. администратора) на АРМ другого пользователя без разрешения администратора безопасности ИСПДн. Работа пользователей на рабочих станциях администраторов без контроля с их стороны не допускается.

Подсистема реализуется с помощью организации резервного копирования обрабатываемых данных, а также резервированием ключевых элементов ИСПДн.

8.3. Подсистема антивирусной защиты

Подсистема антивирусной защиты предназначена для обеспечения антивирусной защиты серверов и АРМ пользователей ИСПДн Центра.

Средства антивирусной защиты предназначены для реализации следующих функций:

- резидентный антивирусный мониторинг,
- антивирусное сканирование,
- скрипт-блокирование,
- централизованную/удаленную установку/деинсталляцию антивирусного продукта, настройку, администрирование, просмотр отчетов и статистической информации по работе продукта,

- автоматизированное обновление антивирусных баз
- ограничение прав пользователя на остановку исполняемых задач и изменения настроек антивирусного программного обеспечения,
- автоматический запуск сразу после загрузки операционной системы.

Подсистема реализуется путем внедрения специального антивирусного программного обеспечения на все элементы ИСПДн.

8.4. Подсистема межсетевого экранирования

Межсетевые экраны (МЭ) обеспечивают безопасность при осуществлении электронного обмена информацией с другими взаимодействующими автоматизированными системами и внешними сетями, разграничение доступа между сегментами корпоративной сети, а также защиту от проникновения и вмешательства в работу АС нарушителей из внешних систем. Согласно Руководящему документу Гостехкомиссии при Президенте РФ «межсетевым экраном называется локальное (однокомпонентное) или функционально-распределенное средство (комплекс), которое реализует контроль за информацией, поступающей в автоматизированную систему и/или выходящей из нее, и обеспечивает защиту автоматизированной системы посредством фильтрации информации, т. е. анализа по совокупности критериев и принятия решения об ее распространении в (из) автоматизированной системе». Однако такое определение имеет общий характер и подразумевает слишком расширенное толкование.

Подсистема межсетевого экранирования предназначена для реализации следующих функций:

- фильтрации открытого и зашифрованного (закрытого) IP-трафика по установленным параметрам;
- фиксации во внутренних журналах информации о проходящем открытом и закрытом IP-трафике;

- идентификации и аутентификацию администратора межсетевого экрана при его локальных запросах на доступ;
- регистрации входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова;
- контроля целостности своей программной и информационной части;
- фильтрации пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;
- фильтрации с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов;
- регистрации и учета запрашиваемых сервисов прикладного уровня;
- блокирования доступа неидентифицированного объекта или субъекта, подлинность которого при аутентификации не подтвердилась, методами, устойчивыми к перехвату;
- контроля за сетевой активностью приложений и обнаружения сетевых атак.

Подсистема реализуется внедрением программно-аппаратных комплексов межсетевого экранирования на границе ЛВС, классом не ниже 3-го уровня защищённости (для специальной категории ПДн).

8.5. Физическая безопасность

Физические меры защиты предназначены для создания физических препятствий на возможных путях проникновения потенциальных нарушителей на объекты Центра, к компонентам Системы и доступа к защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации.

Для разграничения доступа в помещения, где располагается серверное оборудование и другие критически важные объекты ИСПДн, целесообразно

(необходимо) использовать системы физической защиты, позволяющие регистрировать и контролировать доступ исполнителей и посторонних лиц, основанные на методах идентификации и аутентификации (например: магнитные и электронные карты с личными данными, биометрические характеристики работников и т.д.).

Эксплуатация АРМ и серверов должна осуществляться в помещениях, оборудованных надежными автоматическими замками, средствами сигнализации и постоянно находящимися под охраной или наблюдением, исключающим возможность бесконтрольного проникновения в помещения посторонних лиц и обеспечивающим физическую сохранность находящихся в помещении информационных и материальных ресурсов (АРМ, документов, реквизитов доступа и т. п.).

Размещение и установка АРМ и серверов должна исключать возможность визуального просмотра вводимой (выводимой) информации лицами, не имеющими к ней отношения. Уборка помещений, в которых хранится информация ограниченного доступа и/или служебная информация, должна производиться в присутствии ответственного, за которым закреплено данное помещение, с соблюдением мер, исключающих доступ посторонних лиц к защищаемым ресурсам.

Для хранения служебных документов и машинных носителей с защищаемой информацией помещения снабжаются сейфами и металлическими шкафами. Помещения должны быть обеспечены средствами уничтожения документов.

Для обеспечения должного уровня безопасности и для предотвращения вредоносных действий запрещается работать в одиночку (без надлежащего контроля) с критически важными компонентами Системы.

Персоналу, осуществляющему техническое обслуживание обеспечивающих систем (энергоснабжения, сантехники и др.) и сервисов, должен быть предоставлен доступ в защищенные области только в случае необходимости и после получения разрешения.

В нерабочее время защищенные области должны быть физически недоступны и периодически проверяться охраной.

Серверные комнаты, помещения содержащие средства хранения данных и компьютерные залы, поддерживающие критически важные сервисы Центра, должны иметь надежную физическую защиту. При выборе и обустройстве соответствующих помещений необходимо принять во внимание возможность повреждения оборудования в результате пожара, наводнения, взрывов, гражданских беспорядков и других аварий. Следует также рассмотреть угрозы безопасности, которые представляют соседние помещения.

Необходимо соблюдать следующие меры безопасности:

- разместить ключевые (критически важные) системы подальше от общедоступных мест и мест прохождения общественного транспорта;
- элементы здания не должны привлекать внимание и выдавать свое назначение (по возможности); не должно быть явных признаков как снаружи, так и внутри здания, указывающих на присутствие вычислительных ресурсов;
- внутренние телефонные справочники не должны указывать на местонахождение ИСПДн;
- опасные и горючие материалы следует хранить в соответствии с инструкциями на безопасном расстоянии от ИСПДн и критически важных помещений. Не следует хранить расходные материалы для компьютеров в компьютерных залах (например, бумагу для принтеров);

- резервное оборудование и носители информации, на которых хранятся резервные копии, следует разместить на безопасном расстоянии, чтобы избежать их повреждение в случае аварии на основном рабочем месте;
- следует установить соответствующее сигнальное и защитное оборудование, например, тепловые и дымовые детекторы, пожарную сигнализацию, средства пожаротушения, а также предусмотреть пожарные лестницы. Сигнальное и защитное оборудование необходимо регулярно проверять в соответствии с инструкциями производителей. Работники должны быть надлежащим образом подготовлены к использованию этого оборудования;
- процедуры реагирования на чрезвычайные ситуации должны быть документированы, доведены до работников и регулярно тестироваться.

8.6. Подсистема анализа защищенности

Подсистема анализа защищенности, должна обеспечивать выявления уязвимостей, связанных с ошибками в конфигурации ПО ИСПДн, которые могут быть использованы нарушителем для реализации атаки на систему.

Контроль эффективности защиты осуществляется с целью своевременного выявления и предотвращения утечки информации по техническим каналам, за счет несанкционированного доступа к ней, а также предупреждения возможных специальных воздействий, направленных на уничтожение информации или нарушение нормального функционирования средств обработки и передачи информации.

Средства анализа защищенности, так называемые сканеры безопасности (security scanners), помогают определить факт наличия уязвимости на узлах корпоративной сети и своевременно устранить их (до того, как ими воспользуются злоумышленники).

Средства анализа защищенности выполняют серию тестов по обнаружению уязвимостей, аналогичных тем, которые применяют злоумышленники при подготовке и осуществлении атак на корпоративные сети. Поиск уязвимостей основывается на использовании базы данных, которая содержит признаки известных уязвимостей сетевых сервисных программ и может обновляться путем добавления новых описаний уязвимостей. Сканирование начинается с получения предварительной информации о системе, например, о разрешенных протоколах и открытых портах, о версиях операционных систем и т.п., и может заканчиваться попытками имитации проникновения, используя широко известные атаки, например, «подбор пароля».

Средства анализа защищенности сетевых сервисов (служб)

Наиболее распространёнными являются средства анализа защищенности сетевых сервисов (служб) и протоколов. Связано это, в первую очередь, с универсальностью используемых протоколов. Изученность и повсеместное использование таких протоколов, как IP, TCP, HTTP, FTP, SMTP и т.п. позволяют с высокой степенью эффективности проверять защищенность информационной системы, работающей в сетевом окружении.

Использование в сетях Internet/Intranet протоколов TCP/IP, которые характеризуются наличием в них неустранимых уязвимостей, привело к появлению в последнее время новых разновидностей информационных воздействий на сетевые службы и представляющих реальную угрозу защищенности информации. Средства анализа защищенности сетевых служб применяются для оценки защищенности компьютерных сетей по отношению к внутренним и внешним атакам. По результатам анализа защищенности сетевых сервисов этими средствами генерируются отчеты, включающие в себя список обнаруженных уязвимостей, описание связанных с ними возможных угроз и рекомендации по их устранению.

Средства анализа защищенности операционных систем

Вторыми по распространенности являются средства анализа защищенности операционных систем (например, UNIX и Windows NT). Однако, из-за того, что каждый производитель вносит в операционную систему свои изменения (ярким примером является множество разновидностей ОС UNIX), средства анализа защищенности ОС анализируют в первую очередь общие параметры, характерные для всего семейства одной ОС. И лишь для некоторых систем анализируются специфичные для нее параметры.

Средства этого класса предназначены для проверки настроек операционных систем, влияющих на их защищенность. К таким настройкам можно отнести параметры учетных записей пользователей (account), например длину пароля и срок его действия, права пользователей на доступ к критичным системным файлам, уязвимые системные файлы, установленные patch 'и («заплаты») и т.п.

Данные системы в отличие от средств анализа защищенности сетевого уровня проводят сканирование не снаружи, а изнутри анализируемой системы и не предполагают имитацию атак внешних злоумышленников. Кроме возможностей по обнаружению уязвимостей некоторые системы анализа защищенности на уровне ОС позволяющие автоматически устранять часть обнаруженных проблем или корректировать параметры системы, не удовлетворяющие политике безопасности, принятой в Центре.

Средства анализа защищенности операционных систем позволяют осуществлять ревизию механизмов разграничения доступа, идентификации и аутентификации, средств мониторинга, аудита и других компонентов операционных систем с точки зрения соответствия их настроек правилам, установленным в организации. Кроме этого, средствами данного класса проводится контроль целостности и неизменности программных средств и системных установок и проверка наличия уязвимостей системных и прикладных служб. Как правило, такие проверки проводятся с использованием базы данных уязвимостей операционных систем и сервисных служб, которые могут обновляться по мере выявления новых

уязвимостей. Системы анализа защищенности на уровне ОС могут быть использованы не только отделами защиты информации, но и управлениями автоматизации для контроля конфигурации операционных систем.

Анализ защищённости СУБД (Database Scanner)

Система анализа защищенности Database Scanner предназначена для решения одного из важных аспектов управления сетевой безопасностью — обнаружения уязвимостей. Система Database Scanner обнаруживает различные проблемы, связанные с безопасностью баз данных: «слабые» пароли, права доступа к объектам БД. Встроенная база знаний (Knowledge Base), доступная непосредственно из создаваемых отчетов, рекомендует корректирующие действия, которые позволяют устранить обнаруженные уязвимости.

Система Database Scanner может быть использована для анализа защищенности систем управления базами данных (СУБД) Microsoft SQL Server, Oracle и Sybase Adaptive Server. Большинство нарушений безопасности связано с неправильной конфигурацией или нарушениями принятой политики безопасности. Функционал подсистемы может быть реализован программными и программно-аппаратными средствами.

8.7. Подсистема обнаружения вторжений

Подсистема обнаружения вторжений, должна обеспечивать выявление сетевых атак на элементы ИСПДн подключенные к сетям общего пользования и (или) международного обмена.

Функционал подсистемы может быть реализован программными и программно-аппаратными средствами.

8.8. Подсистема криптографической защиты

Подсистема криптографической защиты предназначена для исключения НСД к защищаемой информации в ИСПДн Центра, при ее передаче по каналам связи сетей общего пользования и (или) международного обмена.

Подсистема реализуется внедрения криптографических программно-аппаратных комплексов.

9 ПОЛЬЗОВАТЕЛИ ИСПДН

Пользователи ИСПДН, используемые в настоящей Политике и рекомендуемые к использованию в нормативных и организационно-распорядительных документах, созданных на её основе, приведены в Приложении № 2 «Пользователи ИСПДН».

10 ТРЕБОВАНИЯ К ПЕРСОНАЛУ ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ПДН

Все сотрудники Центра, являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.

При вступлении в должность нового сотрудника непосредственный начальник подразделения, в которое он поступает, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.

Сотрудник должен быть ознакомлен со сведениями настоящей Политики, принятых процедур работы с элементами ИСПДн и СЗПДн.

Сотрудники Центра, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать НСД к ним, а также возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

Сотрудники Центра должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).

Сотрудники Центра должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования по безопасности ПДн и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

Сотрудникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а также записывать на них защищаемую информацию.

Сотрудникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами Центра, третьим лицам.

При работе с ПДн в ИСПДн сотрудники Центра обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ или терминалов.

При завершении работы с ИСПДн сотрудники обязаны защитить АРМ или терминалы с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

Сотрудники Центра должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили принятые политику и процедуры безопасности ПДн.

Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, могущих повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности ПДн.

11 ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЕЙ ИСПДН

Должностные обязанности пользователей ИСПДн описываются в следующих документах:

- Инструкция администратора ИСПДн;
- Инструкция администратора безопасности ИСПДн;
- Инструкция пользователя ИСПДн;
- Инструкция пользователя при возникновении внештатных ситуаций.

Приложение № 1
к Политике информационной безопасности ФГБУ
«НМИЦ» им. В. А. Алмазова» Минздрава России

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Аудит информационной безопасности – систематический, независимый и документируемый процесс получения свидетельств деятельности по обеспечению информационной безопасности и установлению степени выполнения критериев информационной безопасности, а также допускающий возможность формирования профессионального аудиторского суждения о состоянии информационной безопасности организации (ГОСТ Р 53114-2008).

Аутентификация пользователя – подтверждение того, что пользователь соответствует заявленному.

Безопасность информации (данных) – Состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность (ГОСТ Р 53114-2008).

Безопасность информационной технологии – Состояние защищенности информационной технологии, при котором обеспечиваются безопасность информации, для обработки которой она применяется, и информационная безопасность информационной системы, в которой она реализована (ГОСТ Р 53114-2008).

Блокирование информации (данных) – временное прекращение сбора, систематизации, накопления, использования, распространения информации, в том числе её передачи.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на

информацию или ресурсы информационных систем.

Доступ к информации (данным) – возможность получения и использования информации (данных).

Защищаемая информация (защищаемые данные) – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов (ГОСТ Р 53114-2008).

Идентификация риска – процесс обнаружения, распознавания и описания рисков (ГОСТ Р 53114-2008).

Информационная безопасность – защищенность информационных систем (информации и обрабатывающей её инфраструктуры) от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам или инфраструктуре.

Примечания:

1) По ГОСТ Р ИСО/МЭК 27002-2012: **Информационная безопасность** – защита конфиденциальности, целостности и доступности информации; кроме того, сюда могут быть отнесены и другие свойства, например аутентичность, подотчетность, неотказуемость и надежность.

2) По ГОСТ Р 53114-2008: **Информационная безопасность организации** – состояние защищенности интересов организации в условиях угроз в информационной сфере.

Информационная инфраструктура – совокупность объектов информатизации, обеспечивающая доступ потребителей к информационным ресурсам (по ГОСТ Р 53114-2008).

Информационные процессы – **п**роцессы создания, сбора, обработки,

накопления, хранения, поиска, передачи и уничтожения информации.

Информационные ресурсы – документы и массивы документов, содержащиеся в информационных системах (библиотеках, архивах, фондах, банках данных, информационных системах других видов).

Информационная система – система, представляющая собой совокупность информации, а также информационных технологий и технических средств, позволяющих осуществлять обработку информации с использованием средств автоматизации или без использования таких средств.

Информационные технологии – процессы и методы создания, поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Инцидент информационной безопасности – любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность (по ГОСТ Р 53114-2008).

Примечание:

Инцидентами ИБ являются, в частности:

- утрата услуг, оборудования или устройств;
- системные сбои или перегрузки;
- ошибки пользователей;
- несоблюдение политики или рекомендаций по ИБ;
- нарушение физических мер защиты;
- неконтролируемые изменения систем;
- сбои программного обеспечения и отказы технических средств;
- нарушение правил доступа.

Источник угрозы безопасности – субъект доступа, материальный

объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Конфиденциальность информации (данных) – обязательное для соблюдения требование не допускать распространения информации без согласия владельца информации или наличия иного законного основания.

Конфиденциальная информация (данные, сведения) – документированная информация, доступ к которой ограничивается в соответствии с законодательством. К конфиденциальным относятся сведения:

а) о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные);

б) составляющие тайну следствия и судопроизводства;

в) служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с ГК РФ и федеральными законами (служебная тайна);

г) связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией РФ и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и

т.д.);

д) связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с ГК РФ и федеральными законами (коммерческая тайна);

е) о сущности изобретения, исследования, разработки, модели или промышленного образца до официальной публикации информации о них.

Меры обеспечения ИБ – совокупность действий, направленных на разработку и/или практическое применение способов и средств обеспечения информационной безопасности.

Мониторинг ИБ – Непрерывное наблюдение за состоянием и поведением объектов ИБ с целью их контроля, оценки и прогноза в рамках управления ИБ.

Нарушитель ИБ – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности информации при её обработке техническими средствами в информационных системах.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемы информационными системами.

Носитель информации (данных) – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обработка информации (данных) – действия (операции) с информацией, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), блокирование, уничтожение информации.

Объект доверия – объект, в отношении которого необходима уверенность в его безопасности.

Примечание:

Примерами объектов доверия в области ИБ являются: система, сервис (услуга) безопасности, процесс, используемые для обеспечения ИБ.

Объект доступа – единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.

Объект защиты информации – информация либо носитель информации, или информационный процесс, которую (который) необходимо защищать в соответствии с целью защиты информации (ГОСТ Р 53114-2008).

Объект информатизации – совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены (ГОСТ Р 53114-2008).

Оценка риска – процесс, объединяющий идентификацию риска, анализ риска и их количественную оценку (ГОСТ Р 53114-2008).

Политика – общее намерение и направление, официально выраженное руководством (ГОСТ Р ИСО/МЭК 27002-2012).

Технические средства информационных систем – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки информации (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражированиядокументов 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 – лицо, участвующее в функционировании информационной системы либо использующее результаты ее функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программное воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Распространение информации (данных) – действия, направленные на передачу информации определенному кругу лиц или на ознакомление с информацией неограниченного круга лиц, в том числе обнародование в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к информации каким-либо иным способом.

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Риск – сочетание вероятности события и его последствий (ГОСТ Р ИСО/МЭК 27002-2012). Применительно к ИБ, риск – сочетание вероятности нанесения ущерба и тяжести этого ущерба.

Роль ИБ – **с**овокупность прав, привилегий и ограничений на

использование ресурсов корпоративной информационной системы, предоставляемая работникам и третьим лицам для выполнения ими функциональных обязанностей.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки информации, способных функционировать самостоятельно или в составе других систем.

Субъект доступа – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Система защиты информации (данных) – совокупность организационных и технических мероприятий для защиты информации от неправомерного или случайного доступа, уничтожения, изменения,

блокирования, копирования, распространения, а также иных неправомерных действий с ней.

Третья сторона – лица или организация, которые признаны независимыми от участвующих сторон, по отношению к рассматриваемой проблеме (ГОСТ Р ИСО/МЭК 27002-2012).

Угрозы безопасности информации (данных) – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к информации, результатом которого может стать её уничтожение, изменение, блокирование, копирование, распространение, а также иных несанкционированных действий при её обработке в информационных системах.

Уязвимость – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

Целостность информации (данных) – способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях её случайного и (или) преднамеренногоискажения (разрушения).

Приложение № 2к
Политике информационной безопасности ФГБУ
«НМИЦ» им. В. А. Алмазова» Минздрава России

ПОЛОЖЕНИЕ О ПОЛЬЗОВАТЕЛЯХ ИСПДН

В Концепции информационной безопасности ФГБУ «НМИЦ им. В. А. Алмазова» Минздрава России (гл. 4) определены основные категории пользователей. На основании этих категорий производится типизация пользователей ИСПДн, определяя их уровень доступа и возможности.

В ИСПДн Центра можно выделить следующие группы пользователей, участвующих в обработке и хранении ПДн:

- администратор ИСПДн;
- администратор безопасности;
- оператор АРМ;
- администратор сети;
- технического специалиста по обслуживанию периферийного оборудования;
- программист-разработчик ИСПДн.

Данные о группах пользователях, уровне их доступа и информированности отражается в Положении о разграничении прав доступа к обрабатываемым персональным данным.

Уровень полномочий пользователя определяется в соответствии с должностным регламентом, при этом должны соблюдаться следующие требования:

- каждый работник пользуется только предписанными ему правами по отношению к информации, с которой ему необходима работа в соответствии с должностным регламентом;

- пользователи, допущенные к работе, и обслуживающий персонал Системы несут персональную ответственность за нарушения установленного порядка автоматизированной обработки ПДн, правил хранения, использования и передачи, находящихся в их распоряжении защищаемых ресурсов Системы.

Аппаратно-программная конфигурация АРМ пользователей (с которой возможен доступ к защищаемым ресурсам), должна соответствовать кругу возложенных на пользователей функциональных обязанностей.

Все неиспользуемые в работе устройства ввода-вывода информации (USB, COM, LPT порты, дисководы НГМД, DVD и CD-ROM, RW и т.д.) на АРМ должны быть отключены, не нужные для работы программные средства и данные с дисков АРМ должны быть удалены.

5.1. Администратор ИСПДн

Администратор ИСПДн, сотрудник Центра, ответственный за настройку, внедрение и сопровождение ИСПДн. Обеспечивает функционирование подсистемы управления доступом ИСПДн и уполномочен осуществлять предоставление и разграничение доступа конечного пользователя (Оператора АРМ) к элементам, хранящим персональные данные.

Администратор ИСПДн обеспечивает автоматическое введение файлов журналов, отражающих все действия пользователя в отношении механизмов обеспечения информационной безопасности.

Администратор ИСПДн обладает следующим уровнем доступа и знаний:

- обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;
- обладает полной информацией о технических средствах и конфигурации ИСПДн;

- имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;
- обладает правами конфигурирования и административной настройки технических средств ИСПДн.

5.2. Администратор безопасности

Администратор безопасности, сотрудник Центра, ответственный за функционирование СЗПДн.

Администратор безопасности обладает следующим уровнем доступа и знаний:

- обладает правами Администратора ИСПДн;
- обладает полной информацией об ИСПДн;
- имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн;
- не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).

Администратор безопасности уполномочен:

- реализовывать политики безопасности в части настройки СКЗИ, межсетевых экранов и систем обнаружения атак, в соответствии с которыми пользователь (оператор АРМ) получает возможность работать с элементами ИСПДн;
- осуществлять аудит средств защиты;
- устанавливать доверительные отношения своей защищенной сети с сетями других Учреждений.

Администратор безопасности обязан:

- осуществлять проектирование, разработку, контроль реализации политики информационной безопасности и корректировать ее в соответствии с изменяющейся внутренней и внешней информационной средой;
- готовить предложения директору Центра по методике проведения внутреннего анализа (оценки) рисков;
- координировать действия администраторов и сотрудников Центра в ходе проведении проверки состояния информационной безопасности, анализа рисков и подготовки соответствующих отчетов;
- разрабатывать предложения по мероприятиям обеспечения информационной безопасности и защиты ПДн, которые необходимо реализовывать в ИСПДн в соответствии с принятой политикой безопасности и результатами оценки рисков;
- осуществлять разработку практических требований, организационно-технических документов и рекомендаций по реализации мероприятий по обеспечению информационной безопасности, защиты ПДн, настройке аппаратных, программных и программно-аппаратных средств обеспечения информационной безопасности, применяемых в ИСПДн;
- другие обязанности администратора информационной безопасности определяются должностным регламентом.

5.3. Оператор АРМ

Оператор АРМ (пользователь), сотрудник Центра, осуществляющий обработку ПДн. Обработка ПДн включает: возможность просмотра ПДн, ручной ввод ПДн в систему ИСПДн, формирование справок и отчетов по информации, полученной из ИСПД. Оператор не имеет полномочий для управления подсистемами обработки данных и СЗПДн.

Оператор ИСПДн (пользователь) обладает следующим уровнем доступа и знаний:

- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;
- располагает конфиденциальными данными, к которым имеет доступ.

Обязанности пользователей:

- знать положения политики информационной безопасности в части их касающейся;
- строго выполнять требования администратора безопасности по обеспечению реализации по-ложений политики информационной безопасности;
- в случае обнаружения сбоев в работе ИСПДн, а также любых других фактов, расцениваемых как признаки нарушения информационной безопасности, незамедлительно сообщать о них администратору безопасности или администратору ИСПДн;
- в случае необходимости удалённого взаимодействия с ИСПДн использовать только рекомендованные администратором безопасности и администратором ИСПДн средства удалённого доступа и администрирования;
- не осуществлять действий, способных привести к нарушению функционирования или раскрытию параметров ИСПДн.

В частности, не допускается:
а) создание или распространение вредоносных программ и компьютерных вирусов, как заимствованных, так и самостоятельно разработанных;
б) сканирование портов, прослушивание сетевого трафика, а также любые другие попытки анализа сети без письменного разрешения администратора безопасности.
хранить всю информацию, связанную с профессиональной деятельностью, ПДн на файл-сервере или другом средстве хранения информации выделенном для этой цели.

5.4. Администратор сети

Администратор сети, сотрудник Центра, ответственный за функционирование телекоммуникационной подсистемы ИСПДн. Администратор сети не имеет полномочий для управления подсистемами обработки данных и безопасности.

Администратор сети обладает следующим уровнем доступа и знаний:

- обладает частью информации о системном и прикладном программном обеспечении ИСПДн;
- обладает частью информации о технических средствах и конфигурации ИСПДн;
- имеет физический доступ к техническим средствам обработки информации и средствам защиты;
- знает, по меньшей мере, одно легальное имя доступа.

5.5. Технический специалист по обслуживанию периферийного оборудования

Технический специалист по обслуживанию, сотрудник Центра, осуществляющий обслуживание и настройку периферийного оборудования ИСПДн. Технический специалист по обслуживанию не имеет доступа к ПДн, не имеет полномочий для управления подсистемами обработки данных и безопасности.

Технический специалист по обслуживанию обладает следующим уровнем доступа и знаний:

- обладает частью информации о системном и прикладном программном обеспечении ИСПДн;
- обладает частью информации о технических средствах и конфигурации ИСПДн;
- знает, по меньшей мере, одно легальное имя доступа.

5.6. Программист-разработчик ИСПДн

Программисты-разработчики (поставщики) прикладного программного обеспечения, обеспечивающие его сопровождение на защищаемом объекте. К данной группе могут относиться как сотрудники Учреждения, так и сотрудники сторонних организаций.

Лицо этой категории:

- обладает информацией об алгоритмах и программах обработки информации на ИСПДн;
- обладает возможностями внесения ошибок, не декларированных возможностей, программных закладок, вредоносных программ в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения;

может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты ПДн, обрабатываемых в ИСПДн.