«УТВЕРЖДАЮ»
Главный врач ГАУЗ «РКОД МЗ РТ»

_____ Р.Ш. Хасанов

«27» 10 2014 г.

П О Л И Т И К А
безопасности персональных данных, обрабатываемых в информационных системах персональных данных в Государственном автономном учреждении здравоохранения «Республиканский клинический онкологический диспансер Министерства здравоохранения Республики Татарстан»

I. Определения

1.1. Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

1.2. Безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью работников, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

1.3. Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

1.4. Доступ к информации – возможность получения информации и её использования.

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

1.6. Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

1.7. Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

1.8. Информационная технология – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

1.9. Источник угрозы безопасности персональных данных – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности персональных данных.

1.10. Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

1.11. Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не распространять их без согласия субъекта персональных данных или наличия иного законного основания.

1.12. Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

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

1.14. Носитель информации – 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.

1.15. Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

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

1.17. Объект вычислительной техники – стационарный или подвижный объект, который представляет собой комплекс средств

вычислительной техники, предназначенный для выполнения определенных функций обработки информации. К объектам вычислительной техники относятся автоматизированные системы, автоматизированные рабочие места, информационно-вычислительные центры и другие комплексы средств вычислительной техники. К объектам вычислительной техники могут быть отнесены также отдельные средства вычислительной техники, выполняющие самостоятельные функции обработки информации.

1.18. Оператор персональных данных – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

1.19. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

1.20. Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

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

1.22. Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц. Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

1.23. Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

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

1.25. Система защиты персональных данных – совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты персональных данных.

1.26. Средство криптографической защиты информации – средство защиты информации, реализующее алгоритмы криптографического преобразования информации.

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

1.28. Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

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

1.30. Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность 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 при их обработке в информационной системе персональных данных.

1.31. Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

1.32. Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

1.33. Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

II. Общие положения

2.1. Настоящая Политика безопасности персональных данных, обрабатываемых в информационных системах персональных данных в Государственном автономном учреждении здравоохранения

«Республиканский клинический онкологический диспансер Министерства здравоохранения Республики Татарстан» (далее – Учреждение), является официальным документом и разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных в Учреждении.

2.2. В настоящей Политике определены требования к работникам Учреждения, степень ответственности работников, структура и необходимый уровень защищенности, статус и должностные обязанности работников, ответственных за обеспечение безопасности персональных данных в информационных системах персональных данных Учреждения.

2.3. Целью настоящей Политики является обеспечение безопасности персональных данных Учреждения от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности персональных данных.

2.4. 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.

2.5. Информация и связанные с ней ресурсы должны быть доступны только для авторизованных работников. В информационных системах персональных данных должно осуществляться своевременное обнаружение угроз и реагирование на угрозы безопасности персональных данных.

2.6. В информационных системах персональных данных необходимо исключить возможность преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

2.7. Перечень персональных данных, подлежащих защите, определен в Положении о защите персональных данных.

III. Система защиты персональных данных

3.1. Система защиты персональных данных строится на основании:

3.1.1. Перечня персональных данных, подлежащих защите.

3.1.2. Перечня информационных систем персональных данных.

3.1.3. Акта определения уровня защищенности персональных данных при их обработке в информационной системе персональных данных.

3.1.4. Частной модели угроз и нарушителя безопасности персональных данных.

3.1.5. Регламента разграничении прав доступа.

3.1.6. Руководящих документов ФСТЭК России и ФСБ России.

3.2. На основании этих документов определяется необходимый уровень защищенности персональных данных в каждой информационной системе персональных данных Учреждения. Для каждой информационной системы персональных данных должен быть составлен список используемых технических средств, а также программного обеспечения участвующего в обработке персональных данных, подлежащих защите.

3.3. В зависимости от уровня защищенности персональных данных в информационной системе персональных данных и актуальных угроз, система защиты персональных данных может включать следующие технические и программные средства:

3.3.1. Антивирусные средства для объектов вычислительной техники.

3.3.2. Средства межсетевого экранирования.

3.3.3. Средства криптографической защиты информации, при передаче защищаемой информации по каналам связи.

3.4. Так же в список должны быть включены функции защиты, обеспечиваемые штатными средствами информационной системы персональных данных и операционных систем, прикладным программным обеспечением и специальными комплексами, реализующими средства защиты. Список функций защиты может включать:

3.4.1. Управление доступом и разграничение доступа.

3.4.2. Регистрацию и учет действий с информацией.

3.4.3. Обеспечение целостности данных.

3.4.4. Обнаружение вторжений.

3.5. Список используемых средств должен поддерживаться в актуальном состоянии. Все изменения состава системы защиты персональных данных или элементов информационных систем персональных данных должны быть согласованы с Администратором информационной безопасности.

IV. Требования к подсистемам системы защиты персональных данных

4.1. Система защиты персональных данных включает в себя следующие подсистемы:

4.1.1. управления доступом, регистрации и учета.

4.1.2. обеспечения целостности и доступности.

4.1.3. антивирусной защиты.

4.1.4. межсетевого экранирования.

4.1.5. анализа защищенности.

4.1.6. обнаружения вторжений.

4.1.7. криптографической защиты.

4.2. Подсистемы системы защиты персональных данных имеют различный функционал в зависимости от уровня защищенности персональных данных при их обработке в информационной системе персональных данных, определенного в Акте определения уровня защищенности персональных данных при их обработке в информационной системе персональных данных.

V. Подсистема управления доступом, регистрации и учета

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

5.1.1. Идентификации и проверки подлинности субъектов доступа при входе в информационную систему персональных данных.

5.1.2. Идентификации терминалов, узлов сети, каналов связи, внешних устройств по логическим именам.

5.1.3. Идентификации программ, томов, каталогов, файлов, записей, полей записей по именам.

5.1.4. Регистрации входа (выхода) субъектов доступа в систему (из системы), либо регистрации загрузки и инициализации операционной системы и ее останова.

5.1.5. Регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам.

5.1.6. Регистрации попыток доступа программных средств к терминалам, каналам связи, программам, томам, каталогам, файлам, записям, полям записей.

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

VI. Подсистема обеспечения целостности и доступности

6.1. Подсистема обеспечения целостности и доступности предназначена для обеспечения целостности и доступности персональных данных, программных и аппаратных средств информационных систем персональных данных Учреждения, а так же средств защиты, при случайной или намеренной модификации.

6.2. Подсистема реализуется с помощью организации резервного копирования обрабатываемых данных, а так же резервированием ключевых элементов информационных систем персональных данных.

VII. Подсистема антивирусной защиты

7.1. Подсистема антивирусной защиты предназначена для обеспечения антивирусной защиты объектов вычислительной техники Учреждения.

7.2. Средства антивирусной защиты предназначены для реализации следующих функций:

7.2.1. Резидентный антивирусный мониторинг.

7.2.2. Антивирусное сканирование.

7.2.3. Скрипт-блокирование.

7.2.4. Централизованная/удаленная установка/деинсталляция антивирусного продукта, настройка, администрирование, просмотр отчетов и статистической информации по работе продукта.

7.2.5. Автоматизированное обновление антивирусных баз.

7.2.6. Ограничение прав на остановку исполняемых задач и изменения настроек антивирусного программного обеспечения.

7.2.7. Автоматический запуск сразу после загрузки операционной системы.

7.3. Подсистема реализуется путем внедрения специального антивирусного программного обеспечения во все элементы информационных систем персональных данных.

VIII. Подсистема межсетевого экранирования

8.1. Подсистема межсетевого экранирования предназначена для реализации следующих функций:

8.1.1. Фильтрации открытого и зашифрованного (закрытого) IP-трафика.

8.1.2. Фиксации во внутренних журналах информации о проходящем открытом и закрытом IP-трафике.

8.1.3. Идентификации и аутентификации Администратора информационной безопасности или Администратора информационной системы персональных данных при его локальных запросах на доступ.

8.1.4. Регистрации входа (выхода) Администратора информационной безопасности или Администратора информационной системы персональных данных в систему (из системы) либо загрузки и инициализации системы и ее программного останова.

8.1.5. Контроля целостности своей программной и информационной части.

8.1.6. Фильтрации пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств.

8.1.7. Фильтрации с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов.

8.1.8. Регистрации и учета запрашиваемых сервисов прикладного уровня.

8.1.9. Блокирования доступа неидентифицированного объекта или субъекта, подлинность которого при аутентификации не подтвердилась, методами, устойчивыми к перехвату.

8.1.10. Контроля за сетевой активностью приложений и обнаружения сетевых атак.

8.2. Подсистема реализуется внедрением программно-аппаратных комплексов межсетевого экранирования на границе сети.

IX. Подсистема анализа защищенности

9.1. Подсистема анализа защищенности, должна обеспечивать выявление уязвимостей, связанных с ошибками в конфигурации программного обеспечения информационной системы персональных данных, которые могут быть использованы нарушителем для реализации атаки на систему.

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

X. Подсистема обнаружения вторжений

10.1. Подсистема обнаружения вторжений, должна обеспечивать выявление сетевых атак на элементы информационной системы персональных данных, подключенные к сетям общего пользования и (или) международного обмена.

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

XI. Подсистема криптографической защиты

11.1. Подсистема криптографической защиты предназначена для исключения несанкционированного доступа к защищаемой информации в информационных системах персональных данных Учреждения, при ее передаче по каналам связи сетей общего пользования и (или) международного обмена.

11.2. Подсистема реализуется внедрением криптографических программно-аппаратных комплексов.

XII. Работники, обрабатывающие персональные данные в информационных системах персональных данных

12.1. В информационных системах персональных данных Учреждения можно выделить следующие группы работников, участвующих в обработке персональных данных:

12.1.1. Администратор информационной системы персональных данных.

12.1.2. Пользователь информационной системы персональных данных.

12.2. В информационных системах персональных данных Учреждения можно выделить следующие группы работников, не участвующих в обработке персональных данных, но сопровождающие и обслуживающие элементы ИСПДн:

12.2.1. Администратор информационной безопасности.

12.2.2. Ответственный за эксплуатацию объектов вычислительной техники.

Данные о группах работников, уровне их доступа и информированности должны быть отражены в Регламенте разграничения прав доступа.

Должностные обязанности всех работников описаны в соответствующих должностных Инструкциях.

XIII. Требования к работникам по обеспечению защиты персональных данных

13.1. Все работники Учреждения, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению установленного режима безопасности персональных данных.

13.2. При вступлении в должность нового работника непосредственный руководитель структурного подразделения обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите персональных данных, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования информационных систем персональных данных.

13.3. Работник должен быть ознакомлен с настоящей Политикой, установленными процедурами работы с элементами информационной системы персональных данных и системой защиты персональных данных.

13.4. Работники Учреждения, использующие технические средства аутентификации, должны обеспечивать сохранность персональных идентификаторов (электронных ключей) и не допускать несанкционированный доступ к ним, а так же возможность их утери или использования третьими лицами. Работники несут персональную ответственность за сохранность идентификаторов.

13.5. Работники Учреждения должны следовать установленным процедурам поддержания режима безопасности персональных данных при выборе и использовании паролей.

13.6. Работники Учреждения должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все работники, обрабатывающие персональные данные в информационных системах персональных данных, должны знать требования по

безопасности персональных данных и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

13.7. Работникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а так же записывать на них защищаемую информацию.

13.8. Работникам запрещается разглашать защищаемую информацию, которая стала им известна в силу выполнения ими своих должностных обязанностей.

13.9. При работе с персональными данными в информационной системе персональных данных работники Учреждения обязаны исключить возможность просмотра персональных данных третьими лицами с мониторов объектов вычислительной техники.

13.10.При завершении работы с информационной системой персональных данных работники обязаны защитить объекты вычислительной техники с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

13.11.Работники Учреждения должны быть проинформированы об угрозах нарушения режима безопасности персональных данных и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на работников, нарушающих принятые политику и процедуры безопасности персональных данных.

13.12.Работники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы информационной системы персональных данных, а также о выявленных ими событиях, затрагивающих безопасность персональных данных, руководству и лицу, отвечающему за немедленное реагирование на угрозы безопасности персональных данных.

XIV. Ответственность

14.1. В соответствии со статьями 24 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

14.2. Работники, обрабатывающие персональные данные в информационных системах персональных данных, несут ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

14.3. При нарушениях работниками Учреждения правил, связанных с безопасностью персональных данных, они несут ответственность, установленную действующим законодательством Российской Федерации.

Лист ознакомления

№ п/п	Должность	ФИО	Дата	Подпись