УТВЕРЖДЕНО
Приказом
ГАУЗ КО ОКСП
от «09» 01 2017 г.
№ 5/1

Политика обеспечения безопасности персональных данных при их обработке в информационной системе ГАУЗ КО «Областная клиническая стоматологическая поликлиника»

1. Общие положения

1. Положение об обеспечении безопасности персональных данных при их обработке в информационной системе ГАУЗ КО «Областная клиническая стоматологическая поликлиника» (далее - Положение) предназначено для обеспечения эффективной организации и управления доступом пользователей к персонифицированной информации, хранящейся в базе данных (далее - БД), и содержит требования по обеспечению информационной безопасности в части выполнения операций по организации и управлению доступом к базе данных.

2. Работу системного администратора в области защиты информации определяет комплекс организационно-технических мероприятий по обеспечению безопасности персонифицированной информации, хранящейся в базе данных и обрабатываемой средствами вычислительной техники в локальной вычислительной сети.

3. Требования Положения обязательны для выполнения всеми пользователями. Ответственность за выполнение требований Положения несут пользователь информационной системы и руководитель структурного подразделения, в котором работает данный пользователь. Пользователь, впервые начинающий работать с персонифицированными базой данных, обязан ознакомиться с данным Положением.

4. Все пункты Положения, упоминающие подключение к БД, распространяются также и на подключение к информационной системе с использованием БД (далее - ИСБД), если иное не оговорено явно в тексте Положения.

В настоящем Положении использованы следующие термины и определения:

База данных - централизованное хранилище информации, оптимизированное для многопользовательского доступа и работающее под управлением системы управления базой данных (далее - СУБД).

Персонифицированная информация – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных).

Системный администратор - должностное лицо, уполномоченное для выполнения административных функций при работе с локальной и территориальной сетью и обеспечивающее функционирование БД и ее безопасность.

Несанкционированный доступ (НСД) - определяется как доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

Информационная система с использованием БД (ИСБД) - система или приложение, использующее непосредственный доступ к БД.

Пользователи - должностные лица, а также все другие лица и организации, использующие базы данных органов и управлений либо обращающиеся к ним.

ЛВС - локальная вычислительная сеть.

Политика информационной безопасности – комплекс организационно-технических мероприятий, правил и условий использования информационных систем в ГАУЗ КО «Областная клиническая стоматологическая поликлиника», определяющих нормальное функционирование этих систем и обеспечение безопасности информации, обрабатываемой в них, оформленной в виде нормативных документов.

Настоящее Положение устанавливает цели, задачи, порядок проведения мероприятий по обеспечению безопасности при работе с базой данных.

1. Цели и задачи проведения мероприятий по безопасности

Целью проведения мероприятий по обеспечению безопасности при работе с БД является предотвращение вывода из строя системы управления базы данных, предотвращение НСД к БД, находящейся на электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети.

2. Порядок проведения мероприятий по обеспечению работы с БД

Требования к серверному помещению:

- Для обеспечения безопасности баз данных и бесперебойной работы систем серверы и компьютеры управления БД размещается в отдельном помещении.
- Расчет общей площади серверного помещения при проектировании рабочих мест выполняется по рекомендованной норме площади на одно рабочее место: сотрудник - 4,5 кв. м; программист - 6 кв. м; персонал по обслуживанию вычислительной техники - 6 кв. м.

- Отсутствие оконных проемов или установка на них металлических решеток/жалюзи, или использование ударопрочных материалов остекления, подвесной потолок с панелями из негорючего шумопоглощающего материала, стены - панели из негорючего шумопоглощающего материала, отдельный контур заземления электрической сети, пол – напольная плитка, металлическая дверь с уплотнителем и автоматическим контролем доступа, оборудование – серверные и монтажные стойки, датчики охранной и пожарной сигнализации, сплит-система с поддержанием заданных параметров температуры и влажности и с фильтрованием наружного воздуха.

- Для бесперебойной работы серверов БД и предотвращения потери информации рабочие станции и сервера укомплектовываются блоками бесперебойного питания

Приказом по ГАУЗ КО «Областная клиническая стоматологическая поликлиника» определяется и фиксируется круг лиц, имеющих доступ в помещение, где находятся сервера и компьютеры управления БД. Для исключения возможности несанкционированного доступа к серверу БД обеспечивается механическая защита помещения сервера с системой контроля доступа.

3. Порядок работы по защите информации при работе с БД

4.1. Порядок работы пользователя по защите информации при работе с БД.

4.1.1. Порядок работы пользователя по защите информации при работе с БД определяется комплексом организационно-технических мероприятий по обеспечению безопасности информации, хранящейся в БД и обрабатываемой с помощью средств вычислительной техники в ЛВС ГАУЗ КО «Областная клиническая стоматологическая поликлиника».

4.1.2. Решение задач, связанных с организацией и управлением доступа должностных лиц ГАУЗ КО «Областная клиническая стоматологическая поликлиника» к БД, осуществляется системным администратором. При возникновении ситуаций, не описываемых в данном Положении, решение принимает системный администратор, руководствуясь порядком работы системного администратора по защите информации при работе с БД, ГАУЗ КО «Областная клиническая стоматологическая поликлиника».

4.1.3. Ответственность за сохранность и правильное использование информации, полученной из БД, несут пользователь, имеющий доступ к БД, и начальник структурного подразделения, в составе которого работает пользователь. Ответственность наступает с момента поступления информации на рабочую станцию пользователя.

4.1.4. Для обеспечения доступа пользователей к БД на их рабочих станциях должно быть установлено специальное программное обеспечение, обеспечивающее доступ и выполнение операций с информацией в БД.

4.1.5. Пользователям запрещается самостоятельно устанавливать другое программное обеспечение (или менять параметры конфигурации ранее установленных программных средств) для доступа и манипулирования данными в БД, кроме случаев,

обусловленных производственной необходимостью. Запрещается копирование специального ПО и файлов БД на личные съемные носители.

4.1.6. Запрещается использовать для передачи БД не предназначенные для этого средства и каналы связи.

4.1.7. Доступ к БД предоставляется исключительно пользователям, прошедшим инструктаж согласно политике информационной безопасности.

4.1.8. Список лиц, имеющих доступ к БД, определяется приказом Главного врача ГАУЗ КО «Областная клиническая стоматологическая поликлиника».

4.1.9. Для каждого из пользователей, которым необходим доступ к БД, создается учетная запись о пользователе БД, состоящая из имени пользователя и пароля. Не допускается использование простых паролей. Срок действия активной учетной записи пользователя БД ограничен сроком действия служебного контракта. Первоначальное значение пароля устанавливается системным администратором. Периодичность, порядок и технология изменения пароля доводится системным администратором до пользователей. Пользователю запрещается использовать пароль, предоставленный системным администраторам для первоначального доступа к БД, в качестве постоянного рабочего пароля.

4.1.10. Главный врач ГАУЗ КО «Областная клиническая стоматологическая поликлиника» принимает решение о разрешении доступа пользователя к БД или изменения полномочий пользователя БД по ходатайству начальника отдела, в составе которого работает данный пользователь.

4.1.11. Пользователю запрещается передавать в любом виде или сообщать пароли для доступа к БД другим лицам, в том числе и своим руководителям. Запрещается хранение пароля на любых твердых носителях, позволяющих другим лицам получить информацию о пароле.

4.1.12. Пользователю запрещается использовать информацию, полученную в результате доступа к БД, в целях, не предусмотренных его должностным регламентом.

4.1.13. Пользователь обязан не разглашать свои идентификационные данные.

4.1.14. Пользователь, имеющий возможность ввода или изменения данных в БД, обязан обеспечить правильность вводимых данных.

4.1.15. Пользователь обязан блокировать персональный компьютер и закрывать соединение с БД на время своего отсутствия у рабочей станции.

4.1.16. Руководители структурных подразделений обязаны своевременно сообщать системному администратору об изменениях статуса пользователя (увольнение и т.п.).

4.1.17. В случае выявления инцидентов с доступом к БД (фактов несанкционированного доступа к БД, блокировки доступа, утери или компрометации пароля и т.д.) пользователь обязан незамедлительно сообщить об этом системному администратору.

4.1.18. Возможность подключения к БД не дает права пользователям подключаться к БД, если им не предоставлены права доступа к этим БД. Такие подключения рассматриваются как попытки несанкционированного доступа.

4.1.19. При нарушении правил, связанных с информационной безопасностью, пользователь несет ответственность, установленную действующим законодательством Российской Федерации.

4.1.20. Пользователь несет ответственность за все действия, совершенные от имени его учетной записи, если не доказан факт несанкционированного использования учетной записи.

4.1.21. Начальники отделов несут персональную ответственность за неправильное использование специалистами учетных записей пользователей, имеющих доступ к БД, а также за ознакомление (под роспись) с Порядком работы новых пользователей БД в своем структурном подразделении.

4.1.22. При выявлении инцидентов доступ пользователей к БД должен быть приостановлен до окончания расследования инцидента, о чем пользователь либо его начальник (заведующий) уведомляются в кратчайшие сроки. По результатам служебного расследования нарушитель может быть лишен прав доступа к БД, материалы расследования могут быть направлены в соответствующие Службы для привлечения нарушителя к административной ответственности.

4.2. Порядок работы системного администратора по защите информации при работе с БД.

4.2.1. Ответственность за выполнение требований Положения несут системный администратор и начальник отдела, в котором он работает.

4.2.2. Решение задач, связанных с организацией и управлением доступом пользователей к БД, осуществляется системным администратором.

4.2.3. Ответственность за сохранность информации, находящейся в БД, несет системный администратор.

4.2.4. Технологическая модификация и удаление информации в БД должны быть регламентированы для каждой БД.

4.2.5. Системный администратор организует и контролирует процесс установки и конфигурирования стандартного программного обеспечения для работы пользователей с БД, осуществляет сопровождение и тестирование специального программного обеспечения для доступа к БД, обеспечивает разработку дополнительных требований по обеспечению доступа к БД и доведение их до сведения пользователей и их руководителей.

4.2.6. В исключительных случаях с согласия системного администратора возможно отклонение от требований данного Положения при условии, что данное отклонение не влечет значительного риска для информационной безопасности. В таких случаях лицо, принимающее решение о допустимом риске, берет на себя ответственность за возможные последствия. Этим лицом не может быть системный администратор.

4.2.7. Все журналы и документы по безопасности БД хранит системный администратор в электронном виде не менее трех лет.

4.2.8. При нарушениях системным администратором правил, связанных с информационной безопасностью, он несет ответственность, установленную действующим законодательством Российской Федерации.

4.2.9. Системный администратор несет ответственность за все действия, совершенные от имени его учетной записи или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

4.2.10. При выявлении факта НСД системный администратор обязан:

- прекратить доступ к БД со стороны выявленного участка НСД;
- доложить руководству служебной запиской о факте НСД, его результате (успешный, неуспешный) и предпринятых действиях;
- известить начальника (заведующего) структурного подразделения, в котором работает пользователь, от имени учетной записи которого была осуществлена попытка НСД, о факте НСД;
- проанализировать характер НСД;
- внести запись в журнал регистрации попыток несанкционированного доступа к базам данных

4.2.11. При увольнении сотрудника идентификатор и пароль сотрудника удаляются из системы, электронные ключи доступа сдаются сотрудником. Возможность доступа по старым ключам блокируется.

4.2.12. Системный администратор вместе с руководителем сотрудника анализирует целостность данных, к которым имел доступ сотрудник.

4.2.13. В случае обнаружения неправомерных действий специалистов (удаление информации, внесение в систему закладок и вирусов) системный администратор докладывает об этом начальнику отдела, в котором он работает, который в свою очередь докладывает Главному врачу ГАУЗ КО «Областная клиническая стоматологическая поликлиника». По результатам служебного расследования нарушитель может быть привлечен к административной ответственности.