Государственное бюджетное учреждение здравоохранения
«Пензенская областная клиническая больница им. Н.Н. Бурденко»
(ГБУЗ ПОКБ им. Н.Н. Бурденко)

П Р И К А З

27.10.2023 № 161

г. Пенза

Об организации мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

В целях организации работы по обеспечению защиты персональных данных в информационных системах персональных данных субъектов персональных данных при их обработке в ГБУЗ ПОКБ им. Н.Н. Бурденко в соответствии с Федеральным законом РФ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом РФ от 27.07.2006 № 152-ФЗ «О персональных данных», приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 28.10.2022 № 179 «Об утверждении требований к подтверждению уничтожения персональных данных», приказом ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности», приказом Минздрава России от 03.08.2023 № 408 «Об утверждении Перечня документов, образующихся в деятельности Министерства здравоохранения Российской Федерации и подведомственных ему организаций, с указанием сроков хранения», приказ Министерства здравоохранения РФ от 03.07.2023 № 340н «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в сферах деятельности, нормативно-правовое регулирование которых осуществляется Министерством здравоохранения Российской Федерации», **п р и к а з ы в а ю:**

1. Утвердить Положение об организации мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, используемых в ГБУЗ ПОКБ им. Н.Н. Бурденко (Приложение № 1).

2. Утвердить Инструкцию о порядке работы пользователей со средством защиты информации - криптографической системой в ГБУЗ ПОКБ им. Н.Н. Бурденко (Приложение № 2).

3. Утвердить Инструкцию о порядке работы пользователей со средством защиты информации-антивирусной защиты компьютеров в ГБУЗ ПОКБ им. Н.Н. Бурденко (Приложение № 3).

4. Утвердить Положение об использовании сети Интернет в ГБУЗ ПОКБ им. Н.Н. Бурденко (Приложение № 4).

5. Утвердить журнал учета съемных носителей персональных данных в ГБУЗ ПОКБ им. Н.Н. Бурденко (Приложение № 5).

6. Утвердить Положение о реагировании на инциденты информационной безопасности в ГБУЗ ПОКБ им. Н.Н. Бурденко (Приложение № 6).

7. Утвердить Инструкцию по организации резервирования и восстановления программного обеспечения и баз персональных данных в информационных системах персональных данных в ГБУЗ ПОКБ им. Н.Н. Бурденко (Приложение № 7).

8. Утвердить Инструкцию по организации парольной защиты компьютеров ГБУЗ ПОКБ им. Н.Н. Бурденко (Приложение № 8).

9. Утвердить Инструкцию администратора информационных систем персональных данных, ответственного за эксплуатацию информационных систем персональных данных в ГБУЗ ПОКБ им. Н.Н. Бурденко (Приложение № 9).

10. Утвердить Инструкцию администратора безопасности информации в информационных системах персональных данных, эксплуатируемых в ГБУЗ ПОКБ им. Н.Н. Бурденко (Приложение № 10).

11. Утвердить Инструкцию о порядке работы пользователей информационных систем персональных данных, в части обеспечения безопасности данных при обработке в ГБУЗ ПОКБ им. Н.Н. Бурденко (Приложение № 11).

12. Начальнику отдела автоматизированной системы управления Мелехину В.А. обеспечить своевременную актуализацию настоящего приказа.

13. Начальнику отдела документационного обеспечения Беляевой Ю.В. ознакомить с настоящим приказом и приложениями к нему персонально под роспись всех руководителей структурных подразделений (служб, отделов).

28. Руководителям структурных подразделений ознакомить ГБУЗ «Пензенская областная клиническая больница им. Н.Н. Бурденко» ознакомить с настоящим приказом и приложениями к нему всех работников вверенного ему подразделения (персонально, под роспись).

29. Контроль за исполнением настоящего приказа оставляю за собой.

Главный врач А.В. Никишин

Начальник юридического отдела
_____ Н.В. Флеонова «_27_» _10_ 2023 г.
Начальник отдела документационного обеспечения
_____ Ю.В. Беляева «_27_» _10_ 2023 г.

Приложение № 1
к приказу ГБУЗ «Пензенская
областная клиническая
больница им. Н.Н. Бурденко»
от_____№_____

Положение
об организации мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных используемых в ГБУЗ ПОКБ им. Н.Н. Бурденко

1.1. Настоящее Положение регулируется Политикой информационной безопасности информационных систем персональных данных ГБУЗ ПОКБ им. Н.Н. Бурденко (Далее – ИСПДн) и устанавливает состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПДн, направленных на нейтрализацию актуальных угроз безопасности персональных данных.

1.2. Обеспечение безопасности персональных данных при обработке в информационных системах персональных данных (Далее – ПДн) достигается, в частности:

- определением угроз безопасности персональных данных при их обработке в ИСПДн;
- применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;
- применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;
- оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию ИСПДн;
- учетом машинных носителей персональных данных;
- обнаружением фактов несанкционированного доступа к персональным данным и принятием мер, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на ИСПДн и по реагированию на компьютерные инциденты в них;
- восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним может осуществляться посредством регулярного резервного копирования персональных данных;
- установлением данного порядка и правил доступа к персональным данным, обрабатываемым в ИСПДн, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в ИСПДн;
- контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных осуществляться посредством проведения внутреннего и

внешнего аудита, мониторинга реализации защитных мер, модификации системы безопасности по результатам проведенных аудитов.

1.4. Меры по обеспечению безопасности персональных данных реализуются в том числе посредством применения в информационной системе средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия, в случаях, когда применение таких средств необходимо для нейтрализации актуальных угроз безопасности персональных данных.

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных);
- регистрация событий безопасности;
- антивирусная защита;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности персональных данных;
- обеспечение целостности информационной системы и персональных данных;
- обеспечение доступности персональных данных;
- защита среды виртуализации;
- защита технических средств;
- защита информационной системы, ее средств, систем связи и передачи данных;
- выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них;
- управление конфигурацией информационной системы и системы защиты персональных данных.

1.4. Угрозами безопасности персональных данных, актуальными при обработке персональных данных в информационных системах персональных данных, эксплуатируемых в сферах деятельности, нормативно-правовое регулирование которых осуществляется Министерством здравоохранения Российской Федерации, определены:

- угрозы безопасности персональных данных, защищаемых без использования средств криптографической защиты информации (далее - СКЗИ);
- угрозы реализации целенаправленных действий с использованием аппаратных и (или) программных средств с целью нарушения безопасности защищаемых с использованием СКЗИ персональных данных или создания условий для этого.

1.5. Для обеспечения 4 уровня защищенности персональных данных при их обработке в ИСПДн в ГБУЗ ПОКБ им. Н.Н. Бурденко выполняются следующие требования:

- организован режим обеспечения безопасности помещений, в которых размещена ИСПДн, препятствующая возможности неконтролируемого

проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

- обеспечена сохранность носителей персональных данных;

- утвержден документ, определяющий перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

- используются средства защиты информации, прошедшие процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз;

- обеспечение режима, препятствующего возможности неконтролируемого проникновения или пребывания в помещениях, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ;

– помещения оснащены входными дверьми с замками, обеспечения постоянного закрытия дверей помещений на замок и их открытия только для санкционированного прохода, а также опечатывания помещений по окончании рабочего дня или оборудование помещений соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии помещений.

1.6. В ГБУЗ ПОКБ им. Бурденко организованны следующие средства защиты информации в ИСПДн:

- криптографические системы;

- антивирусные программы.

1.7. Также в ГБУЗ ПОКБ им. Н.Н. Бурденко определен порядок доступа в Помещения в рабочее и нерабочее время, а также в нештатных ситуациях, (Приложения № 17, 18 к приказу главного врача от 27.10.2023 № 160 «Об обработке персональных данных в ГБУЗ ПОКБ им. Н.Н. Бурденко») и утвержден перечень лиц, имеющих право доступа в помещения ГБУЗ ПОКБ им. Н.Н. Бурденко (Приложения № 6, 7, 8 к приказу к приказу главного врача от 27.10.2023 № 160 «Об обработке персональных данных в ГБУЗ ПОКБ им. Н.Н. Бурденко»).

Приложение № 2
к приказу ГБУЗ «Пензенская
областная клиническая
больница им. Н.Н. Бурденко»
от_____№_____

Инструкция
о порядке работы пользователей со средством защиты информации - криптографической системой в ГБУЗ ПОКБ им. Н.Н. Бурденко

1. Общие положения

1.1. Настоящая Инструкция определяет порядок организации и обеспечения функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну (далее - криптосредство) в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных (далее - информационная система).

1.2. Пользователь - лицо, участвующее в эксплуатации криптосредства или использующее результаты его функционирования.

1.3. Режимные помещения - помещения, где установлены криптосредства или хранятся ключевые документы к ним.

1.4. Шифровальные (криптографические) средства - криптосредства:

1.5. средства шифрования - аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа (далее - НСД) при ее обработке и хранении;

1.6. средства имитозащиты - аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты от навязывания ложной информации;

1.7. средства электронной цифровой подписи (далее - ЭЦП) - аппаратные, программные и аппаратно-программные средства, обеспечивающие на основе криптографических преобразований реализацию хотя бы одной из следующих функций: создание ЭЦП с использованием закрытого ключа ЭЦП, подтверждение с использованием открытого ключа ЭЦП подлинности ЭЦП, создание закрытых и открытых ключей ЭЦП;

1.8. средства кодирования - средства, реализующие алгоритмы криптографического преобразования информации с выполнением части преобразования путем ручных операций или с использованием автоматизированных средств на основе таких операций;

1.9. средства изготовления ключевых документов (независимо от вида носителя ключевой информации);

1.10. ключевые документы (независимо от вида носителя ключевой информации).

2. Обязанности пользователей криптосредств

2.1.1. Пользователи криптосредств обязаны:

2.1.2. не разглашать информацию, к которой они допущены, в том числе сведения о криптосредствах, ключевых документах к ним и других мерах защиты;

2.1.3. соблюдать требования к обеспечению безопасности персональных данных, требования к обеспечению безопасности криптосредств и ключевых документов к ним;

2.1.4. сообщать о ставших им известными попытках посторонних лиц получить сведения об используемых криптосредствах или ключевых документах к ним;

2.1.5. немедленно уведомлять оператора о фактах утраты или недостачи криптосредств, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемых персональных данных;

2.1.6. сдать криптосредства, эксплуатационную и техническую документацию к ним, ключевые документы в соответствии с порядком, установленным настоящей Инструкции, при увольнении или отстранении от исполнения обязанностей, связанных с использованием криптосредств.

3. Порядок обращения с криптосредствами и криптоключами к ним. Мероприятия при компрометации криптоключей

3.1. При необходимости передачи по техническим средствам связи служебных сообщений ограниченного доступа, касающихся организации и обеспечения функционирования криптосредств, указанные сообщения необходимо передавать только с использованием криптосредств. Передача по техническим средствам связи криптоключей не допускается, за исключением специально организованных систем с децентрализованным снабжением криптоключами.

3.2. Криптосредства, используемые для обеспечения безопасности персональных данных при их обработке в информационных системах, подлежат учету с использованием индексов или условных наименований и регистрационных номеров. Перечень индексов, условных наименований и регистрационных номеров криптосредств определяется Федеральной службой безопасности Российской Федерации.

3.3. Используемые или хранимые криптосредства, эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземплярному учету. При этом программные криптосредства должны учитываться совместно с аппаратными средствами, с которыми осуществляется их штатное функционирование. Если аппаратные или аппаратно-программные криптосредства подключаются к системной шине или к одному из внутренних интерфейсов аппаратных средств, то такие криптосредства учитываются также совместно с соответствующими аппаратными средствами.

3.4. Единицей поэкземплярного учета ключевых документов считается ключевой носитель многократного использования, ключевой блокнот. Если

один и тот же ключевой носитель многократно используют для записи криптоключей, то его каждый раз следует регистрировать отдельно.

3.5. Все полученные экземпляры криптосредств, эксплуатационной и технической документации к ним, ключевых документов должны быть выданы под расписку в соответствующем журнале поэкземплярного учета пользователям криптосредств, несущим персональную ответственность за их сохранность.

3.6. Передача криптосредств, эксплуатационной и технической документации к ним, ключевых документов допускается только между пользователями криптосредств и (или) ответственным пользователем криптосредств под расписку в соответствующих журналах поэкземплярного учета. Такая передача между пользователями криптосредств должна быть санкционирована ответственным пользователем криптосредств.

3.7. Пользователи криптосредств хранят инсталлирующие криптосредства носители, эксплуатационную и техническую документацию к криптосредствам, ключевые документы в шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

3.8. Пользователи криптосредств предусматривают также раздельное безопасное хранение действующих и резервных ключевых документов, предназначенных для применения в случае компрометации действующих ключевых документов.

3.11. Аппаратные средства, с которыми осуществляется штатное функционирование криптосредств, а также аппаратные и аппаратно-программные криптосредства должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы). Место опечатывания (опломбирования) криптосредств, аппаратных средств должно быть таким, чтобы его можно было визуально контролировать. При наличии технической возможности на время отсутствия пользователей криптосредств указанные средства необходимо отключать от линии связи и убирать в опечатываемые хранилища.

3.12. Эксплуатационную и техническую документацию к криптосредствам допускается пересылать заказными или ценными почтовыми отправлениями.

3.13. Уничтожение ключевых носителей осуществляется в соответствии с Приложениями № 22, 23 к приказу главного врача от 27.10.2023 №160 «Об обработке персональных данных в ГБУЗ ПОКБ им. Н.Н. Бурденко».

3.14. Осмотр ключевых носителей многократного использования посторонними лицами не следует рассматривать как подозрение в компрометации криптоключей, если при этом исключалась возможность их копирования (чтения, размножения).

3.15. В случаях недосдачи, непредъявления ключевых документов, а также неопределенности их местонахождения принимаются срочные меры к их розыску.

3.27. Мероприятия по розыску и локализации последствий компрометации ключевых документов организует и осуществляет администратор безопасности информации.

Приложение № 3
к приказу ГБУЗ «Пензенская
областная клиническая
больница им. Н.Н. Бурденко»
от_____№_____

Инструкция
о порядке работы пользователей со средством защиты информации - антивирусной защиты компьютеров в ГБУЗ ПОКБ им. Н.Н. Бурденко

1. Настоящая Инструкция определяет требования к организации защиты систем организации от разрушающего воздействия компьютерных вирусов и устанавливает ответственность руководителей и сотрудников подразделений, эксплуатирующих системы, за их выполнение.

2. К использованию в организации допускаются только лицензионные антивирусные средства.

3. Установка средств антивирусного контроля на компьютерах осуществляется ответственным лицом за работу с персональными данными ГБУЗ ПОКБ им. Н.Н. Бурденко.

4. Применение средств антивирусного контроля.

4.1. Антивирусный контроль всех дисков и файлов на компьютерах должен проводиться ежедневно в начале работы при загрузке компьютера в автоматическом режиме.

4.2 Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных дисках, лентах, CD - ROM и т.п.).

4.3. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

4.4. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера должна быть выполнена антивирусная проверка.

5. Действия при обнаружении вирусов.

5.1. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) сотрудник подразделения самостоятельно или вместе с ответственным за работу с персональными данными ГБУЗ ПОКБ им. Н.Н. Бурденко должен провести внеочередной антивирусный контроль своего компьютера.

5.2. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов сотрудники подразделений обязаны:

5.2.1. приостановить работу;

5.2.2. немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя и ответственного за работу с персональными данными ГБУЗ ПОКБ им. Н.Н. Бурденко, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;

5.2.3. совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;

5.2.4. провести лечение или уничтожение зараженных файлов;

6. Ответственность.

6.1. Ответственность за проведение мероприятий антивирусного контроля в подразделении и соблюдение требований настоящей Инструкции возлагается на ответственного за работу с персональными данными ГБУЗ ПОКБ им. Н.Н. Бурденко и всех сотрудников подразделения, являющихся пользователями компьютера.

7. Периодический контроль за состоянием антивирусной защиты, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции сотрудниками подразделений организации осуществляется ответственным за работу с персональными данными ГБУЗ ПОКБ им. Н.Н. Бурденко.

Приложение № 4
к приказу ГБУЗ «Пензенская
областная клиническая
больница им. Н.Н. Бурденко»
от_____№_____

Положение
об использовании сети Интернет в ГБУЗ ПОКБ им. Н.Н. Бурденко

1. Общие положения

1.1. Настоящее положение предназначено для организации работы пользователей сети Интернет ГБУЗ ПОКБ им. Н.Н. Бурденко.

1.2. Основной целью подключения компьютеров к сети Интернет является предоставление возможности ведения информационно-аналитической работы с использованием общедоступных информационных ресурсов этой сети и обеспечение электронного документооборота с использованием электронно-цифровой подписи.

1.3. Подключение к сети Интернет предполагает предоставление стандартного интерфейса пользователя сети, в том числе:

1.3.1. электронную почту e-mail;

1.3.2. доступ к файлам-серверам сети Интернет по протоколу fttp;

1.3.3. использование гипертекстовых ресурсов сети Интернет (World-Wide-Web (WWW);

1.3.4. возможность доступа к поисковым средствам сети Интернет.

1.4. Иное использование сети Интернет запрещается.

1.5. Основным фактором риска на рабочем месте пользователя сети Интернет является умышленное проникновение в среду пользователя сети с целью нарушения целостности и конфиденциальности информации.

1.6. Ответственный за использование сети Интернет ГБУЗ ПОКБ им. Н.Н. Бурденко начальник АСУ.

2. Порядок использования сети Интернет сотрудниками и работниками государственного бюджетного учреждения здравоохранения «Пензенская областная клиническая больница им. Н.Н. Бурденко»

2.1. Все пользователи сети Интернет должны быть ознакомлены с положением об использовании сети Интернет в ГБУЗ ПОКБ им. Н.Н. Бурденко и выполнять пункты данного положения.

2.2. Все компоненты программно-аппаратного обеспечения пользователя сети Интернет должны использоваться исключительно в служебных целях.

2.3. Каждый пользователь сети Интернет несет персональную ответственность за свои действия и за вводимую/выводимую информацию.

2.4. Компьютеры должны быть оснащены антивирусными программами и средствами контроля целостности программного обеспечения.

2.5. Техническая поддержка и сопровождение средств вычислительной техники в ГБУЗ ПОКБ им. Н.Н. Бурденко, подключенных к сети Интернет,

осуществляется ответственным за использование сети Интернет ГБУЗ ПОКБ им. Н.Н. Бурденко.

2.6. Пользователю сети Интернет запрещается самостоятельная реконфигурация компьютера, добавление или удаление программного обеспечения, а также распространение и установка на других компьютерах ГБУЗ ПОКБ им. Н.Н. Бурденко любого программного обеспечения, полученного по сети Интернет.

2.7. О всех ситуациях, связанных с нарушениями работы программно-технического комплекса, пользователь обязан поставить в известность ответственного за использование сети Интернет ГБУЗ ПОКБ им. Н.Н. Бурденко.

Приложение № 5
к приказу ГБУЗ «Пензенская
областная клиническая
больница им. Н.Н. Бурденко»
от_____№_____

УТВЕРЖДАЮ
главный врач ГБУЗ
«Пензенская областная
клиническая больница
им. Н.Н. Бурденко»
_____
«_____» _____20__

ЖУРНАЛ
учета съемных носителей персональных данных
в ГБУЗ ПОКБ им. Н.Н. Бурденко

Начат «__» _____ 201_ г.

Окончен «__» _____ 201_ г.

На _____листах

п/п	Метка съемного носителя (учетный номер)	Фамилия исполнителя	(Получил, вернул, передал)	Дата записи информации	Подпись исполнителя	Примечание*

_____ _____

Должность и ФИО ответственного за хранение Подпись

* Причина и основание окончания использования (№ и дата отправки адресату или распоряжения о передаче, № и дата акта утраты, неисправность, заполнение подлежащими хранению данными)

Приложение № 6
к приказу ГБУЗ «Пензенская
областная клиническая
больница им. Н.Н. Бурденко»
от_____№_____

**Положение о реагировании
на инциденты информационной безопасности в ГБУЗ ПОКБ им. Н.Н. Бурденко**

1. Назначение и область действия

1.1. Настоящее Положение о реагировании на инциденты информационной безопасности (далее – «Положение») определяет основные правила и требования по обеспечению информационной безопасности ГБУЗ ПОКБ им. Н.Н. Бурденко от угроз, связанных с некорректным информированием об инцидентах или использованием информации о них.

1.2. Соответствует Политике информационной безопасности ГБУЗ ПОКБ им. Н.Н. Бурденко.

1.3. Распространяется на всех работников ГБУЗ ПОКБ им. Н.Н. Бурденко, использующих информационные ресурсы и системы Учреждения (Далее-Пользователей). Является обязательным для исполнения.

2. Основные требования

2.1. Все пользователи информационных систем, услуг и ресурсов ГБУЗ ПОКБ им. Н.Н. Бурденко должны сообщать о любых замеченных или подозреваемых в недостатках безопасности в системах или услугах так оперативно, насколько это возможно.

2.2. Все пользователи должны быть осведомлены о своей обязанности сообщать ответственным лицам (см. раздел 3.2) и своему руководству об известных им или подозреваемых ими нарушениях информационной безопасности (Далее- ИБ), а также должны быть проинформированы о том, что ни при каких обстоятельствах они не должны пытаться использовать ставшие им известными слабые стороны системы безопасности.

2.3. Пользователи должны знать способы информирования об известных или предполагаемых случаях нарушения информационной безопасности с использованием телефонной связи, электронной почты и других методов. Необходимо обеспечить контроль и учет сообщений об инцидентах и принятие соответствующих мер.

2.4. Работникам учреждения запрещается распространять предупреждения о вирусах и иных угрозах безопасности, полученные от третьих лиц. Эти предупреждения необходимо перенаправлять в адрес ответственных лиц (см. раздел 3.2).

2.5. В случае обнаружения пропажи информационных ресурсов или компонентов информационных систем учреждения следует незамедлительно сообщить об этом своему непосредственному руководителю.

2.6. Расследование инцидентов (нарушений) информационной безопасности в Учреждении осуществляется в порядке, определенном

действующим законодательством РФ и внутренними документами Учреждения, и обязательно документируется.

2.7. ГБУЗ ПОКБ им. Н.Н. Бурденко осуществляет сбор соответствующих показаний (свидетельств), которые могут быть использованы для подтверждения действий, направленных против лица либо учреждения и (или) нарушающих его права, в порядке, определенном действующим законодательством.

2.8. Если инцидент ИБ может привести к судебному разбирательству против лица или организации, то информация о таком инциденте должна собираться, храниться и представляться согласно правилам оформления свидетельств, изложенным в соответствующих инструкциях.

2.9. Все инциденты ИБ должны быть идентифицированы, зафиксированы, доведены до соответствующих служб и решены (минимизированы негативные последствия).

3. Роли и ответственность

3.1. Ответственность за соблюдение данного Положения возлагается на всех работников ГБУЗ ПОКБ им. Н.Н. Бурденко и третьих лиц, использующих информационные ресурсы и системы учреждения.

3.2. Ответственность за реализацию данного Положения возлагается на: руководителей подразделений ГБУЗ ПОКБ им. Н.Н. Бурденко, работников, ответственных за администрирование сегментов информационной телекоммуникационной системы учреждения; работников, выполняющих следующие функции: администраторов информационных систем, администраторов локальной вычислительной сети, администраторов по обеспечению безопасности информации.

Приложение № 7
к приказу ГБУЗ «Пензенская
областная клиническая
больница им. Н.Н. Бурденко»
от_____№_____

Инструкция
по организации резервирования и восстановления программного обеспечения и баз персональных данных в информационных системах персональных данных в ГБУЗ ПОКБ им. Н.Н. Бурденко

1. Общие положения

1.1. Настоящая инструкция разработана в соответствии с требованиями подпункта «б» п. 13 Постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», с целью обеспечения возможности незамедлительного восстановления персональных данных (далее - ПДн), модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

1.2. Инструкция определяет правила и объемы резервирования, а также порядок восстановления работоспособности информационных систем персональных данных (далее - ИСПДн) ГБУЗ ПОКБ им. Н.Н. Бурденко.

2. Резервируемое программное обеспечение и базы персональных данных

2.1. В ИСПДн резервированию подлежит:

- общее программное обеспечение (операционная система и программные драйверы устройств (принтера, монитора, видеокарты и т.п.), поставляемые с компонентами автоматизированных рабочих мест (далее - АРМ), входящими в состав ИСПДн);
- прикладное программное обеспечение, используемое для обработки персональных данных (средства обработки текстов и таблиц, специализированные программы и т.п.);
- базы ПДн (тестовые и табличные файлы, а также файлы баз данных специализированных программ);
- программное обеспечение средств защиты информации, в том числе средств антивирусной защиты.

3. Порядок резервирования и хранения резервных копий

3.1. Резервирование общего и прикладного программного обеспечения, а также программного обеспечения средств защиты информации обеспечивается путем хранения у администратора безопасности информации в ИСПДн машинных носителей информации, содержащих дистрибутивы данного программного обеспечения.

3.2. Машинные носители информации обновлений общего и прикладного программного обеспечения, а также программного обеспечения средств защиты

информации должны также храниться у администратора безопасности информации в ИСПДн.

3.3. Допускается хранение машинных носителей прикладного программного обеспечения и машинных носителей с обновлениями к нему в структурных подразделениях, эксплуатирующих ИСПДн.

3.4. Резервирование баз ПДн, а также текстовых и табличных файлов, содержащих персональные данные, допускается только на учтенные установленным порядком машинные носители информации.

3.5. Резервирование осуществляется ежемесячно администратором безопасности информации ИСПДн, под контролем администратора ,ответственного за эксплуатацию ИСПДн.

3.6. Резервные носители ПДн хранятся в структурных подразделениях, эксплуатирующих ИСПДн, в порядке, предусмотренном для носителей информации ПДн.

3.7. К резервному носителю ПДн должна быть приложена учетная карточка, в которой делаются отметки о дате резервирования.

3.8. Резервные носители ПДн не могут быть переданы за пределы структурных подразделений, эксплуатирующих ИСПДн.

3.9. Копирование информации с резервных носителей ПДн, за исключением случая восстановления работоспособности ИСПДн, запрещается.

4. Порядок восстановления работоспособности ИСПДн

4.1. Восстановление работоспособности ИСПДн осуществляется в случаях сбоев, отказов и аварий технических средств и систем ИСПДн, а также ее программного обеспечения.

4.2. Данные работы осуществляются администратором безопасности информации в ИСПДн в соответствии с эксплуатационной документацией на программное обеспечение до полного восстановления работоспособности.

4.3. Восстановление ПДн, созданных после их последнего резервирования, осуществляется структурным подразделением, осуществляющим эксплуатацию ИСПДн.

4.4. В случае необходимости привлечения для восстановления работоспособности ИСПДн представителей сторонних организаций, должна быть обеспечена невозможность их ознакомления с ПДн. Ответственность за выполнение данного требования возлагается на администратора безопасности информации в ИСПДн и руководителя структурного подразделения, обеспечивающего ее эксплуатацию.

Приложение № 8
к приказу ГБУЗ «Пензенская
областная клиническая
больница им. Н.Н. Бурденко»
от_____№_____

Инструкция
по организации парольной защиты компьютеров
в ГБУЗ ПОКБ им. Н.Н. Бурденко

1. Данная инструкция призвана регламентировать организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) при работе на компьютерах с персональными данными.

2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей на компьютерах и контроль за действиями исполнителей при работе с паролями возлагается на ответственное лицо за работу с персональными данными ГБУЗ ПОКБ им. Н.Н. Бурденко.

3. Личные пароли должны генерироваться и распределяться централизованно либо выбираться исполнителями самостоятельно с учетом следующих требований:

- длина пароля должна быть не менее установленной (обычно 6-8 символов);
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, номера телефонов и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в заданном числе (например в 6-ти) позициях;
- личный пароль пользователь не имеет права сообщать никому.

4. Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

5. В случае, если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на ответственное лицо за работу с персональными данными ГБУЗ ПОКБ им. Н.Н. Бурденко. Для генерации «стойких» значений паролей могут применяться специальные программные средства. Система централизованной генерации и распределения паролей должна исключать возможность ознакомления в подразделениях с паролями других сотрудников подразделений.

6. При наличии технологической необходимости использования имен и паролей некоторых сотрудников (исполнителей) в их отсутствие (например, в случае возникновении нештатных ситуаций, форс-мажорных обстоятельств и

т.п.), такие сотрудники обязаны сразу же после смены своих паролей их новые значения (вместе с именами своих учетных записей) в запечатанном конверте или опечатанном пенале передавать на хранение ответственному за работу с персональными данными ГБУЗ ПОКБ им. Н.Н. Бурденко (руководителю своего подразделения). Опечатанные конверты (пеналы) с паролями исполнителей должны храниться в сейфе. Для опечатывания конвертов (пеналов) должны применяться личные печати владельцев паролей (при их наличии у исполнителей), либо печать подразделения.

7. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в месяц.

8. Внеплановая смена личного пароля или удаление учетной записи пользователя системы в случае прекращения его полномочий (увольнение, переход на другую работу внутри организации и т.п.) должна производиться ответственным за работу с персональными данными ГБУЗ ПОКБ им. Н.Н. Бурденко немедленно после окончания последнего сеанса работы данного пользователя с системой.

9. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и т.п.) администраторов средств защиты и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой подсистем АС.

10. В случае компрометации личного пароля пользователя системы должны быть немедленно предприняты меры по внеплановой смене паролей (в зависимости от полномочий владельца скомпрометированного пароля).

11. Хранение сотрудником (работником) значений своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у ответственного за работу с персональными данными ГБУЗ ПОКБ им. Н.Н. Бурденко.

Приложение № 9
к приказу ГБУЗ «Пензенская
областная клиническая
больница им. Н.Н. Бурденко»
от_____№_____

Инструкция
администратора информационных систем персональных данных, ответственного за эксплуатацию информационной системы персональных данных в ГБУЗ ПОКБ им. Н.Н. Бурденко

1. Общие положения

1.1. Настоящая инструкция определяет основные ответственность, права и обязанности ответственного за эксплуатацию информационной системы персональных данных (далее - ИСПДн) ГБУЗ ПОКБ им. Н.Н. Бурденко по вопросам защиты информации в ИСПДн, используемой в работе в учреждении.

1.2. Ответственный за эксплуатацию ИСПДн назначается приказом главного врача и осуществляет контроль за соблюдением порядка работы пользователей ИСПДн, установленного соответствующей инструкцией, на которых проводится обработка персональных данных, дополнительно к своим непосредственным обязанностям.

1.3. Ответственный за эксплуатацию ИСПДн непосредственно подчиняется ответственному за организацию обработки персональных данных (далее - ПДн) ГБУЗ ПОКБ им. Н.Н. Бурденко в части, касающейся защиты информации в ИСПДн, и осуществляет контроль за выполнением требований организационно-распорядительных документов по обеспечению безопасности информации при ее обработке в ИСПДн структурных подразделений Учреждения.

2. Обязанности ответственного за эксплуатацию ИСПДн

Ответственный за эксплуатацию ИСПДн обязан:

2.1. знать перечень автоматизированных рабочих мест (далее - АРМ), входящих в состав ИСПДн и перечень задач, решаемых с их использованием;

2.2. обеспечивать постоянный контроль за выполнением пользователями ИСПДн требований инструкций по обеспечению безопасности обработки ПДн;

2.3. немедленно сообщать ответственному за организацию обработки ПДн в части, касающейся защиты информации, об обнаруженных фактах (попытках) несанкционированного доступа к информации и АРМ, и принимать необходимые меры по пресечению нарушений;

2.4. организовать ведение «Журнала учета съёмных носителей ГБУЗ ПОКБ им. Н.Н. Бурденко»;

2.5. осуществлять контроль за правильностью использования и хранения машинных носителей информации и документов, содержащих ПДн;

2.6. осуществлять контроль за правильностью использования и хранения персональных идентификаторов и личных паролей пользователями;

2.7. разъяснять сотрудникам структурного подразделения вопросы

обеспечения информационной безопасности и правила работы с используемыми средствами защиты информации;

2.8. требовать от сотрудников структурного подразделения соблюдения правил организации парольной защиты (в соответствии с «Инструкцией по организации парольной защиты компьютеров государственного бюджетного учреждения здравоохранения «Пензенская областная клиническая больница им. Н.Н. Бурденко» (Приложение № 8);

2.9. контролировать использование сотрудниками и установленных на АРМ, входящих ИСПДн;

2.10. при подключении объектов критической инфраструктуры (Далее-КИИ) к локальным сетям проводить оценку возможности их подключения, осуществлять техническую возможность подключения, участвовать в настройке и пуско-наладке медицинского оборудования, с целью осуществления безопасности ПДн в ИСПДн.

2.11. контролировать прохождение антивирусного контроля (в соответствии с «Инструкцией по организации антивирусной защиты в информационных системах персональных данных» при применении машинных носителей информации;

2.12. немедленно прекращать работы на АРМ при несоблюдении установленной технологии обработки информации и невыполнении требований по безопасности.

3. Права ответственного за эксплуатацию ИСПДн

Ответственный за эксплуатацию ИСПДн имеет право:

3.1. требовать от пользователей ИСПДн соблюдения установленных технологий обработки информации и выполнения инструкций по обеспечению безопасности информации в ИСПДн;

3.2. Требовать доступ в помещения и к объектам КИИ при их установке, настройке, пуско-наладке, предоставлять замечания по техническому оснащению и подключению к локальной сети, с целью осуществления безопасности ПДн в ИСПДн.

3.2. инициировать проведение служебных расследований по фактам нарушения требований защиты информации, утвержденных соответствующими инструкциями, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов ИСПДн;

3.3. имеет право подавать свои предложения по совершенствованию организационных, технологических и технических мер защиты на своем участке работы.

Приложение № 10
к приказу ГБУЗ «Пензенская
областная клиническая
больница им. Н.Н. Бурденко»
от_____№_____

Инструкция
администратора безопасности информации в информационных системах персональных данных, эксплуатируемых в ГБУЗ ПОКБ им. Н.Н. Бурденко

1. Общие положения

1.1. Настоящая инструкция определяет основные обязанности, права и ответственность администратора безопасности информации в информационных системах персональных данных (далее - ИСПДн) ГБУЗ ПОКБ им. Н.Н. Бурденко (Далее –Учреждения).

1.2. Администратор безопасности информации в ИСПДн назначается приказом главного врача ГБУЗ ПОКБ им. Н.Н. Бурденко.

1.3. Администратор безопасности информации в ИСПДн (далее - Администратор безопасности информации) осуществляет контроль выполнения требований и организационных мероприятий по обеспечению защиты информации при использовании автоматизированных рабочих мест (далее - АРМ) дополнительно к своим непосредственным обязанностям.

2. Обязанности администратора безопасности информации в ИСПДн

2.1. Администратор безопасности информации обязан знать перечень установленного в ИСПДн программного обеспечения (далее - ПО).

2.2. Администратор безопасности информации обязан осуществлять постоянный контроль за выполнением сотрудниками структурных подразделений Учреждения, эксплуатирующими ИСПДн, мероприятий по обеспечению безопасности ПДн, обрабатываемых в ИСПДн.

2.3. Администратор безопасности информации обязан анализировать журнал системы защиты информации от несанкционированного доступа (далее - НСД), в случае отсутствия системы защиты от НСД журнал безопасности операционной системы.

2.4. Администратор безопасности информации обязан контролировать целостность печатей (пломб, защитных наклеек) на компонентах АРМ ИСПДн.

2.5. Администратор безопасности информации обязан немедленно ответственному за организацию обработки ПДн информацию об имевших место попытках несанкционированного доступа к информации и техническим средствам АРМ, а также принимать необходимые меры по устранению нарушений:

- установить причины, по которым стал возможным НСД;
- установить последствия, к которым привел НСД;
- зафиксировать случай НСД в виде документа (акта, служебной записки и т.д.) с описанием причин НСД, предполагаемых или установленных

нарушителей и последствий;

- провести проверку настроек средств защиты информации (далее - СЗИ) и операционных систем (далее - ОС) на соответствие требованиям руководящих документов ФСТЭК России и разрешительной системы доступа к ресурсам ИСПДн учреждения, при необходимости провести настройку;

- провести инструктаж пользователей ИСПДн по выполнению требований защиты.

2.6. Администратор безопасности информации обязан обеспечивать строгое выполнение требований по обеспечению защиты информации при организации технического обслуживания АРМ.

2.7. Администратор безопасности информации обязан вести журнал учета средств защиты информации используемых в ИСПДн и журнал учета съемных носителей персональных данных в ГБУЗ ПОКБ им. Н.Н. Бурденко.

2.8. Администратор безопасности информации обязан производить администрирование средств защиты персональных данных (далее - ПДн) в ИСПДн;

2.9. Администратор безопасности информации обязан присутствовать (участвовать) в работах по внесению изменений в аппаратно-программную конфигурацию АРМ.

2.10. Администратор безопасности информации обязан контролировать соответствие документально утвержденного состава аппаратной и программной конфигурации АРМ реальным конфигурациям АРМ ИСПДн.

2.11. Администратор безопасности информации обязан осуществлять контроль за порядком создания, учета, хранения и использования резервных и архивных копий массивов данных.

2.12. Администратор безопасности информации обязан проводить работу по выявлению возможных каналов вмешательства в процесс функционирования ИСПДн и осуществления НСД к информации и техническим средствам вычислительной техники. При выявлении таковых сообщать о них ответственному за организацию обработки ПДн.

2.13. Администратор безопасности информации обязан проводить инструктаж сотрудников - пользователей ИСПДн по правилам работы с используемыми техническими средствами и средствами защиты информации в соответствии с технической документацией на используемые средства защиты.

3. Права администратора безопасности информации в ИСПДн

3.1. Администратор безопасности информации имеет право требовать от сотрудников (пользователей ИСПДн) выполнения «Инструкции о порядке работы пользователей информационных систем персональных данных» в части обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных.

3.2. Администратор безопасности информации имеет право инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов ИСПДн.

3.3. Администратор безопасности информации имеет право обращаться к ответственному за организацию обработки ПДн с требованием прекращения

работы в ИСПДн при несоблюдении установленной технологии обработки информации и невыполнении требований по защите, обозначенных в документах из п. 3.1.

4. Ответственность администратора безопасности информации в ИСПДн

4.1. На администратора безопасности информации в ИСПДн возлагается персональная ответственность за качество проводимых им работ по обеспечению безопасности ПДн в ИСПДн в учреждении.

4.2. Администратор безопасности информации в ИСПДн несет ответственность по действующему законодательству за разглашение сведений ограниченного распространения, ставших известными ему по роду работы.

Приложение № 11
к приказу ГБУЗ «Пензенская
областная клиническая
больница им. Н.Н. Бурденко»
от_____№_____

Инструкция
о порядке работы пользователей информационных систем персональных данных, в части обеспечения безопасности данных при обработке в ГБУЗ ПОКБ им. Н.Н. Бурденко

1. Настоящая инструкция определяет порядок действий пользователей информационных систем персональных данных (далее - ИСПДн) в части обеспечения безопасности персональных данных (далее - ПДн) при их обработке в ИСПДн.

2. Допуск пользователей для работы за автоматизированным рабочим местом (далее - АРМ) осуществляется на основании трудового договора с работником учреждения.

3. Пользователь ИСПДн – работник ГБУЗ ПОКБ им. Н.Н. Бурденко, имеющий доступ для работы в информационных системах персональных данных.

4. Пользователь ИСПДн имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн. При этом для хранения информации, содержащей ПДн, разрешается использовать только машинные носители информации, учтенные в «журнале учета съёмных носителей персональных данных в ГБУЗ ПОКБ им. Н.Н. Бурденко».

5. Пользователь несет ответственность за правильность включения и выключения АРМ, входа в систему и все действия при работе в ИСПДн.

6. Вход пользователя в систему может осуществляться по выдаваемому ему электронному идентификатору или по персональному паролю.

7. Запись информации, содержащей ПДн, может, осуществляется пользователем ИСПДн на съемные машинные носители информации, соответствующим образом учтенные в «журнале учета съёмных носителей ГБУЗ ПОКБ им. Н.Н. Бурденко».

8. При работе со съемными машинными носителями информации пользователь каждый раз перед началом работы обязан проверить их на отсутствие вирусов и иных вредоносных программ с использованием штатных антивирусных средств, установленных на АРМ. В случае обнаружения вирусов либо вредоносных программ пользователь ИСПДн обязан немедленно прекратить их использование и действовать в соответствии с требованиями Инструкции по организации антивирусной защиты.

9. Каждый сотрудник, участвующий в рамках своих служебных обязанностей в процессах обработки персональных данных в ИСПДн и имеющий доступ к АРМ, программному обеспечению и данным ИСПДн, несет персональную ответственность за свои действия и обязан:

8.1. строго соблюдать установленные соответствующими Инструкциями правила обеспечения безопасности информации ИСПДн;

8.2. знать и строго выполнять правила работы со средствами защиты информации, установленными на АРМ;

8.3. хранить в тайне свой пароль (пароли). Выполнять требования Инструкции по организации парольной защиты в полном объеме;

8.4. хранить установленным порядком свое индивидуальное устройство идентификации (ключ) и другие реквизиты в сейфе (металлическом шкафу);

8.5. немедленно известить администратора безопасности информации в ИСПДн в случае утери индивидуального устройства идентификации (ключа) или при подозрении компрометации личных ключей и паролей, а также при обнаружении:

- нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на составляющих компонентах АРМ или иных фактов совершения в его отсутствие попыток несанкционированного доступа (далее - НСД) к АРМ;

- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации АРМ ИСПДн;

- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования компонентов АРМ, а также перебоев в системе электроснабжения;

- некорректного функционирования установленных на АРМ технических средств защиты;

- непредусмотренных отводов кабелей и подключенных устройств.

9. Пользователю АРМ категорически запрещается:

- использовать компоненты программного и аппаратного обеспечения АРМ в неслужебных целях;

- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИСПДн или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные архивом дистрибутивов установленного программного обеспечения АРМ;

- осуществлять обработку ПДн в присутствии посторонних (не допущенных к данной информации) лиц;

- записывать и хранить конфиденциальную информацию (содержащую персональные данные) на неучтенных машинных носителях информации (гибких магнитных дисках, флеш-накопителях и т.п.);

- оставлять включенным без присмотра АРМ, не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);

- оставлять без личного присмотра на рабочем месте или в ином месте свое персональное устройство идентификации, машинные носители и распечатки, содержащие персональные данные;

- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации;

- размещать средства ИСПДн так, чтобы с них существовала возможность визуального считывания информации.