Приложение 10
к приказу МБУДО
«Красноармейская ДШИ»
от 18.07.2017 № 28-о.д.

Инструкция
пользователя информационных систем персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий документ разработан в соответствии с нормативными документами по безопасности информации и определяет порядок обеспечения информационной безопасности при проведении работ пользователями информационных систем персональных данных (далее – ИСПДн) Муниципального бюджетного учреждения дополнительного образования «Красноармейская детская школа искусств» (далее – Учреждение).

1.2. Субъектами доступа к ресурсам ИСПДн являются администратор безопасности (далее – АБ), пользователи и обслуживающий персонал.

1.3. Обрабатываемая в ИСПДн информация относится к сведениям, составляющим персональные данные (далее – ПДн).

1.4. Машинные носители информации имеют пометку «ПДн».

1.5. Пользователи получают свои права на доступ к ресурсам ИСПДн через АБ.

1.6. Пользователи имеют право письменно вносить предложения по изменению и дополнению данной Инструкции.

1.7. Изменения и дополнения к данной Инструкции утверждаются в установленном порядке.

1.8. Право толкования положений настоящей Инструкции возлагается на Руководителя Учреждения.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

2.2. Автоматизированное рабочее место (АРМ) – персональный компьютер и подключенные к нему периферийные устройства – принтер, многофункциональные устройства, сканеры и т.д.

2.3. Доступ к информации – возможность получения информации и ее использования.

2.4. Защита информации — деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на информацию, то есть процесс, направленный на достижение информационной безопасности.

2.5. Информация - сведения (сообщения, данные) независимо от формы их представления.

2.6. Информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2.7. Несанкционированный доступ (НСД) – доступ к информации, хранящейся на различных типах носителей (бумажных, магнитных, оптических и т. д.) в компьютерных базах данных, файловых хранилищах, архивах, секретных частях и т. д. различных организаций путем изменения (повышения, фальсификации) своих прав доступа.

2.8. 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.

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

2.10. Средство защиты информации (СЗИ) – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

3. ОБЯЗАННОСТИ

Пользователь обязан:

3.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций и распоряжений, регламентирующих порядок действий по защите информации.

3.2. Выполнять на автоматизированном рабочем месте (далее – АРМ) только те процедуры, которые определены технологическим процессом обработки ПДн.

3.3. Знать и соблюдать установленные требования к обработке ПДн, учету и хранению носителей информации, обеспечению безопасности ПДн, а также руководящих и организационно-распорядительных документов.

3.4. Соблюдать требования парольной политики в соответствии с «Инструкцией по организации парольной защиты».

3.5. Получить уникальное имя и персональный идентификатор (при его наличии) от АБ. Пользователь обязан помнить и соблюдать в тайне свои имена и пароли, не допускается их запись на каких-либо носителях в целях напоминания.

3.6. Во время работы располагать экран монитора так, чтобы затруднить посетителям просмотр отображаемой информации. Жалюзи на окнах должны быть закрыты.

3.7. При возникновении подозрения на наличие вредоносного программного обеспечения (частые ошибки в работе программ, появление посторонних графических и

звуковых эффектов, искажения данных, неконтролируемое пропадание файлов, появление сообщений о системных ошибках, замедление работы компьютера и т.п.) самостоятельно или вместе с АБ ИСПДн провести внеочередной антивирусный контроль своего АРМ. При самостоятельном проведении антивирусного контроля - уведомить о результатах АБ ИСПДн для определения им факта наличия или отсутствия вредоносного программного обеспечения.

3.8. В случае появления информационного окна средства антивирусной защиты, сигнализирующем об обнаружении вредоносного программного обеспечения:

3.8.1. приостановить обработку данных;

3.8.2. немедленно поставить в известность о факте обнаружения вредоносного программного обеспечения АБ ИСПДн, владельца зараженных файлов, а также смежные структурные подразделения, использующие эти файлы в работе;

3.8.3. совместно с владельцем файлов, зараженных вредоносным программным обеспечением, провести анализ необходимости дальнейшего их использования;

3.8.4. произвести лечение или уничтожение зараженных файлов (для выполнения требований данного пункта привлечь АБ ИСПДн).

3.9. Немедленно вызывать АБ ИСПДн и поставить в известность руководителя структурного подразделения при обнаружении:

3.9.1. нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на аппаратных средствах АРМ или иных фактов совершения в его отсутствие попыток несанкционированного доступа к защищаемой АРМ;

3.9.2. несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств АРМ;

3.9.3. отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования узлов АРМ или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения;

3.9.4. некорректного функционирования установленных на АРМ технических средств защиты;

3.9.5. непредусмотренных отводов кабелей и подключенных к АРМ дополнительных устройств.

3.10. При утере или подозрении на утечку своего имени, пароля и персональных идентификаторов пользователь должен немедленно сообщить об этом АБ.

3.11. Обо всех выявленных нарушениях, связанных с информационной безопасностью Учреждения, а так же для получения консультаций по вопросам информационной безопасности, необходимо обратиться к АБ.

3.12. При отсутствии визуального контроля за рабочей станцией доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировка>.

3.13. В ИСПДн осуществляется блокирование сеанса доступа пользователя после

20 минут его бездействия (неактивности) в информационной системе.

3.14. Принимать меры по реагированию в случае возникновения внештатных ситуаций и аварийных ситуаций с целью ликвидации их последствий в пределах возложенных на него функций.

3.15. Пользователям **запрещается**:

- разглашать **защищаемую информацию** посторонним лицам;
- копировать защищаемую информацию на неучтенные внешние носители;
- самостоятельно устанавливать, тиражировать или модифицировать программное и аппаратное обеспечение, изменять установленный порядок функционирования технических и программных средств;
- подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства;
- отключать (блокировать) средства защиты информации;
- выполнять на АРМ работы, не предусмотренные технологическим процессом обработки ПДн;
- сообщать (или передавать) посторонним лицам параметры своей учетной записи (имя, персональный идентификатор (при его наличии) и пароль) в ИСПДн;
- оставлять без присмотра и передавать другим лицам персональный идентификатор;
- привлекать посторонних лиц для ремонта или настройки АРМ без согласования с ответственным за обеспечение безопасности ПДн;
- оставлять без присмотра свое АРМ, не активизировав блокировку доступа, или оставлять свое АРМ включенным по окончании работы;
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к нарушению безопасности персональных данных.

4. ПОРЯДОК РАБОТЫ ПОЛЬЗОВАТЕЛЯ С РЕСУРСАМИ ИСПДН

4.1. Начало работы на ПЭВМ

При включении ПЭВМ необходимо дождаться завершения загрузки и готовности системы защиты информации (далее – СЗИ) и операционной системы (далее – ОС) к идентификации пользователя. Идентификация пользователя осуществляется по уникальному имени и паролю с использованием персонального идентификатора, если таковой предусмотрен комплектацией СЗИ. Для получения доступа к ресурсам ИСПДн пользователь должен приложить к считывателю персональный идентификатор (при его наличии) и ввести с клавиатуры свой пароль. Если после ввода пароля СЗИ выдаст сообщение об ошибке, пользователь должен обратиться к АБ.

4.2. Завершение работы на ПЭВМ

По окончании работы пользователь должен либо завершить штатными средствами

сеанс своей работы (без выключения ПЭВМ), либо завершить работу ПЭВМ стандартным способом (при этом выключить ПЭВМ).

4.3. Требования к распечатыванию информации

Все распечатываемые документы должны быть учтены. Бракованные бумажные носители и черновики документов должны быть уничтожены.

При отсутствии пользователя на рабочем месте либо в присутствии лиц, не имеющих допуска к ресурсам ИСПДн, все документы, содержащие ПДн, должны быть недоступны для просмотра и иного их использования.

5. ОРГАНИЗАЦИЯ ПАРОЛЬНОЙ ЗАЩИТЫ

5.1. Личные пароли доступа к элементам ИСПДн выдаются пользователям АБ или создаются самостоятельно.

5.2. Полная плановая смена паролей в ИСПДн проводится не реже одного раза в 12 месяцев.

5.3. Правила формирования пароля:

– пароль должен состоять не менее чем из 6 символов;

– в пароле должны присутствовать символы из числа прописных и строчных букв английского алфавита от A до Z; десятичных цифр (от 0 до 9); символы, не принадлежащие алфавитно-цифровому набору (например, !, $, #, %);

– запрещается использовать в качестве пароля имя учетной записи, простые пароли типа «123», «111», «qwerty» и им подобные, а также имена и даты рождения пользователей ИСПДн и их родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно вычислить, основываясь на информации о пользователе;

– запрещается использовать в качестве пароля один и тот же повторяющийся символ, либо повторяющуюся комбинацию из нескольких символов;

– запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);

– запрещается выбирать пароли, которые уже использовались ранее.

5.4. Правила ввода пароля:

– ввод пароля должен осуществляться с учетом регистра, в котором пароль был задан;

– во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами.

5.5. Правила хранения пароля:

– запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах;

– запрещается сообщать другим пользователям личный пароль и/или регистрировать их в системе под своей учетной записью.

5.6. Лица, использующие паролирование, обязаны:

– четко знать и строго выполнять требования настоящей Инструкции и других руководящих документов по паролированию;

– своевременно сообщать АБ об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

6. ОТВЕТСТВЕННОСТЬ

6.1. Пользователь несет персональную ответственность за:

– сохранность носителей информации и содержащейся на них информации (в рабочее время);

– соблюдение требований данной Инструкции, неправомерное использование ресурсов ИСПДн и за все действия, совершенные от имени его учетной записи в ИСПДн, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учетной записи.

6.2. За разглашение персональных данных и нарушение порядка работы со средствами ИСПДн, содержащими персональные данные, работники могут быть привлечены к гражданской, уголовной, административной, дисциплинарной и иной предусмотренной законодательством Российской Федерации ответственности.

Приложение 11
к приказу МБУДО
«Красноармейская ДШИ»
от 18.07.2017 № 28-о.д.

Инструкция
о порядке работы с персональными данными

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Данная Инструкция разработана с целью защиты интересов Муниципального бюджетного учреждения дополнительного образования «Красноармейская детская школа искусств» (далее – Учреждение) и субъектов персональных данных, в целях предотвращения раскрытия (передачи), а также соблюдения надлежащих правил обращения с персональными данными.

1.2. Данная Инструкция предназначена для использования всеми работниками Учреждения, допущенными к работе с персональными данными.

1.3. Отнесение информации к сведениям, содержащим персональные данные, осуществляется в соответствии с «Перечнем персональных данных…».

1.4. Работники Учреждения, доступ которых к персональным данным необходим для выполнения ими своих трудовых обязанностей, должны быть ознакомлены под роспись с настоящей Инструкцией и предупреждены о возможной ответственности за ее нарушение.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. Информация – сведения (сообщения, данные) независимо от формы их представления.

2.2. Доступ к информации – возможность получения информации и ее использования.

2.3. Носитель информации – любой материальный объект или среда, используемый для хранения или передачи информации.

2.4. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу.

2.5. Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2.6. 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.

2.7. Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

3. ПОРЯДОК РАБОТЫ СО СВЕДЕНИЯМИ, СОДЕРЖАЩИМИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

3.1. При обработке персональных данных на бумажных и съемных носителях (дискетах, дисках, USB flash носителях и т.п.), компьютерах и других технических средствах, работники Учреждения обязаны следить как за сохранностью самих бумажных документов, съемных носителей, компьютеров и других технических средств, так и за сохранностью содержащейся в них информации, а именно не допускать неправомерного ознакомления с ней лиц, не имеющих допуска к работе с персональными данными.

3.2. Запрещается хранение или оставление бумажных документов и съемных носителей, содержащих персональные данные, в виде, позволяющем осуществить визуальный просмотр содержащихся в них персональных данных, их фотографирование или несанкционированное создание копий. Напечатанные документы, содержащие персональные данные, должны изыматься из принтеров немедленно. Хранение бумажных документов и съемных носителей, содержащих персональные данные, допускается только в специальных закрытых шкафах, сейфах и помещениях, к которым исключен доступ лиц, не допущенных к обработке соответствующих персональных данных.

3.3. Запрещается без прямой служебной необходимости делать выписки персональных данных, распечатывать документы с персональными данными или записывать персональные данные на съемные носители.

3.4. Запрещается использовать для передачи персональных данных съемные носители, не учтенные в соответствии с «Инструкцией по учету машинных носителей…».

3.5. Запрещается выносить документы, съемные носители или переносные компьютеры, содержащие персональные данные, за пределы служебных помещений Учреждения, если это не требуется для выполнения трудовых обязанностей и если на это не дано разрешение ответственного за организацию обработки персональных данных Учреждения.

3.6. Бумажные документы с персональными данными, у которых истек срок хранения, лишние или испорченные копии документов с персональными данными, должны быть уничтожены без возможности их восстановления (например, в шредерах).

3.7. Бумажные документы с персональными данными, съемные носители с персональными данными, а также встроенные в компьютеры носители с персональными данными должны уничтожаться под контролем ответственного за организацию обработки персональных данных способом, исключающим дальнейшее восстановление информации.

3.8. Мониторы компьютеров, использующихся для обработки персональных данных,

должны быть ориентированы таким образом, чтобы исключить визуальный просмотр информации с них лицами, не имеющими допуска к обработке персональных данных.

3.9. Категорически запрещается упоминать в разговоре с посторонними лицами сведения, содержащие персональные данные.

3.10. Запрещается в нерабочее время или за пределами служебных помещений упоминать в разговоре с кем-либо, включая любых работников Учреждения, сведения, содержащие персональные данные.

3.11. Запрещается обсуждать порядок доступа, места хранения, средства и методы защиты персональных данных с кем-либо, кроме ответственного за организацию обработки персональных данных, ответственного за обеспечение безопасности персональных данных, администратора безопасности, руководства, или лица, уполномоченного руководством на обсуждение данных вопросов.

4. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Работники Учреждения, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъектов, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с федеральными законами Российской Федерации.

4.2. Руководитель Учреждения за нарушение норм, регулирующих получение, обработку и защиту персональных данных субъектов, несет административную ответственность согласно ст. 5.27 и 5.39 Кодекса об административных правонарушениях Российской Федерации, а также возмещает субъекту ущерб, причиненный неправомерным использованием информации, содержащей персональные данные этого субъекта.

Приложение 12
к приказу МБУДО
«Красноармейская ДШИ»
от 18.07.2017 № 28-о.д.

Инструкция
по организации антивирусной защиты

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий документ разработан в соответствии с нормативными документами по безопасности информации и определяет требования к организации защиты информационной системы персональных данных (далее – ИСПДн) Муниципального бюджетного учреждения дополнительного образования «Красноармейская детская школа искусств» (далее – Учреждение) от разрушающего воздействия компьютерных вирусов и другого вредоносного программного обеспечения (далее – вредоносное ПО), устанавливает ответственность администратора безопасности (далее – АБ) за выполнение указанных требований.

2.1. К использованию в Учреждении допускаются только лицензионные средства антивирусной защиты, централизованно закупленные у разработчиков или поставщиков данных средств.

3.1. Установка средств антивирусного контроля на компьютеры и серверы ИСПДн Учреждения осуществляется АБ или под его контролем, настройка параметров средств антивирусного контроля осуществляется в соответствии с руководствами по применению конкретных антивирусных средств и требованиями нормативных документов ФСТЭК РФ в области защиты персональных данных.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

1.1. Антивирусная защита – комплекс мер, направленных на предотвращение, обнаружение и обезвреживание действий вредоносного ПО при помощи антивирусных программных продуктов.

2.1. Автоматизированное рабочее место (АРМ) – персональный компьютер и подключенные к нему периферийные устройства – принтер, многофункциональные устройства, сканеры и т.д.

3.1. Информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

4.1. Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу.

3. ПРИМЕНЕНИЕ СРЕДСТВ АНТИВИРУСНОГО КОНТРОЛЯ

1.1. Антивирусный контроль должен осуществляться в режиме постоянной

антивирусной защиты. Ежедневно в начале работы при загрузке компьютера (для серверов – при перезапуске) в автоматическом режиме должна проводиться проверка загружаемых модулей операционной системы.

2.1. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), хранящаяся на АРМ, передающаяся по сети, а также информация на съемных носителях. Контроль входящей информации должен осуществляться автоматически, непосредственно после ее приема.

3.1. Процедура обновления баз данных средства антивирусной защиты должна проводиться не реже одного раза в день на всех АРМ ИСПДн, работающих в сети, не реже одного раза в неделю для всех АРМ ИСПДн, работающих автономно.

4.1. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено АБ на предмет отсутствия вредоносного программного обеспечения. Непосредственно после установки (изменения) программного обеспечения должна быть выполнена антивирусная проверка на всех защищаемых серверах и АРМ ИСПДн.

5.1. При возникновении подозрения на наличие вредоносного программного обеспечения (частые ошибки в работе программ, появление посторонних графических и звуковых эффектов, искажения данных, неконтролируемое пропадание файлов, появление сообщений о системных ошибках, замедление работы компьютера и т.п.) пользователь обязан самостоятельно или вместе с АБ провести внеочередной антивирусный контроль своего АРМ. При самостоятельном проведении антивирусного контроля - уведомить о результатах АБ для определения им факта наличия или отсутствия вредоносного программного обеспечения.

4. **ОТВЕТСТВЕННОСТЬ**

1.1. Ответственность за проведение мероприятий антивирусного контроля и настройку средств антивирусного контроля в ИСПДн Учреждения в соответствии с требованиями настоящей Инструкции возлагается на АБ.

Периодический контроль за состоянием антивирусной защиты (обновление антивирусной программы и антивирусных баз, а также проверка работоспособности средств антивирусной защиты) в ИСПДн Учреждения, осуществляется АБ.

Приложение 13
к приказу МБУДО
«Красноармейская ДШИ»
от 18.07.2017 № 28-о.д.

Инструкция
по организации парольной защиты

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий документ разработан в соответствии нормативными документами по безопасности информации и регламентирует процессы генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационных системах персональных данных (далее – ИСПДн) Муниципального бюджетного учреждения дополнительного образования «Красноармейская детская школа искусств» (далее – Учреждение), а также контроль над действиями пользователей и обслуживающего персонала системы при работе с паролями.

1.2. Осуществление процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на администратора безопасности ИСПДн.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. Информация – сведения (сообщения, данные) независимо от формы их представления.

2.2. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу.

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

2.4. Пароль – секретная комбинация цифр, знаков, слов, или осмысленное предложение, служащие для защиты информации от несанкционированного доступа к информационным ресурсам.

2.5. Компрометация пароля – раскрытие, обнаружение или утеря пароля.

3. ПРАВИЛА ФОРМИРОВАНИЯ ПАРОЛЕЙ

3.1. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями информационной системы самостоятельно с учетом следующих требований:

- длина пароля должна быть не менее 6 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 имя пользователя, легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т.д.), последовательности символов и знаков (111, qwerty, абвгд и т.д.), общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетаний букв и знаков, которые можно угадать, основываясь на информации о пользователе;

- при смене пароля новое значение должно отличаться от предыдущего не менее чем в шести позициях.

3.2. Работникам допускается использовать пароли, составленные из первых букв слов запоминающихся высказываний в разном регистре, смешанные в произвольном порядке со специальными символами (например, Кожзгсф7!).

3.3. В случае если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на администратора безопасности ИСПДн.

3.4. Для обеспечения возможности использования имен и паролей некоторых работников в их отсутствие (например, в случае возникновении нештатных ситуаций, форс-мажорных обстоятельств и т.п.), работники обязаны сразу же после установки своих паролей передавать их на хранение вместе с именами своих учетных записей администратору безопасности ИСПДн в запечатанном конверте или опечатанном пенале. Опечатанные конверты (пеналы) с паролями работников должны храниться в сейфе, к которому исключен доступ других работников Учреждения и посторонних лиц. Для опечатывания конвертов (пеналов) должны применяться личные печати владельцев паролей (при их наличии), либо печать администратора безопасности ИСПДн. Все конверты (пеналы) с паролями в обязательном порядке фиксируются в «Журнале учета паролей пользователей…».

4. ВВОД ПАРОЛЯ

4.1. При вводе пароля пользователю необходимо исключить произнесение его вслух, возможность его просмотра посторонними лицами и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерами и т.п.).

4.2. При неверном вводе пароля более 5 раз, учетная запись пользователя должна блокироваться не менее чем на 3 минуты и не более чем на 15 минут.

5. ПОРЯДОК СМЕНЫ ЛИЧНЫХ ПАРОЛЕЙ

5.1. Смена паролей должна проводиться регулярно, не реже одного раза в 12 месяцев, самостоятельно каждым пользователем.

5.2. В случае прекращения полномочий пользователя (увольнение, переход на другую работу и т.п.) должно производиться немедленное удаление его учетной записи сразу после окончания последнего сеанса работы данного пользователя с системой.

5.3. Срочная (внеплановая) полная смена паролей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и т.п.) ответственного за

обеспечение безопасности персональных данных, администратора безопасности и других работников, которым по роду работы были предоставлены полномочия по управлению системой парольной защиты.

5.4. Администратор безопасности ИСПДн ведет «Журнал учета паролей пользователей...», в котором он отмечает причины внеплановой смены паролей пользователей.

5.5. Временный пароль, заданный администратором безопасности ИСПДн при регистрации нового пользователя, должен действовать в течение ограниченного срока времени. Пользователь должен изменить временный пароль при первом входе в систему.

6. ХРАНЕНИЕ ПАРОЛЯ

6.1. Запрещается записывать пароли на бумаге, в файле, электронной записной книжке, мобильном телефоне и любых других носителях информации.

6.2. Запрещается сообщать свой пароль полностью или частично другим пользователям, запрещается спрашивать или подсматривать пароль других пользователей.

6.3. Запрещается регистрировать других пользователей в ИСПДн со своим личным паролем, запрещается входить в ИСПДн под учетной записью и паролем другого пользователя.

7. ДЕЙСТВИЯ В СЛУЧАЕ УТЕРИ И КОМПРОМЕТАЦИИ ПАРОЛЯ

7.1. В случае утери или компрометации (разглашения, утраты) или подозрения в компрометации пароля пользователя должна быть немедленно проведена внеплановая процедура смены пароля.

8. ОТВЕТСТВЕННОСТЬ

8.1. Каждый пользователь ИСПДн несет персональную ответственность за соблюдение требований настоящей Инструкции и за все действия, совершенные от имени его учетной записи в ИСПДн, если с его стороны не было предпринято необходимых действий для предотвращения компрометации пароля его учетной записи.

8.2. Ответственность за контроль проведения мероприятий по организации парольной защиты в отделах возлагается на ответственного за обеспечение безопасности персональных данных.

8.3. За разглашение персональных данных и нарушение порядка работы со средствами ИСПДн, обрабатывающими персональные данные, работники могут быть привлечены к гражданской, уголовной, административной, дисциплинарной и иной предусмотренной законодательством Российской Федерации ответственности.