

6

МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 21 г. Сальска

ПРИНЯТО

педагогическим советом
МБОУ СОШ № 21 г. Сальска
Протокол № 1
от "30" августа 2013 г.

УТВЕРЖДЕНО

приказом № 261 от "30" августа 2013 г.
директор МБОУ СОШ № 21 г. Сальска
 С.Г. Хомутова /

Положение

Об обработке и защите персональных данных работников, состоящих в трудовых отношениях с муниципальным бюджетным общеобразовательным учреждением средней общеобразовательной школой № 21 г. Сальска

1. Общие положения

Настоящее Положение устанавливает порядок приема, учета, сбора, поиска, обработки, накопления и хранения документов, содержащих сведения, отнесенные к персональным данным сотрудников муниципального бюджетного общеобразовательного учреждения средней общеобразовательной школы № 21 г. Сальска. (Далее – Учреждение). Под сотрудниками подразумеваются лица, имеющие трудовые отношения с МБОУ СОШ № 21 г. Сальска.

1.1. Цель

Настоящее Положение является локальным актом, регламентирующим деятельность учреждения, направленную на обеспечение защиты персональных данных, хранящихся у работодателя.

1.2. Основания

Основанием для разработки данного Положения являются:

- Конституция РФ;
- Трудовой кодекс РФ;
- Кодекс РФ об административных правонарушениях;
- ФЗ от 20.02.1995 № 24 «Об информации, информатизации и защите информации»;
- Указ Президента РФ № 188 от 06.09.1997 «Об утверждении перечня сведений конфиденциального характера»;
- ФЗ РФ от 27.07.2006 № 152 –ФЗ «О персональных данных».

1.3. Положение о защите персональных данных и изменения к нему вводятся приказом по основной деятельности МБОУ СОШ № 21 г. Сальска. Все сотрудники учреждения должны быть ознакомлены под расписку с данным Положением.

1.3. Понятие и состав персональных данных

Под персональными данными сотрудников понимается конфиденциальная, строго охраняемая информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного сотрудника, а также сведения о фактах, событиях и обстоятельствах жизни сотрудника, позволяющие идентифицировать его личность. К персональным данным относятся:

- все биографические сведения сотрудника;
- образование;

- специальность;
- занимаемая должность;
- наличие судимостей;
- адрес местожительства;
- домашний телефон;
- состав семьи;
- место работы или учебы членов семьи и родственников;
- размер заработной платы;
- содержание трудового договора;
- состав декларируемых сведений о наличии материальных ценностей;
- содержание декларации, подаваемой в налоговую инспекцию;
- подлинники и копии приказов по личному составу;
- личные дела, личные карточки (форма Т2) и трудовые книжки сотрудников;
- основания к приказам по личному составу;
- дела, содержащие материалы по повышению квалификации и переподготовке сотрудников, их аттестации, служебным расследованиям;
- копии отчетов, направляемые в органы статистики;
- анкета;
- копии документов об образовании;
- результаты медицинского обследования на предмет годности к осуществлению трудовых обязанностей;
- фотографии и иные сведения, относящиеся к персональным данным сотрудника.

Указанные документы являются конфиденциальными соответствующий гриф ограничения на них не ставится ввиду их массовости и единого места обработки и хранения.

Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении 75 лет срока хранения, если иное не определено законом.

Собственником информационных ресурсов (персональных данных) – является субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения этими ресурсами. Это любой гражданин, к личности которого относятся соответствующие персональные данные, и который вступил (стал сотрудником) или изъявил желание вступить в трудовые отношения с работодателем. Субъект персональных данных самостоятельно решает вопрос передачи работодателю своих персональных данных.

Держателем персональных данных является работодатель, которому сотрудник добровольно передает во владение свои персональные данные. Работодатель выполняет функцию владения этими данными и обладает полномочиями распоряжения ими в пределах, установленных законодательством.

Права и обязанности работодателя в трудовых отношениях осуществляются физическим лицом, уполномоченным работодателем. Указанные права и обязанности он может делегировать нижестоящим руководителям – своим заместителям, работа которых требует знания персональных данных работников или связана с обработкой этих данных.

Потребителями (пользователями) персональных данных являются юридические и физические лица, обращающиеся к собственнику или держателю персональных данных за получением необходимых сведений и пользующиеся ими без права передачи и разглашения.

3. Принципы обработки персональных данных

Обработка персональных данных включает в себя их получение, хранение, комбинирование, передачу, а также актуализацию, блокирование, защиту, уничтожение.

Получение, хранение, комбинирование, передача или любое другое использование персональных данных сотрудника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности сотрудников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

Все персональные данные сотрудника получаются у него самого. Если персональные данные сотрудника возможно получить только у третьей стороны, то сотрудник должен быть уведомлен об этом заранее, и от него должно быть получено письменное согласие. Работодатель должен сообщить сотруднику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа сотрудника дать письменное согласие на их получение.

Не допускается получение и обработка персональных данных сотрудника о его политических, религиозных и иных убеждениях и частной жизни, а также о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных законодательством РФ.

При принятии решений относительно сотрудника на основании его персональных данных не допускается использование данных, полученных исключительно в результате их автоматизированной обработки или электронного получения.

В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции РФ возможно получение и обработка данных о частной жизни сотрудника только с его письменного согласия.

Пакет анкетно - биографических и характеризующих материалов (далее пакет) сотрудника формируется после издания приказа о его приеме на работу. Пакет обязательно содержит личную карточку формы Т-2, а также может содержать документы, содержащие персональные данные сотрудника, в порядке, отражающем процесс приема на работу.

Все документы хранятся в папках в алфавитном порядке фамилий сотрудников.

Пакет пополняется на протяжении всей трудовой деятельности сотрудника в данной организации. Изменения, вносимые в карточку Т-2, должны быть подтверждены соответствующими документами (например, копия свидетельства о браке).

Сотрудник отдела кадров, ответственный за документационное обеспечение кадровой деятельности, принимает от принимаемого на работу сотрудника документы, проверяет полноту их заполнения и правильность указываемых сведений в соответствии с предъявленными документами.

Под блокированием персональных данных понимается временное прекращение операций по их обработке по требованию субъекта персональных данных при выявлении им недостоверности обрабатываемых сведений или неправомерных действий в отношении его данных.

Сотрудник обязан:

- передавать работодателю или его представителю комплекс достоверных, документированных персональных данных, состав которых предусмотрен законодательством РФ;
- своевременно сообщать работодателю об изменении своих персональных данных.

Сотрудник имеет право на:

- полную информацию о своих персональных данных и обработке этих данных;
- свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные сотрудника, за исключением случаев, предусмотренных законодательством РФ;
- определение своих представителей для защиты своих персональных данных;
- требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований. При отказе работодателя исключить или исправить персональные данные сотрудника он имеет право заявить в письменной форме работодателю о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера сотрудник имеет право дополнить заявлением, выражающим его собственную точку зрения;
- требование об извещении работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные сотрудника, обо всех произведенных в них исключениях, исправлениях или дополнениях;
- обжалование в суд любых неправомерных действий или бездействия работодателя при обработке и защите его персональных данных.

4. Доступ к персональным данным

Персональные данные добровольно передаются сотрудником непосредственно держателю этих данных и потребителям внутри МБОУ СОШ №21 г.Сальска исключительно для обработки и использования в работе.

Внешний доступ. К числу массовых потребителей персональных данных вне МБОУ СОШ №21 г.Сальска можно отнести государственные и муниципальные структуры:

- налоговая инспекция;
- правоохранительные органы;
- органы статистики;
- военный комиссариат;
- органы социального страхования;
- пенсионный фонд;
- органы местного самоуправления;
- министерство образования;
- МУ РЦО;
- МУ ИМЦ;
- УО Сальского района.

В кадровой службе хранятся личные дела, трудовые книжки сотрудников, работающих в настоящее время. Для этого используются шкафы и сейф, которые закрываются на ключ. Личные карточки формы Т-2 располагаются в алфавитном порядке.

После увольнения документы по личному составу передаются на хранение в архив Учредителя.

5. Передача персональных данных

При передаче персональных данных сотрудника работодатель должен соблюдать следующие требования:

Передача внешнему потребителю:

- передача персональных данных от держателя или его представителей внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных;
- при передаче персональных данных сотрудника потребителям за пределы МБОУ СОШ №21 г.Сальска работодатель не должен сообщать эти данные третьей стороне без письменного согласия сотрудника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью сотрудника или в случаях, установленных федеральным законом;
- ответы на правомерные письменные запросы других учреждений и организаций даются с разрешения директора МБОУ СОШ №21 г.Сальска только в письменной форме и в том объеме, который позволяет не разглашать излишний объем персональных сведений;
- не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу;
- по возможности персональные данные обезличиваются.

Передача внутреннему потребителю. Работодатель вправе разрешать доступ к персональным данным сотрудников внутреннему потребителю, на которого возлагается ответственность за соблюдение конфиденциальности информации. Потребители персональных данных должны подписать обязательство о неразглашении персональных данных сотрудников (Приложение №1).

6. Защита персональных данных

Под угрозой или опасностью утраты персональных данных понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей, внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

Защита персональных данных представляет собой жестко регламентированный технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой деятельности учреждения.

6.1. «Внутренняя защита»

Основным виновником несанкционированного доступа к персональным данным является, как правило, персонал, работающий с документами и базами данных. Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий и ответственности внутренних пользователей конфиденциальной информацией.

Для защиты персональных данных сотрудников необходимо соблюдать ряд мер:

- ограничение и регламентация состава сотрудников, функциональные обязанности которых требуют конфиденциальных знаний;
- строгое избирательное и обоснованное распределение документов и информации между сотрудниками;

- рациональное размещение рабочих мест сотрудников, при котором исключалось бы бесконтрольное использование защищаемой информации;
- знание сотрудниками требований нормативно – методических документов по защите информации и сохранении тайны;
- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- определение и регламентация состава сотрудников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;
- организация порядка уничтожения информации;
- своевременное выявление нарушения требований разрешительной системы доступа сотрудниками учреждения;
- воспитательная и разъяснительная работа с сотрудниками учреждения по предупреждению утраты ценных сведений при работе с конфиденциальными документами;
- не допускается выдача личных дел сотрудников на рабочие места заместителей директора; личные дела могут выдаваться на рабочее место только руководителю учреждения;
- персональные компьютеры, в которых содержатся персональные данные, должны быть защищены паролями доступа.

6.2. «Внешняя защита»

Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лиц, пытающихся совершить несанкционированный доступ и овладение информацией. Целью и результатом несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др.

Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности учреждения: посетители, сотрудники школы, родители. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в кадровой службе.

Для защиты персональных данных сотрудников необходимо соблюдать ряд мер:

- порядок приема, учета и контроля деятельности посетителей;
- пропускной режим учреждения;
- порядок охраны территории, учебного корпуса, внутренних помещений, транспортного средства.

7. Ответственность за разглашение конфиденциальной информации, связанной с персональными данными

Персональная ответственность – одно из главных требований к организации функционирования системы защиты персональной информации и является обязательным условием обеспечения эффективности этой системы.

Руководитель, разрешающий доступ сотрудника к конфиденциальному документу, несет персональную ответственность за данное разрешение.

Каждый сотрудник учреждения, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

Нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) влечет дисциплинарную, административную, гражданско-правовую или уголовную ответственность граждан и юридических лиц.

Приложение 1

Список работников, допущенных к обработке персональных данных

№ п/п	Ф.И.О. работника	Должность	Дата приема на работу	Адрес, телефон	Примечание

Приложение 2

ЖУРНАЛ

обращений по ознакомлению с персональными данными

№ п/п	Ф.И.О. работника	Дата обращения	Запрашиваемый документ (данные)	Отметка о выполнении	Подпись заявителя	Примечание

АНКЕТА

для родителей (законных представителей)*

Ф.И.О.: _____

Дата рождения: _____

Образование: _____

Место работы: _____

Занимаемая должность: _____

Домашний адрес: _____

Домашний телефон: _____

Служебный телефон: _____

E-mail: _____

Дата заполнения: " ____ " 20 ____ г. Личная подпись

ИНСТРУКЦИЯ

о порядке обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные

I. Общие положения

1. Инструкция о порядке обеспечения конфиденциальности при обращении с информацией, содержащей персональные данные (далее - Инструкция), является обязательной для всех структурных подразделений образовательного учреждения (далее - ОУ).

2. Под персональными данными понимается любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в т. ч. его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное и имущественное положение, образование, профессия, доходы и др.

3. Обеспечение конфиденциальности персональных данных не требуется в случае обезличивания персональных данных, а также в отношении общедоступных персональных данных.

В общедоступные источники персональных данных (в т. ч. справочники, адресные книги) в целях информационного обеспечения с письменного согласия субъекта персональных данных могут включаться его фамилия, имя, отчество, год и место рождения, адрес и другие сведения.

4. Конфиденциальность персональных данных предусматривает обязательное получение согласия субъекта персональных данных (наличие иного законного основания) на их обработку. Согласие не требуется на обработку данных:

- необходимых для доставки почтовых отправлений организациями почтовой связи;
- включающих в себя только фамилию, имя и отчество субъекта;
- работа с которыми проводится в целях исполнения обращения (запроса) субъекта персональных данных, трудового или иного договора с ним, однократного пропуски в здание или в иных аналогичных целях;
- обработка которых осуществляется без средств автоматизации.

5. Порядок ведения перечней персональных данных в структурных подразделениях ОУ утверждается локальным актом. Осуществлять обработку и хранение конфиденциальных данных, не внесенных в перечень, запрещается.

6. Все работники, постоянно работающие в помещениях, в которых ведется обработка персональных данных, должны иметь допуск (разрешение) к работе с соответствующими видами персональных данных.

7. Работникам, осуществляющим обработку персональных данных, запрещается сообщать их устно или письменно кому бы то ни было, если это не вызвано служебной необходимостью, а также оставлять материальные носители с персональными данными без присмотра в незапертом помещении. После подготовки и передачи документа в соответствии с резолюцией файлы черновиков и вариантов документа должны переноситься подготовившим их работником на маркированные носители, предназначенные для хранения персональных данных. Без согласования с руководителем структурного подразделения формирование и хранение баз данных (картотек, файловых архивов и др.), содержащих конфиденциальные данные, запрещается.

8. Передача персональных данных допускается только в случаях, установленных Федеральными законами от 27.07.2006 № 152-ФЗ "О персональных данных" и от 02.05.2006 № 59-ФЗ "О порядке рассмотрения обращений граждан Российской Федерации", действующими инструкциями по работе со служебными документами и обращениями граждан, а также по письменному поручению (резолюции) вышестоящих должностных лиц.

Запрещается передача персональных данных по телефону, факсу, электронной почте, за исключением случаев, установленных законодательством и действующими инструкциями по работе со служебными документами и обращениями граждан. Ответы на запросы граждан и организаций даются в том объеме, который позволяет не разглашать конфиденциальные данные, за исключением данных, содержащихся в материалах заявителя или опубликованных в общедоступных источниках.

10. Ответственность за защиту обрабатываемых персональных данных возлагается на работников подразделений ОУ, осуществляющих такую обработку по договору с оператором, а также на иные лица, осуществляющие обработку или хранение конфиденциальных данных в ОУ. Лица, виновные в нарушении норм, регулирующих обработку и хранение конфиденциальных данных, несут дисциплинарную, административную и уголовную ответственность в соответствии с законодательством РФ и ведомственными нормативными актами.

II. Порядок обеспечения безопасности при обработке и хранении персональных данных, осуществляемых без использования средств автоматизации

11. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна быть организована таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения материальных носителей персональных данных и установить перечень лиц, осуществляющих обработку.

12. При хранении материальных носителей необходимо соблюдать условия, обеспечивающие сохранность персональных данных и исключая несанкционированный доступ к ним. Лица, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть проинформированы о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также об особенностях и правилах выполнения такой обработки.

13. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях. При фиксации персональных данных на материальных носителях не допускается на одном материальном носителе размещать персональные данные, цели обработки которых заведомо не совместимы. Для обработки персональных данных каждой категории должен использоваться отдельный материальный носитель.

14. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, и невозможности обработки одних персональных данных

отдельно от других, зафиксированных на том же носителе, должны быть приняты меры по обеспечению раздельной обработки персональных данных, исключающие одновременное копирование иных персональных данных, не подлежащих распространению и использованию.

15. Уничтожение или обезличивание всех или части персональных данных (если это допускается материальным носителем) производится способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание). Уточнение персональных данных производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

III. Порядок обеспечения безопасности при обработке и хранении персональных данных, осуществляемых с использованием средств автоматизации

16. Безопасность персональных данных при их обработке в информационных системах, хранении и пересылке обеспечивается с помощью системы защиты персональных данных, включающей специальные средства защиты информации, а также используемые в информационной системе информационные технологии.

17. Допуск лиц к обработке персональных данных в информационных системах осуществляется на основании соответствующих разрешительных документов и ключей (паролей) доступа.

18. Работа с информационными системами должна быть организована таким образом, чтобы обеспечить сохранность носителей персональных данных и средств защиты информации, а также исключить возможность неконтролируемого пребывания в помещениях, где они находятся, посторонних лиц.

19. Компьютеры и (или) электронные папки, в которых содержатся файлы с персональными данными, для каждого пользователя должны быть защищены индивидуальными паролями доступа, состоящими из шести и более символов.

20. Работа на компьютерах с персональными данными без паролей доступа или под чужими или общими (одинаковыми) паролями, а также пересылка персональных данных без использования специальных средств защиты по общедоступным сетям связи, в т. ч. сети Интернет, запрещается.

21. При обработке персональных данных в информационных системах пользователями должно быть обеспечено:

- использование предназначенных для этого разделов (каталогов) носителей информации, встроенных в технические средства, или съемных маркированных носителей;
- недопущение физического воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
- постоянное использование антивирусного обеспечения для обнаружения зараженных файлов и незамедлительное восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- недопущение несанкционированного выноса из помещений, установки и подключения оборудования, а также удаления, инсталляции или настройки программного обеспечения.

22. При обработке персональных данных в информационных системах разработчики и администраторы систем должны обеспечивать:

- обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;
- учет лиц, допущенных к работе с персональными данными в информационных системах, прав и паролей доступа;
- учет применяемых средств защиты информации, эксплуатационной и технической документации к ним;
- контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
- описание системы защиты персональных данных.

23. Специфические требования к защите персональных данных в отдельных автоматизированных системах устанавливаются инструкциями по их использованию и эксплуатации.

24. Работники подразделений ОУ и лица, выполняющие работы по договорам и контрактам, имеющие отношение к обработке персональных данных, должны быть ознакомлены с Инструкцией под расписку.

Приложение 5

ИНСТРУКЦИЯ

пользователя, осуществляющего обработку персональных данных на объектах вычислительной техники

I. Общие положения

1. Инструкция пользователя, осуществляющего обработку персональных данных на объектах вычислительной техники (далее - Инструкция), регламентирует основные обязанности, права и ответственность пользователя, допущенного к автоматизированной обработке персональных данных и иной конфиденциальной информации на объектах вычислительной техники (ПЭВМ) образовательного учреждения (далее - ОУ).

2. Инструкция регламентирует деятельность пользователя, который имеет допуск к обработке соответствующих категорий персональных данных и обладает необходимыми навыками работы на ПЭВМ.

II. Обязанности пользователя

3. При выполнении работ в пределах своих функциональных обязанностей пользователь несет персональную ответственность за соблюдение требований нормативных документов по защите информации.

4. Пользователь обязан:

- выполнять требования Инструкции по обеспечению режима конфиденциальности проводимых работ;
- при работе с персональными данными исключать присутствие в помещении, где расположены средства вычислительной техники, не допущенных к обрабатываемой информации лиц, а также располагать во время работы экран видеомонитора так, чтобы отображаемая на нем информация была недоступна для просмотра посторонними лицами;
- соблюдать правила работы со средствами защиты информации, а также установленный режим разграничения доступа к техническим средствам, программам, данным и файлам с персональными данными при ее обработке;

- после окончания обработки персональных данных в рамках выполнения одного задания, а также по окончании рабочего дня производить стирание остаточной информации с жесткого диска ПЭВМ;
- оповещать обслуживающий ПЭВМ персонал, а также непосредственного руководителя обо всех фактах или попытках несанкционированного доступа к информации, обрабатываемой в ПЭВМ;
- не допускать "загрязнения" ПЭВМ посторонними программными средствами;
- знать способы выявления нештатного поведения используемых операционных систем и пользовательских приложений, меры предотвращения ухудшения ситуации;
- знать и соблюдать правила поведения в экстренных ситуациях, порядок действий при ликвидации последствий аварий;
- помнить личные пароли и персональные идентификаторы;
- знать штатные режимы работы программного обеспечения, пути проникновения и распространения компьютерных вирусов;
- при применении внешних носителей информации перед началом работы проводить их проверку на наличие компьютерных вирусов.

5. 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.) пользователь должен провести внеочередной антивирусный контроль своей рабочей станции. В случае обнаружения зараженных компьютерными вирусами файлов пользователь обязан:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов своего непосредственного руководителя, администратора системы, а также смежные подразделения, использующие эти файлы в работе;
- оценить необходимость дальнейшего использования файлов, зараженных вирусом;
- провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта следует привлечь администратора системы).

6. Пользователю ПЭВМ запрещается:

- записывать и хранить персональные данные на неуценных в установленном порядке машинных носителях информации;
- удалять с обрабатываемых или распечатываемых документов грифы конфиденциальности;
- самостоятельно подключать к ПЭВМ какие-либо устройства, а также вносить изменения в состав, конфигурацию и размещение ПЭВМ;
- самостоятельно устанавливать и/или запускать на ПЭВМ любые системные или прикладные программы, загружаемые по сети Интернет или с внешних носителей;
- осуществлять обработку персональных данных в условиях, позволяющих просматривать их лицами, не имеющими к ним допуска, а также нарушающих требования к эксплуатации ПЭВМ;
- сообщать кому-либо устно или письменно личные атрибуты доступа к ресурсам ПЭВМ;

- отключать (блокировать) средства защиты информации;
- производить какие-либо изменения в подключении и размещении технических средств;
- производить иные действия, ограничения на исполнение которых предусмотрены утвержденными регламентами и инструкциями;
- бесконтрольно оставлять ПЭВМ с загруженными персональными данными, установленными маркированными носителями, электронными ключами и выведенными на печать документами, содержащими персональные данные.

III. Права пользователя

7. Пользователь ПЭВМ имеет право:

- обрабатывать (создавать, редактировать, уничтожать, копировать, выводить на печать) информацию в пределах установленных ему полномочий;
- обращаться к обслуживающему ПЭВМ персоналу с просьбой об оказании технической и методической помощи при работе с общесистемным и прикладным программным обеспечением, установленным в ПЭВМ, а также со средствами защиты информации.

IV. Заключительные положения

8. Особенности обработки персональных данных пользователями отдельных автоматизированных систем могут регулироваться дополнительными инструкциями.

9. Работники подразделений ОУ и лица, выполняющие работы по договорам и контрактам и имеющие отношение к обработке персональных данных на объектах вычислительной техники, должны быть ознакомлены с Инструкцией под расписку.

Приложение 6

ИНСТРУКЦИЯ

по проведению мониторинга информационной безопасности и антивирусного контроля

1. Инструкция по проведению мониторинга информационной безопасности и антивирусного контроля (далее - Инструкция) регламентирует порядок планирования и проведения мероприятий, направленных на обеспечение безопасности автоматизированных систем, обрабатывающих персональные данные, от несанкционированного доступа, распространения, искажения и утраты информации, необходимой в работе образовательного учреждения (далее - ОУ).
2. Мониторинг работоспособности аппаратных компонентов автоматизированных систем, обрабатывающих персональные данные, осуществляется в процессе их администрирования и при проведении работ по техническому обслуживанию оборудования. Наиболее существенные компоненты системы, имеющие встроенные средства контроля работоспособности (серверы, активное сетевое оборудование), должны постоянно контролироваться в рамках работы администраторов соответствующих систем.
3. Мониторинг парольной защиты предусматривает:
 - контроль соблюдения сроков действия паролей (не более трех месяцев);
 - периодическую (не реже одного раза в месяц) проверку пользовательских паролей на количество символов и очевидность с целью выявления слабых паролей, которые легко угадать или дешифровать с помощью специализированных программных средств ("взломщиков" паролей).
4. Мониторинг целостности программного обеспечения включает:
 - проверку контрольных сумм и цифровых подписей каталогов и файлов сертифицированных программных средств при загрузке операционной системы;

- сверку дубликатов идентификаторов пользователей;
- проверку и восстановление системных файлов администраторами систем с резервных копий при несовпадении контрольных сумм.

5. Мероприятия, направленные на предупреждение и своевременное выявление попыток несанкционированного доступа, в т. ч. выявление фактов сканирования определенного диапазона сетевых портов в короткие промежутки времени с целью обнаружения сетевых анализаторов, изучающих систему и определяющих места ее уязвимости, осуществляются с использованием средств операционной системы и специальных программных средств. Они должны сопровождаться фиксацией неудачных попыток входа в систему в системном журнале и протоколированием работы сетевых сервисов.

6. Мониторинг производительности автоматизированных систем, обрабатывающих персональные данные, осуществляется по обращениям пользователей в ходе администрирования систем

и проведения профилактических работ для выявления попыток несанкционированного доступа, повлекших существенное уменьшение производительности.

7. Системный аудит производится ежеквартально и в особых ситуациях. Он включает в себя проведение обзоров безопасности, тестирование системы и контроль внесения изменений в системное программное обеспечение.

8. Обзоры безопасности проводятся с целью проверки соответствия текущего состояния систем, обрабатывающих персональные данные, уровню безопасности, удовлетворяющему требованиям политики безопасности, и включают:

- составление отчетов о безопасности пользовательских ресурсов (в т. ч. о наличии повторяющихся пользовательских имен и идентификаторов, неправильных форматах регистрационных записей, пользователей без пароля, неправильной установке домашних каталогов пользователей и уязвимостях пользовательских окружений);
- проверку содержимого файлов конфигурации на соответствие списку для проверки;
- анализ данных об обнаружении изменений системных файлов со времени проведения последней проверки (контроль целостности системных файлов);
- проверку прав доступа и других атрибутов системных файлов (команд, утилит и таблиц);
- оценку правильности настройки механизмов аутентификации и авторизации сетевых сервисов;
- проверку корректности конфигурации системных и активных сетевых устройств (мостов, маршрутизаторов, концентраторов и сетевых экранов).

9. Активное тестирование надежности механизмов контроля доступа производится путем осуществления попыток проникновения в информационную систему с помощью автоматического инструментария или вручную.

10. Пассивное тестирование механизмов контроля доступа осуществляется путем анализа конфигурационных файлов системы. Сначала информация об известных уязвимостях извлекается из документации и внешних источников, а затем осуществляется проверка конфигурации системы с целью выявления опасных состояний системы, т. е. таких состояний, в которых могут проявлять себя известные уязвимости. Если система находится в опасном состоянии, то с целью нейтрализации уязвимостей необходимо выполнить одно из следующих действий:

- изменить конфигурацию системы (для ликвидации условий проявления уязвимости);

- установить программные коррективы либо другие версии программ, в которых данная уязвимость отсутствует;
- отказаться от использования системного сервиса, содержащего данную уязвимость.

И. Внесение изменений в системное программное обеспечение осуществляется администраторами систем, обрабатывающих персональные данные, с обязательным соблюдением следующих условий:

- документирование изменений в соответствующем журнале;
- уведомление работника, которого касается изменение;
- анализ претензий, в случае если это изменение причинило кому-нибудь вред;
- разработка планов действий в аварийных ситуациях для восстановления работоспособности системы, если внесенное в нее изменение вывело ее из строя.

12. Для защиты от вредоносных программ и вирусов необходимо использовать только лицензионные или сертифицированные свободно распространяемые антивирусные средства.

13. Для защиты серверов и рабочих станций используются:

- резидентные антивирусные мониторы, контролирующие подозрительные действия программ;
- утилиты для обнаружения и анализа новых вирусов.

14. При подозрении на наличие не выявленных установленными средствами защиты заражений следует использовать Live CD с другими антивирусными средствами.

15. Установка и настройка средств защиты от вредоносных программ и вирусов на рабочих станциях и серверах автоматизированных систем, обрабатывающих персональные данные, осуществляется администраторами соответствующих систем в соответствии с руководствами по установке приобретенных средств защиты.

16. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено администратором системы на отсутствие вредоносных программ и компьютерных вирусов. После установки (изменения) программного обеспечения рабочей станции необходимо провести антивирусную проверку.

17. Запуск антивирусных программ осуществляется автоматически по заданию, созданному с использованием планировщика задач, входящего в поставку операционной системы либо поставляемого вместе с антивирусными программами.

18. Антивирусный контроль рабочих станций проводится ежедневно в автоматическом режиме. Если проверка всех файлов на дисках рабочих станций занимает неприемлемо большое время, то допускается проводить выборочную проверку загрузочных областей дисков, оперативной памяти, критически важных инсталлированных файлов операционной системы и загружаемых файлов по сети или с внешних носителей. В этом случае полная проверка осуществляется не реже одного раза в неделю в период неактивности пользователя. Пользователям рекомендуется проводить полную проверку во время перерыва на обед путем перевода рабочей станции в соответствующий автоматический режим функционирования в запечатом помещении.

Обязательному антивирусному контролю подлежит любая информация (исполняемые файлы, текстовые файлы любых форматов, файлы данных), получаемая пользователем по сети или загружаемая со съемных носителей (магнитных дисков, оптических дисков, флэш-накопителей и т. п.). Контроль информации проводится антивирусными средствами в процессе или сразу после ее загрузки на рабочую станцию пользователя. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

- анализ претензий, в случае если это изменение причинило кому-нибудь вред;

- разработка планов действий в аварийных ситуациях для восстановления работоспособности системы, если внесенное в нее изменение вывело ее из строя.
12. Для защиты от вредоносных программ и вирусов необходимо использовать только лицензионные или сертифицированные свободно распространяемые антивирусные средства.
13. Для защиты серверов и рабочих станций используются:
- резидентные антивирусные мониторы, контролирующие подозрительные действия программ;
 - утилиты для обнаружения и анализа новых вирусов.
14. При подозрении на наличие не выявленных установленными средствами защиты заражений следует использовать Live CD с другими антивирусными средствами.
15. Установка и настройка средств защиты от вредоносных программ и вирусов на рабочих станциях и серверах автоматизированных систем, обрабатывающих персональные данные, осуществляется администраторами соответствующих систем в соответствии с руководствами по установке приобретенных средств защиты.
16. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено администратором системы на отсутствие вредоносных программ и компьютерных вирусов. После установки (изменения) программного обеспечения рабочей станции необходимо провести антивирусную проверку.
17. Запуск антивирусных программ осуществляется автоматически по заданию, созданному с использованием планировщика задач, входящего в поставку операционной системы либо поставляемого вместе с антивирусными программами.
18. Антивирусный контроль рабочих станций проводится ежедневно в автоматическом режиме. Если проверка всех файлов на дисках рабочих станций занимает неприемлемо большое время, то допускается проводить выборочную проверку загрузочных областей дисков, оперативной памяти, критически важных инсталлированных файлов операционной системы и загружаемых файлов по сети или с внешних носителей. В этом случае полная проверка осуществляется не реже одного раза в неделю в период неактивности пользователя. Пользователям рекомендуется проводить полную проверку во время перерыва на обед путем перевода рабочей станции в соответствующий автоматический режим функционирования в запертом помещении.
19. Обязательному антивирусному контролю подлежит любая информация (исполняемые файлы, текстовые файлы любых форматов, файлы данных), получаемая пользователем по сети или загружаемая со съемных носителей (магнитных дисков, оптических дисков, флэш-накопителей и т. п.). Контроль информации проводится антивирусными средствами в процессе или сразу после ее загрузки на рабочую станцию пользователя. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.
20. Устанавливаемое на серверы программное обеспечение предварительно проверяется администратором системы на отсутствие компьютерных вирусов и вредоносных программ. Непосредственно после установки (изменения) программного обеспечения сервера должна быть выполнена антивирусная проверка.
21. На серверах систем, обрабатывающих персональные данные, необходимо применять специальное антивирусное программное обеспечение, позволяющее:
- осуществлять антивирусную проверку файлов в момент попытки записи файла на сервер;
 - проверять каталоги и файлы по расписанию с учетом нагрузки на сервер.
22. На серверах электронной почты следует применять антивирусное программное обеспечение, позволяющее осуществлять проверку всех входящих сообщений. В случае если проверка входящего сообщения на почтовом сервере показала наличие в нем вируса

или вредоносного кода, отправка данного сообщения блокируется. При этом должно осуществляться автоматическое оповещение администратора почтового сервера, отправителя сообщения и адресата.

23. Антивирусные базы на всех рабочих станциях и серверах необходимо регулярно обновлять.

24. Администратор системы должен проводить регулярные проверки протоколов работы антивирусных программ с целью выявления пользователей и каналов, через которых распространяются вирусы. При обнаружении зараженных вирусом файлов администратору необходимо выполнить следующие действия:

- отключить от компьютерной сети рабочие станции, представляющие вирусную опасность, до полного выяснения каналов проникновения вирусов и их уничтожения;
- немедленно сообщить о факте обнаружения вирусов непосредственному начальнику, в т. ч. указать предположительный источник (отправитель, владелец и т. д.) зараженного файла, тип зараженного файла, тип вируса, а также рассказать о характере содержащейся в файле информации и выполненных антивирусных мероприятиях.

25. Если администратор системы, обрабатывающей персональные данные, подозревает или получил сообщение о том, что его система подвергается атаке или уже была скомпрометирована, он должен определить системные ресурсы, безопасность которых была нарушена, а также установить:

- была ли попытка несанкционированного доступа (далее - НСД);
- когда, как и при каких обстоятельствах была предпринята попытка НСД;
- продолжается ли НСД в настоящий момент;
- кто является источником НСД;
- что является объектом НСД;
- какова была мотивация нарушителя;
- точку входа нарушителя в систему;
- была ли попытка НСД успешной.

26. Для выявления попытки НСД необходимо:

- установить, какие пользователи в настоящее время работают в системе и на каких рабочих станциях;
- выявить подозрительную активность пользователей, проверить, все ли пользователи вошли в систему со своих рабочих мест и не работает ли кто из них в системе необычно долго;
- убедиться, что никто из пользователей не использует подозрительные программы или программы, не относящиеся к его области деятельности.

27. При анализе системных журналов администратор должен:

- проверить наличие подозрительных записей в системных журналах, сделанных в период предполагаемой попытки НСД, включая вход в систему пользователей, которые должны были отсутствовать в этот период времени, а также входы в систему из неожиданных мест, в необычное время и на короткий период времени;
- убедиться в том, что системный журнал не уничтожен и в нем отсутствуют пробелы;
- просмотреть списки команд, выполненных пользователями в рассматриваемый период времени;

- проверить наличие исходящих сообщений электронной почты, адресованных подозрительным хостам;
- проверить журналы на наличие мест, которые выглядят необычно;
- выявить неудачные попытки входа в систему.

28. В ходе анализа журналов активного сетевого оборудования (мостов, переключателей, маршрутизаторов, шлюзов) следует проверить:

- нет ли в них подозрительных записей, сделанных в период предполагаемой попытки НСД;
- есть ли в них пробелы, а также места, которые выглядят необычно;
- были ли попытки изменения таблиц маршрутизации и адресных таблиц.

Кроме того, необходимо проверить конфигурацию сетевых устройств с целью определения возможности нахождения в системе программы, просматривающей весь сетевой трафик.

29. Для обнаружения в системе следов, оставленных злоумышленником в виде файлов, вирусов, троянских программ, изменения системной конфигурации следует:

- составить базовую схему того, как обычно выглядит система;
- провести поиск подозрительных файлов, скрытых файлов, имен файлов и каталогов, которые обычно используются злоумышленниками;
- проверить содержимое системных файлов, которые обычно изменяются злоумышленниками;
- оценить целостность системных программ;
- проверить систему аутентификации и авторизации.

30. Особенности мониторинга информационной безопасности персональных данных в отдельных автоматизированных системах могут регулироваться дополнительными инструкциями.

31. Работники подразделений ОУ и лица, выполняющие работы по договорам и контрактам, имеющие отношение к проведению мониторинга информационной безопасности и антивирусного контроля при обработке персональных данных, должны быть ознакомлены с Инструкцией под расписку.

Приложение 7

ИНСТРУКЦИЯ

по организации парольной защиты

I. Общие положения

1. Инструкция по организации парольной защиты (далее - Инструкция) призвана регламентировать организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационных системах образовательного учреждения (далее - ОУ), а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах информационной системы (далее - ИС) ОУ и контроль за действиями исполнителей и обслуживающего персонала при работе с паролями возлагается на системного администратора ОУ.

II. Правила формирования паролей

3. Личные пароли генерируются и распределяются централизованно либо выбираются пользователями информационной системы самостоятельно с учетом следующих требований:

- пароль должен состоять не менее чем из восьми символов;
- в пароле обязательно должны присутствовать буквы из верхнего и нижнего регистров, цифры и специальные символы (@, #, \$, &, *, % и т. п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т. д.), последовательности ности символов и знаков (111, qwerty, abed и т. д.), общепринятые сокращения (ЭВМ, ЛВС, USER и т. п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетания букв и знаков, которые можно угадать, основываясь на информации о пользователе;
- при смене пароля новый пароль должен отличаться от старого не менее чем в шести позициях.

4. В случае если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на уполномоченных сотрудников центра дистанционного образования.

5. При технологической необходимости использования имен и паролей некоторых работников (исполнителей) в их отсутствие (в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т. п.) такие работники обязаны сразу же после смены своих паролей их новые значения (вместе с именами своих учетных записей) в запечатанном конверте или опечатанном пенале передать на хранение ответственному за информационную безопасность подразделения (руководителю своего подразделения). Опечатанные конверты (пеналы) с паролями исполнителей должны храниться в сейфе. Для их опечатывания рекомендуется использовать печать отдела кадров.

III. Ввод пароля

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

IV. Порядок смены личных паролей

7. Смена паролей проводится регулярно, не реже одного раза в три месяца.

8. В случае прекращения полномочий пользователя (увольнение, переход на другую работу и т. п.) системный администратор должен немедленно удалить его учетную запись сразу после окончания последнего сеанса работы данного пользователя с системой.

9. Срочная (внеплановая) полная смена паролей производится в случае прекращения полномочий (увольнение, переход на другую работу и т. п.) администраторов информационной системы и других работников, которым по роду работы были предоставлены полномочия по управлению системой парольной защиты.

10. Смена пароля производится самостоятельно каждым пользователем в соответствии с п. 5 Инструкции и/или в соответствии с указанием в системном баннере-предупреждении (при наличии технической возможности).

11. Временный пароль, заданный системным администратором при регистрации нового пользователя, следует изменить при первом входе в систему.

V. Хранение пароля

12. Хранение пользователем своего пароля на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе либо в сейфе у системного администратора или руководителя подразделения в опечатанном пенале.

13. Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации.

14. Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем. Действия в случае утери и компрометации пароля

15. В случае утери или компрометации пароля пользователя должны быть немедленно предприняты меры в соответствии с п. 9 или 10 Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

VI. Ответственность при организации парольной защиты

16. 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 информации о пароле.

17. Ответственность за организацию парольной защиты в структурных подразделениях ОУ возлагается на системного администратора.

18. Работники ОУ и лица, имеющие отношение к обработке персональных данных в информационных системах ОУ, должны быть ознакомлены с Инструкцией под расписку.

**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП

Сертификат 603332450510203670830559428146817986133868575788

Владелец Светличная Татьяна Ивановна

Действителен с 17.10.2021 по 17.10.2022