Приложение № 10

К приказу Директора МБОУ СОШ

д.Султанбеково МР Аскинский район

РБ

от «21» 11 2018 г. № 88 ОД

Инструкция

по обеспечению безопасности персональных данных

СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1. Назначение документа

Документ определяет основные обязанности, права и ответственность пользователей информационных систем персональных данных в МБОУ СОШ д.Султанбеково МР Аскинский район РБ (далее Оператор).

2. Область применения

Настоящий документ обязаны знать и использовать в работе следующие должностные лица:

Таблица 1. Область применения

Наименование должности/роли
Ответственный за организацию обработки ПДн
Ответственный за обеспечение безопасности ПДн
Пользователи ИСПДн

3. Вводимые определения терминов

Таблица 2. Перечень сокращений

Сокращение	Расшифровка сокращения
ИБ	Информационная безопасность – комплекс организационно – технических мероприятий, обеспечивающий конфиденциальность, целостность и доступность информации
ИСПДн	Информационная система персональных данных
НСД	Несанкционированный доступ
ПДн	Персональные данные
ПЭВМ	Персональная электронная вычислительная машина
СВТ	Средства вычислительной техники
СЗПДн	Система защиты персональных данных

Таблица 3. Перечень терминов

Наименование термина	Определение термина
Информационная система персональных данных	Совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств

Наименование термина	Определение термина
Несанкционированный доступ	Доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своему функциональному предназначению и техническим характеристикам
Оператор	государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.
Персональные данные	Любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)

1. ОСНОВНЫЕ ПОЛОЖЕНИЯ

Настоящий документ определяет основные обязанности, права и ответственность субъектов ПДн при автоматизированной и неавтоматизированной обработке ПДн.

Ознакомление руководителей и работников структурных подразделений Оператора с требованиями настоящей рабочей инструкции проводит ответственный за обеспечение безопасности ПДн.

2. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ В ИСПДН

2.1 ФУНКЦИИ И ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЕЙ

Каждый работник, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки ПДн и имеющий доступ к ИСПДн, несет персональную ответственность за свои действия и обязан:

- Строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и аппаратными средствами ИСПДн;
- Выполнять свои функциональные обязанности строго в рамках прав доступа к внутренним и внешним информационным ресурсам, техническим средствам, полученным в установленном порядке;
- Знать и строго выполнять правила работы со средствами защиты информации, установленными в ИСПДн;
- Хранить в тайне свои реквизиты доступа (пароли);
- Соблюдать требования нормативных документов, регламентирующих правила обеспечения безопасности ПДн;
- Немедленно ставить в известность ответственного за организацию обработки ПДн и непосредственного руководителя подразделения в случае утери личных реквизитов доступа или при подозрении компрометации личных паролей, а также:
- при подозрении на совершение попыток НСД к ПЭВМ;
- при обнаружении несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ИСПДн.

- Немедленно ставить в известность ответственного за организацию обработки ПДн при обнаружении:

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

- некорректного функционирования установленных технических средств защиты информации;

- недокументированных свойств или ошибок в ИСПДн;

- Лично присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию закрепленной за ним ПЭВМ;

- При обработке на ПЭВМ защищаемой информации и необходимости использовать носители информации применять только учтенные носители;

Работникам категорически ЗАПРЕЩАЕТСЯ:

- Использовать компоненты программного и аппаратного обеспечения ИСПДн в неслужебных целях;

- Разглашать защищаемую информацию третьим лицам;

- Хранить и обрабатывать личную информацию на ПЭВМ и серверах ИСПДн;

- При работе в сети Интернет:

использовать информационные ресурсы сети Интернет, содержание которых нарушает действующее законодательство Российской Федерации;

использовать информационные ресурсы сети Интернет для целей, не связанных с областью производственной деятельности пользователя;

- Самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИСПДн или устанавливать дополнительно любые программные и аппаратные средства;

- Оставлять без присмотра включенную ПЭВМ, не активизировав средства защиты от НСД (блокировку учетной записи);

- Хранить в общедоступном месте персональные реквизиты доступа к ИСПДн;

- Оставлять без личного присмотра свои машинные носители информации и распечатки, содержащие сведения ограниченного распространения;

- Использовать в работе неучтенные носители информации для обработки защищаемой информации.

Умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты.

2 ОРГАНИЗАЦИЯ АНТИВИРУСНОЙ ЗАЩИТЫ

К использованию в Организации допускаются только лицензионные и сертифицированные ФСТЭК средства антивирусной защиты, централизованно закупленные у разработчиков или поставщиков данных средств.

Установка средств антивирусного контроля на компьютерах (серверах локальной вычислительной сети ИСПДн Организации) осуществляется ответственным за обеспечение безопасности обработки ПДн.

Ежедневно в начале работы при загрузке компьютера (для серверов локальной вычислительной сети - при перезапуске) в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов автоматизированных рабочих мест (далее - АРМ).

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. Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема. Контроль исходящей информации необходимо проводить непосредственно перед архивированием, отправкой (или записью на съемный носитель.

В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов работники обязаны:

приостановить работу;

немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за обработку ПДн, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;

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

провести лечение или уничтожение зараженных файлов.

3 ОРГАНИЗАЦИЯ ПАРОЛЬНОЙ ЗАЩИТЫ

Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями автоматизированной 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 легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ 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 3 позициях;

личный пароль пользователь не имеет права сообщать никому.

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.

Личная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в 6 (шесть) месяцев.

Внеплановая смена личного пароля или удаление учетной записи пользователя ИСПДн в случае прекращения его полномочий (увольнение, переход на другую работу и т.п.) должна производиться ответственным за обеспечение безопасности персональных данных немедленно после окончания последнего сеанса работы данного пользователя с системой.

Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и другие обстоятельства) ответственного за обеспечение безопасности персональных данных и других работников, которым по роду работы были предоставлены полномочия по управлению парольной защитой подсистем ИСПДн.

В случае компрометации личного пароля пользователя ИСПДн владелец скомпрометированного пароля должен сообщить о факте утери или компрометации пароля ответственному за обработку персональных данных и должны быть немедленно предприняты меры в соответствии с п.4 или п.5 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

Повседневный контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на ответственного за обработку персональных данных и руководителей подразделений.

ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

1 ФУНКЦИИ И ОБЯЗАННОСТИ РАБОТНИКОВ

Каждый работник, участвующий в рамках своих функциональных обязанностей в процессах неавтоматизированной обработки ПДн и имеющий доступ к ПДн, несет персональную ответственность за свои действия и обязан:

Строго соблюдать установленные правила обеспечения безопасности информации при работе с ПДн;

Помещать бумажные носители ПДн по завершении работы с ними на прежнее место либо возвращены лицу, выдавшему их для работы;

О факте утраты носителей информации, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов (металлических шкафов), личных печатей и о других фактах, которые могут привести к разглашению ПДн, немедленно сообщить ответственному за организацию обработки ПДн в Организации;

Хранить бумажные носители ПДн в местах установленных согласно документа «Приказ об утверждении мест хранения»;

Хранить бумажные носители персональных данных таким образом, чтобы исключить возможность просмотра персональных данных лицами, не допущенными к обработке персональных данных данной категории в соответствие с «Перечнем должностей, допущенных к работе с персональными данными», а также третьими лицами;

Вносить уточнения в ПДн, содержащихся на бумажных носителях ПДн, посредством затирания или вымарывания ПДн с применением пасты-штрих с последующей росписью субъекта ПДн (если внесение уточнений не позволяют технические особенности бумажного носителя ПДн, то этот носитель передается субъекту ПДн, а вместо него изготавливается новый бумажный носитель с уточненными ПДн).

ботникам категорически ЗАПРЕЩАЕТСЯ:

Бесконтрольно оставлять бумажные носители ПДн или передавать их на хранение другим лицам;

Оставлять одних в помещении лиц, не включенные в список лиц, имеющих право доступа к персональным данным;

Разглашать защищаемую информацию третьим лицам;

Самовольно вносить изменения в поля типовых форм документов.

4. ЗАЩИТА ПДН ОТ УТЕЧКИ ПО ВИДОВЫМ КАНАЛАМ

При возникновении угрозы просмотра ПДн посторонними лицами, необходимо прекратить обработку ПДн, а бумажные носители разместить таким образом, чтобы был исключен просмотр с них информации (перевернут текстом вниз, убрать в ящик стола или хранилище). Осуществлять работу с документами, содержащими персональные данные, только при условии отсутствия возможности просмотра данных документов через окна (закрытие штор, жалюзи, монитор повернут от окна).

5. ДЕЙСТВИЯ ПЕРСОНАЛА ВО ВНЕШТАТНЫХ СИТУАЦИЯХ ПРИ ОБРАБОТКЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ И ПЕРСОНАЛЬНЫХ ДАННЫХ

Под аварийной ситуацией понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн.

Все действия в процессе реагирования на аварийные ситуации должны документироваться в «Журнале учета нештатных ситуаций, фактов вскрытия и опечатывания ПЭВМ, выполнения профилактических работ, установки и модификации аппаратных и программных средств информационной системы персональных данных».

Под инцидентом понимается отказ или повреждение технических устройств, отклонение от технологического процесса, нарушение положений федеральных законов и иных нормативных правовых актов Российской Федерации, а также нормативных технических документов.

При обнаружении инцидента в кратчайшие сроки, не превышающие одного рабочего дня, ответственный за организацию безопасности персональных данных предпринимает меры по

работоспособности системы. Предпринимаемые меры по возможности вышестоящим руководством. По необходимости, иерархия может быть нарушена, с целью получения высококвалифицированной консультации в кратчайшие сроки. При необходимости привлекаются квалифицированные работники сторонних организаций с целью восстановления работоспособности в кратчайшие сроки.

ОТВЕТСТВЕННОСТЬ ЗА НЕИСПОЛНЕНИЕ (НЕНАДЛЕЖАЩЕЕ ИСПОЛНЕНИЕ) НАСТОЯЩЕЙ ИНСТРУКЦИИ

Все пользователи ИСПДн несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящей рабочей инструкцией и другими нормативными документами, регламентирующими требования обеспечения безопасности ПДн, в соответствии с действующим трудовым законодательством Российской Федерации.

НОРМАТИВНЫЕ ССЫЛКИ

Внешние нормативные и распорядительные документы

Таблица 5. Внешние нормативные и распорядительные документы

Наименование документа
Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных