Приложение 15
к приказу МАУДО «ДПШ»
от 31.08.2020 № 276/1-од

Инструкция
ответственного за обеспечение безопасности персональных данных в информационных системах

I. Общие положения

1. Данная Инструкция определяет основные обязанности и права ответственного за обеспечение безопасности персональных данных в информационных системах, в том числе персональных данных, Муниципального автономного учреждения дополнительного образования «Дворец пионеров и школьников им. Н.К. Крупской г. Челябинска» (далее - МАУДО «ДПШ»).

2. Ответственный за обеспечение безопасности персональных данных в информационных системах назначается приказом директора.

3. Решение вопросов обеспечения информационной безопасности входит в прямые служебные обязанности ответственного за обеспечение безопасности персональных данных в информационных системах.

4. Ответственный за обеспечение безопасности персональных данных в информационных системах обладает правами доступа к любым программным и аппаратным ресурсам информационной системы (далее - ИС) МАУДО «ДПШ».

5. Целью защиты информации является:

5.1. Предотвращение утечки, хищения, утраты, подделки информации, а также неправомерных действий по уничтожению, модификации, искажению, несанкционированному копированию, блокированию информации, предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы обеспечения правового режима документированной информации как объекта собственности.

5.2. Защита конституционных прав граждан на сохранение личной тайны и конфиденциальности информации, имеющейся в ИС МАУДО «ДПШ».

5.3. Сохранение конфиденциальности информации в соответствии с законодательством Российской Федерации.

5.4. Обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

6. Основными видами угроз безопасности защищаемой информации являются:

- противоправные действия третьих лиц;
- ошибочные действия пользователей ИС;
- отказы и сбои технических средств ИС, приводящие к её модификации, блокированию, уничтожению или несанкционированному копированию, а также нарушению правил эксплуатации ЭВМ и сетевого оборудования.

II. Термины и определения

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

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

База данных – это информация, упорядоченная в виде набора элементов, записей одинаковой структуры.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и / или воздействия на защищаемую информацию или ресурсы информационной системы.

Дистрибутив программного обеспечения – это файл или файлы, предназначенные для установки программного обеспечения.

Доступ к информации – возможность получения информации и её использования (ст.2 Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и защите информации»).

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

Конфиденциальная информация – документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации (ФСТЭК. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К) Москва 2001).

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 путём изменения (повышения, фальсификации) своих прав доступа.

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

Обработка информации – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с информацией, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение информации.

Пользователь – работник, участвующий в рамках своих функциональных обязанностей в процессах обработки информации.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (ст.3 Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»).

Резервное копирование – процесс создания копии данных на носителе (дисковом массиве, магнитной ленте и т. д.), предназначенном для восстановления данных в оригинальном месте их расположения в случае их повреждения или разрушения.

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

Угрозы безопасности защищаемой информации (УБЗИ) – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к защищаемой информации, результатом которого может стать уничтожение, изменение, блокирование, копирование, предоставление, распространение информации, а также иные неправомерные действия при их обработке в информационной системе.

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

Утечка защищаемой информации – неконтролируемое распространение информации от ее носителя.

III. Общие обязанности

8. Ответственный за обеспечение безопасности персональных данных в информационных системах обязан:

1) знать перечень сведений, составляющих защищаемую информацию и условия ее обработки в МАУДО «ДПШ»;

2) знать перечень установленных в отделах МАУДО «ДПШ» технических средств, в том числе съёмных носителей, конфигурацию ИС и перечень задач, решаемых с её использованием;

3) определять полномочия пользователей ИС (оформление разрешительной системы доступа), минимально необходимых им для выполнения служебных (трудовых) обязанностей;

4) осуществлять учёт съемных носителей информации, их уничтожение, либо контроль процедуры их уничтожения, вести «Журнал учета съемных носителей информации»;

5) осуществлять оперативный контроль за работой пользователей защищённых АРМ и адекватно реагировать на возникающие нештатные ситуации, фиксировать их в «Журнале учета работ в информационных системах»;

6) периодически проверять актуальность сертификатов соответствия используемых средств защиты информации в информационных системах;

7) блокировать доступ к защищаемой информации при обнаружении нарушений порядка их обработки;

8) реагировать на попытки несанкционированного доступа к информации в установленном гл. VIII настоящей Инструкции порядке;

9) устанавливать и осуществлять настройку средств защиты информации в рамках компетенции;

10) по мере необходимости вносить изменения в конфигурацию технических средств ИС, отражать соответствующие изменения в перечне АРМ информационной системы;

11) осуществлять непосредственное управление и контроль режимов работы функционирования применяемых в ИС средств защиты информации, осуществлять проверку правильности их настройки (выборочное тестирование);

12) периодически контролировать целостность печатей (пломб, наклеек) технических средств, используемых для обработки защищаемой информации;

13) проводить работу по выявлению возможных каналов утечки информации, изучать текущие тенденции в области защиты персональных данных;

14) проводить разбирательства и составление заключений по фактам несоблюдения условий хранения носителей информации, нарушения правил работы с техническими и программными средствами ИС, в том числе со средствами защиты информации, или по другим нарушениям, которые могут привести к снижению степени защищённости;

15) предоставлять доступ к ИС новым пользователям, предоставлять им возможность задать личный пароль, соответствующий требованиям Инструкции по организации парольной защиты;

16) производить мероприятия по внеплановой смене личных паролей;

17) вносить плановые и внеплановые изменения в учётную запись пользователей ИС, в том числе по требованию руководителя структурного подразделения и в случае увольнения работника;

18) осуществлять периодическое резервное копирование баз данных и сопутствующей защищаемой информации, а также осуществлять внеплановое создание резервных копий по требованию пользователей ИС и в иных случаях, когда это необходимо для обеспечения сохранности персональных данных;

19) осуществлять восстановление информации из резервных копий по требованию пользователей ИС и в иных случаях, когда это необходимо для восстановления утраченных сведений;

20) хранить дистрибутивы программного обеспечения, установленного в ИС, в том числе дистрибутивы средств защиты информации, в месте, исключающем несанкционированный доступ к ним третьих лиц;

21) вносить свои предложения по совершенствованию мер защиты информации в ИС, разработке и принятии мер по предотвращению возможных опасных последствий нарушений, приводящих к снижению степени защищённости;

22) заниматься обслуживанием установленных средств криптографической защиты информации (в том числе персональных данных);

23) знать законодательство РФ о защите информации, следить за его изменениями;

24) выполнять иные мероприятия, требуемые техническими и программными средствами ИС для поддержания их функционирования;

25) при использовании в информационных системах технологий беспроводного доступа, разграничивать доступ к беспроводной сети, контролировать предоставление доступа к беспроводной сети только тем пользователям, которым он необходим для выполнения установленных должностных обязанностей (при наличии сертифицированных средств защиты информации);

26) контролировать запрет обработки защищаемой информации с использованием технологии беспроводного доступа к сети (при отсутствии сертифицированных средств защиты информации).

IV. Порядок работы со съёмными носителями

9. Под съемными носителями (далее – носители) в настоящей Инструкции понимаются следующие носители информации:

- USB-флеш-накопитель;
- оптические диски (CD, DVD) однократной и многократной записи;
- электронные накопители информации (в т.ч. съемные жесткие диски).

10. Носители, содержащие защищаемую информацию, подлежат обязательному учету ответственным за обеспечение безопасности персональных данных в информационных системах в Журнале учета съемных носителей информации.

11. Носители, содержащие защищаемую информацию, должны иметь специальную маркировку. Тип маркировки выбирается ответственным за обеспечение безопасности персональных данных в информационных системах.

12. При поступлении нового носителя, который будет использоваться для хранения или передачи защищаемой информации, ответственный за обеспечение безопасности персональных данных в информационных системах регистрирует его в Журнале учета съемных носителей информации.

13. Учет выдачи носителей ведётся в Журнале учета съемных носителей информации, в котором указывается маркировка носителя, дата, время, фамилия, имя и отчество должностного лица, получившего материальный носитель, его подпись.

14. В случае возврата должностным лицом носителя в Журнале учета съемных носителей информации ответственным за обеспечение безопасности персональных данных в информационных системах проставляется отметка о возврате с указанием даты, времени возврата, личных подписей передающей и принимающей стороны.

V. Разграничение доступа пользователей к информационным ресурсам и средствам защиты информации

15. Защита от несанкционированного доступа осуществляется:

1) идентификацией и проверкой подлинности пользователей ИС при доступе к информационным ресурсам МАУДО «ДПШ»;

2) разграничением доступа к обрабатываемым базам данных. Пользователь ИС имеет доступ только к тем информационным ресурсам, которые разрешены для него. Для осуществления доступа к информационным ресурсам, ответственный за обеспечение безопасности персональных данных в информационных системах назначает конкретному пользователю ИС идентифицирующее имя пользователя и персональный пароль доступа.

16. Ответственный за обеспечение безопасности персональных данных в информационных системах должен осуществлять мероприятия по обеспечению защиты информационных ресурсов МАУДО «ДПШ» от несанкционированного доступа и непреднамеренных изменений и разрушений, а также иметь в наличии средства восстановления, резервные копии, предусматривающие процедуру восстановления свойств информационных ресурсов после сбоев и отказов оборудования.

VI. Действия при обнаружении попыток несанкционированного доступа

17. К попыткам несанкционированного доступа относятся:

- сеансы работы с ИС незарегистрированных пользователей, или пользователей, нарушивших установленную периодичность доступа, или срок действия полномочий которых истёк, или превышающих свои полномочия по доступу к данным;

- действия третьего лица, пытающегося получить доступ (или уже получившего доступ) к ИС, при использовании учётной записи администратора или другого пользователя ИС, методом подбора пароля, использования пароля, разглашённого владельцем учётной записи или любым другим методом.

18. При выявлении факта несанкционированного доступа ответственный за обеспечение безопасности персональных данных в информационных системах обязан:

1) прекратить несанкционированный доступ к ИС;

2) доложить директору МАУДО «ДПШ» служебной запиской о факте несанкционированного доступа, его результате (успешный, неуспешный) и предпринятых действиях;

3) известить руководителя структурного подразделения, в котором работает пользователь, от имени учетной записи которого была осуществлена попытка несанкционированного доступа, о факте несанкционированного доступа.

VII. Права

19. Ответственный за обеспечение безопасности персональных данных в информационных системах, имеет право:

1) требовать от пользователей ИС выполнения инструкций в части работы с программными, аппаратными средствами ИС и защищаемой информацией;

2) блокировать доступ к защищаемой информации любых пользователей, если это необходимо для предотвращения нарушения режима защиты информации;

3) проводить внеплановые антивирусные проверки при возникновении угрозы появления вредоносных программ;

4) производить периодические попытки взлома паролей пользователей в целях тестирования системы контроля доступа на наличие уязвимостей. В случае успешной попытки – вправе требовать у пользователя изменения пароля;

5) проводить служебные расследования и опрашивать пользователей по фактам несоблюдения условий хранения носителей информации, нарушения правил работы с техническими и программными средствами ИС, в том числе со средствами защиты информации, или по другим нарушениям, которые могут привести к снижению степени защищённости.

VIII. Ответственность

20. Ответственный за обеспечение безопасности персональных данных в информационных системах несёт персональную ответственность за соблюдение требований настоящей Инструкции, за средства защиты информации, применяемые в ИС МАУДО «ДПШ», за качество проводимых им работ по обеспечению безопасности защищаемой информации и за все действия, совершенные от имени его учётной записи в ИС, если с его стороны не было предпринято необходимых

действий для предотвращения несанкционированного использования его учётной записи.

21. Ответственный за обеспечение безопасности персональных данных в информационных системах при нарушении норм, регулирующих получение, обработку и защиту информации, несёт дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

22. Разглашение защищаемой информации (передача ее посторонним лицам, в том числе другим работникам, не имеющим к ней допуск), ее публичное раскрытие, утрата документов и иных носителей, содержащих защищаемую информацию субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных локальными нормативно-правовыми актами (приказами, распоряжениями) МАУДО «ДПШ», влечет наложение на работника, имеющего доступ к защищаемой информации, дисциплинарных взысканий в виде: замечания, выговора, увольнения. Работник МАУДО «ДПШ», имеющий доступ к защищаемой информации субъекта и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба МАУДО «ДПШ» (в соответствии с п.7 ст.243 Трудового кодекса РФ).

В отдельных случаях, при разглашении защищаемой информации, работник, совершивший указанный проступок, несет ответственность в соответствии со ст.13.11, 13.14 Кодекса об административных правонарушениях РФ.

23. В случае незаконного сбора или публичного распространения информации о частной жизни лица (нарушения неприкосновенности частной жизни), предусмотрена ответственность в соответствии со ст.137 Уголовного кодекса РФ.