ПРИЛОЖЕНИЕ 4
к распоряжению администрации
Белоярского района
от 16 августа 2016 года № 262-р

ИНСТРУКЦИЯ

администратора безопасности информационных систем персональных данных

I. Общие положения

1.1. Данная Инструкция определяет основные обязанности и права администратора безопасности информационных систем персональных данных администрации Белоярского района.

1.2. Администратор безопасности информационных систем персональных данных (далее – ИСПДн) назначается распоряжением главы Белоярского района.

1.3. Решение вопросов обеспечения информационной безопасности входит в прямые служебные обязанности администратора безопасности ИСПДн.

1.4. Администратор безопасности ИСПДн обладает правами доступа к любым программным и аппаратным ресурсам ИСПДн администрации Белоярского района.

1.5. Целью защиты информации является:

1.5.1. 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.

1.5.2. Защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в ИСПДн администрации Белоярского района.

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

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

1.6. Основными видами угроз безопасности персональных данных являются:

1.6.1. Противоправные действия третьих лиц.

1.6.2. Ошибочные действия пользователей ИСПДн.

1.6.3. Отказы и сбои технических средств ИСПДн, приводящие к её модификации, блокированию, уничтожению или несанкционированному копированию, а также нарушению правил эксплуатации ЭВМ и сетевого оборудования.

II. Термины и определения

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

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

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

2.4. **Вредоносная программа –** программа, предназначенная для осуществления несанкционированного доступа и / или воздействия на персональные данные или ресурсы информационной системы персональных данных

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

2.6. **Доступ к информации** – возможность получения информации и её использования (ст. 2 ФЗ РФ от 27.07.2006 г. N 149-ФЗ «Об информации, информационных технологиях и защите информации»).

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

2.8. **Информационная система персональных данных (ИСПДн)** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

2.9. **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).

2.10. **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.

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

2.12. **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 (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

2.13. **Пользователь** – сотрудник, участвующий в рамках своих функциональных обязанностей в процессах обработки персональных данных.

2.14. **Персональные данные** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

2.15. **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.

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

2.17. **Угрозы безопасности персональных данных (УБПДн)** – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в информационной системе персональных данных (ст. 19 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»)

2.18. **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 (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

2.19. **Утечка персональных данных** – неконтролируемое распространение персональных данных от носителя персональных данных.

III. Общие обязанности

Администратор безопасности ИСПДн обязан:

3.1. Знать перечень сведений, составляющих персональные данные и условия обработки персональных данных в администрации Белоярского района.

3.2. Знать перечень установленных в органах администрации Белоярского района технических средств, в том числе съёмных носителей, конфигурацию ИСПДн и перечень задач, решаемых с её использованием.

3.3. Определять полномочия пользователей ИСПДн (оформление разрешительной системы доступа), минимально необходимых им для выполнения служебных (трудовых) обязанностей.

3.4. Осуществлять учёт съемных носителей информации, их уничтожение, либо контроль процедуры их уничтожения, вести «Журнал учета съемных носителей информации».

3.5. Осуществлять учёт и периодический контроль над составом и полномочиями пользователей автоматизированных рабочих мест (далее АРМ).

3.6. Осуществлять оперативный контроль за работой пользователей защищённых АРМ и адекватно реагировать на возникающие нештатные ситуации, фиксировать их в «Журнале учета работ в информационных системах персональных данных».

3.7. Блокировать доступ к персональным данным при обнаружении нарушений порядка их обработки.

3.8. Реагировать на попытки несанкционированного доступа к информации в установленном гл.VIII настоящей Инструкции порядке.

3.9. Устанавливать и осуществлять настройку средств защиты информации в рамках компетенции.

3.10. По мере необходимости вносить изменения в конфигурацию технических средств ИСПДн, отражать соответствующие изменения в Техническом паспорте информационной системы.

3.11. Осуществлять непосредственное управление и контроль режимов работы функционирования применяемых в ИСПДн средств защиты информации, осуществлять проверку правильности их настройки (выборочное тестирование).

3.12. Периодически контролировать целостность печатей (пломб, наклеек) технических средств, используемых для обработки персональных данных.

3.13. Проводить работу по выявлению возможных каналов утечки персональных данных, изучать текущие тенденции в области защиты персональных данных.

3.14. Проводить разбирательства и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, нарушения правил работы с техническими и программными средствами ИСПДн, в том числе со средствами защиты информации, или по другим нарушениям, которые могут привести к снижению уровня защищённости персональных данных.

3.15. Предоставлять доступ к ИСПДн новым пользователям, предоставлять им возможность задать личный пароль, соответствующий требованиям Инструкции по организации парольной защиты.

3.16. Производить мероприятия по внеплановой смене личных паролей.

3.17. Вносить плановые и внеплановые изменения в учётную запись пользователей ИСПДн, в том числе по требованию руководителя органа администрации Белоярского района и в случае увольнения сотрудника.

3.18. Осуществлять периодическое резервное копирование баз персональных данных и сопутствующей защищаемой информации, а также осуществлять внеплановое создание резервных копий по требованию пользователей ИСПДн и в иных случаях, когда это необходимо для обеспечения сохранности персональных данных.

3.19. Осуществлять восстановление информации из резервных копий по требованию пользователей ИСПДн и в иных случаях, когда это необходимо для восстановления утраченных сведений.

3.20. Хранить дистрибутивы программного обеспечения, установленного в ИСПДн, в том числе дистрибутивы средств защиты информации, в месте, исключающем несанкционированный доступ к ним третьих лиц.

3.21. Вносить свои предложения по совершенствованию мер защиты персональных данных в ИСПДн, разработке и принятии мер по предотвращению возможных опасных последствий нарушений, приводящих к снижению уровня защищённости персональных данных.

3.22. Заниматься обслуживанием установленных средств криптографической защиты информации (в том числе персональных данных).

3.23. Знать законодательство РФ о защите персональных данных, следить за его изменениями.

3.24. Выполнять иные мероприятия, требуемые техническими и программными средствами ИСПДн для поддержания их функционирования.

IV. Порядок работы со съёмными носителями персональных данных

4.1. Под съемными носителями (далее – носители) в настоящей инструкции понимаются следующие носители информации:

1) дискеты;
2) оптические диски (CD, DVD) однократной и многократной записи;
3) электронные накопители информации (флэш-память, съемные жесткие диски).

4.2. Носители, содержащие персональные данные, подлежат обязательному учету администратором безопасности ИСПДн в Журнале учета съемных носителей информации.

4.3. Носители, содержащие персональные данные, должны иметь специальную маркировку. Тип маркировки выбирается администратором безопасности ИСПДн.

4.4. При поступлении нового носителя, который будет использоваться для хранения или передачи персональных данных, администратор безопасности ИСПДн регистрирует его в Журнале учета съемных носителей информации.

4.5. 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.

4.6. В случае возврата должностным лицом носителя в Журнале учета съемных носителей информации администратором безопасности ИСПДн 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

5.1. Защита от несанкционированного доступа осуществляется:

5.1.1. Идентификацией и проверкой подлинности пользователей ИСПДн при доступе к информационным ресурсам администрации Белоярского района.

5.1.2. Разграничением доступа к обрабатываемым базам данных. Пользователь ИСПДн имеет доступ только к тем информационным ресурсам, которые разрешены для него. Для осуществления доступа к информационным ресурсам, администратор безопасности

ИСПДн назначает конкретному пользователю ИСПДн идентифицирующее имя пользователя и персональный пароль доступа.

5.2. Администратор безопасности ИСПДн должен осуществлять мероприятия по обеспечению защиты информационных ресурсов администрации Белоярского района 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

6.1. К попыткам несанкционированного доступа относятся:

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

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

6.2. При выявлении факта несанкционированного доступа администратор безопасности ИСПДн обязан:

1) прекратить несанкционированный доступ к ИСПДн;

2) доложить главе Белоярского района служебной запиской о факте несанкционированного доступа, его результате (успешный, неуспешный) и предпринятых действиях;

3) известить руководителя органа администрации Белоярского района, в котором работает пользователь, от имени учетной записи которого была осуществлена попытка несанкционированного доступа, о факте несанкционированного доступа.

VII. Права

Администратор безопасности ИСПДн имеет право:

7.1. Требовать от пользователей ИСПДн выполнения инструкций в части работы с программными, аппаратными средствами ИСПДн и персональными данными.

7.2. Блокировать доступ к персональным данным любых пользователей, если это необходимо для предотвращения нарушения режима защиты персональных данных.

7.3. Проводить внеплановые антивирусные проверки при возникновении угрозы появления вредоносных программ.

7.4. 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.

7.5. Проводить служебные расследования и опрашивать пользователей по фактам несоблюдения условий хранения носителей персональных данных, нарушения правил работы с техническими и программными средствами ИСПДн, в том числе со средствами защиты информации, или по другим нарушениям, которые могут привести к снижению уровня защищённости персональных данных.

VIII. Ответственность

8.1. Администратор ИСПДн несёт персональную ответственность за соблюдение требований настоящей Инструкции, за средства защиты информации, применяемые в ИСПДн администрации Белоярского района, за качество проводимых им работ по обеспечению безопасности персональных данных и за все действия, совершенные от имени

его учётной записи в ИСПДн, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учётной записи.

8.2. Администратор ИСПДн при нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несёт дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

8.3. Разглашение персональных данных субъекта (передача их посторонним лицам, в том числе другим сотрудникам, не имеющим к ним допуск), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных локальными нормативно-правовыми актами (приказами, распоряжениями) Администрации Белоярского района, влечет наложение на сотрудника, имеющего доступ к персональным данным, дисциплинарных взысканий в виде: замечания, выговора, увольнения. Сотрудник Администрации Белоярского района, имеющий доступ к персональным данным субъекта и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба Администрации Белоярского района (в соответствии с п.7 ст. 243 Трудового кодекса РФ).

8.3.1. В отдельных случаях, при разглашении персональных данных, сотрудник, совершивший указанный проступок, несет ответственность в соответствии со статьей 13.14 Кодекса об административных правонарушениях РФ.

8.4. 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.

_____