Приложение № 9

Утверждено

постановлением Администрации

Ельцовского района

от 07.10.2024 № 220

ИНСТРУКЦИЯ

ответственного за обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных Администрации Ельцовского района Алтайского края

I. Общие положения

1.1. Данная Инструкция определяет основные обязанности и права ответственного за обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных Администрации Ельцовского района Алтайского края (далее – Администрация).

2.1. Для организации деятельности по защите персональных данных при их обработке в информационных системах Администрации назначается должностное лицо, ответственное за обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных (далее – Ответственный).

3.1. Ответственный назначается распоряжением Администрации или лицом, назначенным в установленном порядке непосредственным руководителем должностного лица.

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

5.1. Ответственный обладает правами доступа к любым программным и аппаратным ресурсам информационной системы (далее - ИС) Администрации.

6.1. Целью защиты информации является:

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.
2. Защита конституционных прав граждан на сохранение личной тайны и конфиденциальности информации, имеющейся в ИС Администрации.
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.

7.1. Основными видами угроз безопасности защищаемой информации являются:

1. Противоправные действия третьих лиц.
2. Ошибочные действия пользователей ИС.
3. Отказы и сбои технических средств ИС, приводящие к её модификации, блокированию, уничтожению или несанкционированному копированию, а также нарушению правил эксплуатации ЭВМ и сетевого оборудования.
4. Выполнение норм обеспечения безопасности, установленных Приказом ФСТЭК России от 18.02.2013 № 21 (ред. от 14.05.2020) «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», определено в Положении по защите персональных данных в информационных системах.

II. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

1. Автоматизированное рабочее место (АРМ) - персональный компьютер и подключенные к нему периферийные устройства - принтер, многофункциональные устройства, сканеры и т.д.
2. Антивирусная защита **-** комплекс мер, направленных на предотвращение, обнаружение и обезвреживание действий вредоносного ПО при помощи антивирусных программных продуктов.
3. База данных **-** это информация, упорядоченная в виде набора элементов, записей одинаковой структуры.
4. Вредоносная программа **-** программа, предназначенная для осуществления несанкционированного доступа и/или воздействия на защищаемую информацию или ресурсы информационной системы.
5. Дистрибутив программного обеспечения - это файл или файлы, предназначенные для установки программного обеспечения.
6. Доступ к информации - возможность получения информации и её использования.
7. Защита информации **-** деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на информацию, то есть процесс, направленный на достижение информационной безопасности.
8. Информационная система **-** совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.
9. Информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.
10. Инцидент неправомерной или случайной передачи персональных данных **-** установленный факт неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных, обязывающий оператора с момента выявления такого инцидента уведомить Роскомнадзор о произошедшем инциденте в установленной форме.
11. Компьютерный инцидент (событие информационной безопасности) -

непредвиденное или нежелательное событие (группа событий) безопасности, которое привело (могут привести) к нарушению функционирования информационной системы или возникновению угроз безопасности информации (нарушению конфиденциальности, целостности, доступности), в том числе персональных данных.

1. Контролируемая зона **-** это пространство (территория, здание, часть здания, помещения), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств.
2. Конфиденциальная информация **-** документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ.
3. Несанкционированный доступ (НСД) **-** доступ к информации, хранящейся на различных типах носителей (бумажных, машинных) в компьютерных базах данных, файловых хранилищах, архивах, секретных частях и т. д. различных организаций путём изменения (повышения, фальсификации) своих прав доступа.
4. Носитель информации **-** любой материальный объект или среда, используемый для хранения или передачи информации.
5. 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.
6. Пользователь **-** работник, участвующий в рамках своих функциональных обязанностей в процессах обработки информации.
7. Персональные данные **-** любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).
8. Персональные данные, разрешенные субъектом персональных данных для распространения - персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном Федеральным законом 152-ФЗ «О персональных данных».
9. Распространение персональных данных **-** действия, направленные на раскрытие персональных данных неопределенному кругу лиц.
10. 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.
11. Средство защиты информации (СЗИ) **-** техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.
12. Субъект персональных данных **-** физическое лицо, которое прямо или косвенно определено или определяемо с помощью персональных данных.
13. Угрозы безопасности информации **-** совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного доступа к защищаемой информации (персональных данных), результатом которого может стать уничтожение, изменение, блокирование, копирование, предоставление, распространение информации, а также иные неправомерные действия при их обработке в информационной системе.
14. Уничтожение информации **-** действия, в результате которых становится невозможным восстановить содержание защищаемой информации в информационной системе и (или) в результате которых уничтожаются материальные носители информации.
15. Утечка защищаемой информации **-** неконтролируемое распространение информации от ее носителя.
16. Уязвимость- недостаток (слабость) информационной системы, который (которая) создает потенциальные или реально существующие условия для реализации или проявления угроз безопасности информации.

III. ОБЩИЕ ОБЯЗАННОСТИ

Ответственный обязан:

1. Осуществлять деятельность в области защиты персональных данных, направленную на обеспечение безопасности персональных данных в информационных системах Администрации.
2. Знать перечень сведений, составляющих защищаемую информацию и условия ее обработки в Администрации.
3. Знать перечень установленных в отделах Администрации технических средств, в том числе съёмных машинных носителей, конфигурацию ИС и перечень задач, решаемых с её использованием.
4. Определять полномочия пользователей ИС (оформление разрешительной системы доступа), минимально необходимые им для выполнения служебных (трудовых) обязанностей.
5. Осуществлять учёт машинных носителей персональных данных, их уничтожение, либо контроль процедуры их уничтожения, вести «Журнал учета съемных машинных носителей персональных данных».
6. Осуществлять оперативный контроль за работой пользователей АРМ ИСПДн и адекватно реагировать на возникающие нештатные ситуации.
7. Периодически проверять актуальность сертификатов соответствия используемых средств защиты информации в информационных системах.
8. Блокировать доступ к защищаемой информации при обнаружении нарушений порядка их обработки.
9. Реагировать на попытки несанкционированного доступа к информации, компьютерные инциденты в порядке, установленном главой VI настоящей Инструкции и Порядоком реагирования на инциденты информационной безопасности.
10. Устанавливать и осуществлять настройку средств защиты информации в рамках компетенции.
11. По мере необходимости вносить изменения в конфигурацию технических средств ИС, отражать соответствующие изменения в перечне автоматизированных рабочих мест информационной системы, проводить анализ потенциального воздействия планируемых изменений в конфигурации информационной системы на обеспечение защиты персональных данных.
12. Осуществлять непосредственное управление и контроль режимов работы функционирования применяемых в ИС средств защиты информации, осуществлять проверку правильности их настройки (выборочное тестирование).
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 съемных носителей персональных данных, 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 антивирусной защиты в информационных системах персональных данных.
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 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, исключающим несанкционированный доступ к ним третьих лиц.
21. Вносить свои предложения по совершенствованию мер защиты информации в ИС, разработке и принятию 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).
27. При необходимости реализации удаленного доступа к информационной системе устанавливать виды доступа пользователей и ограничения на использование удаленного доступа в соответствии с задачами (функциями) информационной системы, предоставлять удаленный доступ только тем пользователям, которым он необходим для выполнения установленных должностных обязанностей, проводить контроль и мониторинг удаленного доступа на предмет несанкционированного доступа к информационной системе.
28. Обеспечивать регламентацию и контроль использования мобильных технических средств, в том числе устанавливать параметры доступа к мобильным средствам, проводить проверки на предмет выявления несанкционированного использования мобильных технических средств для доступа к информационной системе.

IV. Порядок работы с машинными носителями

1. Под машинными носителями (далее - носители) в настоящей инструкции понимаются съемные машинные носители и несъемные машинные носители.
2. Под несъемными машинными носителями в настоящей инструкции понимаются накопители на жестких дисках, встроенные в корпус средств вычислительной техники (серверов, автоматизированных рабочих мест, сетевых хранилищ и т.п.).
3. Под съемными машинными носителями (далее - съемные носители) в настоящей инструкции понимаются следующие носители информации:

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

1. Носители, содержащие персональные данные, подлежат обязательному учету Ответственным в Журнале учета съемных машинных носителей персональных данных.
2. Учет выдачи съемных носителей ведётся в Журнале учета съемных машинных носителей персональных данных, в котором указывается маркировка носителя, дата, время, фамилия, имя и отчество должностного лица, получившего материальный носитель, его подпись.
3. Учет встроенных в портативные или стационарные технические средства машинных носителей информации может вестись в журналах материально-технического учета в составе соответствующих технических средств. При использовании в составе одного технического средства информационной системы нескольких встроенных машинных носителей информации, конструктивно объединенных в единый ресурс для хранения информации, допускается присвоение регистрационного номера техническому средству в целом.
4. При поступлении нового носителя, который будет использоваться для хранения или передачи персональных данных, Ответственный регистрирует его в Журнале учета съемных носителей персональных данных.
5. В случае возврата должностным лицом съемного носителя в Журнале учета съемных машинных носителей персональных данных Ответственным проставляется отметка о возврате с указанием даты, времени возврата, личных подписей передающей и принимающей стороны.
6. Ответственным должно обеспечиваться уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания.

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

1. Защита от несанкционированного доступа осуществляется:
2. Идентификацией и проверкой подлинности пользователей ИС при доступе к информационным ресурсам Администрация.
3. Ограничением неуспешных попыток входа в информационную систему.
4. Блокированием сеанса доступа в информационную систему после установленного ответственным за обеспечение безопасности времени бездействия.
5. 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 назначает конкретному пользователю ИС идентифицирующее имя пользователя и персональный пароль доступа.
6. Ответственный должен осуществлять мероприятия по обеспечению защиты информационных ресурсов Администрации от несанкционированного доступа, 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. Регистрация событий безопасности

6.1. Ответственный определяет события безопасности (включая компьютерные инциденты), подлежащие регистрации с учетом способов реализации угроз безопасности для информационных систем персональных данных и срок их хранения.

1. К событиям безопасности должны быть отнесены любые проявления состояния информационных систем, указывающие на возможность нарушения конфиденциальности, целостности или доступности персональных данных, доступности компонентов информационной системы, нарушения процедур, установленных организационно-распорядительными документами по защите персональных данных, а также на нарушение штатного функционирования средств защиты информации.
2. К регистрируемым событиям информационной безопасности относятся события безопасности, а также организационно-технические события информационной безопасности в инфраструктуре ИС.
3. Состав и содержание информации о событиях безопасности, должны, как минимум, обеспечить возможность идентификации типа события безопасности, даты и времени события безопасности, идентификационной информации источника события безопасности, результат события безопасности (успешно или неуспешно), субъект доступа (пользователь и (или) процесс), связанный с данным событием безопасности.
4. Ответственный реагирует на инциденты (компьютерные инциденты) в соответствии, с Порядоком реагирования на инциденты информационной безопасности.

VII. Обновление программного обеспечения

1. В случае выпуска обновления для используемого в информационных системах программного обеспечения Ответственный обязан оценить необходимость обновления этого программного обеспечения.
2. Обновление программного обеспечения необходимо:
3. если в программном обеспечении была обнаружена уязвимость и обновление позволяет ее нейтрализовать;
4. если продолжение работоспособности программного обеспечения невозможно без обновления.
5. Обновление средств защиты информации должно осуществляться только в случае появления информационного сообщения на сайте производителя средства защиты информации о необходимости обновления или в случае истечения срока действия сертификата соответствия на данное средство защиты информации. Обновление средств защиты информации должно осуществляться только на сертифицированные версии.
6. В случае принятия решения о необходимости обновления программного обеспечения, в т.ч. средств защиты информации, Ответственный должен получить обновления доверенным способом (приобрести обновленный дистрибутив у разработчика или дилера, скачать обновления с сайта разработчика и т.д.).
7. После получения дистрибутива программного обеспечения, Ответственный должен проверить целостность полученных обновлений. Для этого осуществляется контрольное суммирование исполняемых файлов обновлений и сверка контрольных сумм с эталонными, представленными на официальном сайте разработчика, в формуляре и т.д.
8. В случае совпадения контрольных сумм, Ответственный должен осуществить копирование образа операционной системы автоматизированного рабочего места, на котором требуется обновить программное обеспечение, вместе со всем установленным на данном автоматизированном рабочем месте программным обеспечением, либо создать точку восстановления средствами операционной системы.
9. Обновление программного обеспечения должно осуществляться в соответствии с эксплуатационной документацией на данное программное обеспечение.
10. После обновления программного обеспечения Ответственный проверяет работоспособность автоматизированного рабочего места. В случае возникновения проблем с работоспособностью, Ответственный восстанавливает операционную систему из точки восстановления или из образа системы.

VIII. Права

Ответственный 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. Требовать от пользователей ИС выполнения Инструкции по организации антивирусной защиты в информационных системах персональных данных.
  4. Проводить внеплановые антивирусные проверки при возникновении угрозы появления вредоносных программ.
  5. 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.
  6. 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.

IX. Ответственность

1. Ответственный несёт персональную ответственность за соблюдение требований настоящей Инструкции, за средства защиты информации, применяемые в ИС Администрации, 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.
2. Ответственный при нарушении норм, регулирующих получение, обработку и защиту информации, несёт дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.
3. 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, установленные локальными нормативно-правовыми актами (распоряжениями) Администрации, влекут наложение на работника, имеющего доступ к защищаемой информации, дисциплинарных взысканий (в соответствии с разделом XI главой 39 статьей 243 пунктом 7 Трудового кодекса РФ).
4. В случае незаконного сбора или публичного распространения информации о частной жизни лица (нарушения неприкосновенности частной жизни) предусмотрена ответственность в соответствии с разделом VII главой 19 статьей 137 Уголовного кодекса РФ.

С инструкцией ознакомлен:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_