РОССИЙСКАЯ ФЕДЕРАЦИЯ
АДМИНИСТРАЦИЯ
СЕЛЬСКОГО ПОСЕЛЕНИЯ
КРАСНЫЙ ЯР
МУНИЦИПАЛЬНОГО РАЙОНА
КРАСНОЯРСКИЙ
САМАРСКОЙ ОБЛАСТИ
ПОСТАНОВЛЕНИЕ

от 26.05.2015 г. № 154

с.Красный Яр

Об утверждении инструкций, определяющих работу в информационных системах персональных данных в администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области

В соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 01 ноября 2012 года № 1119, Администрация сельского поселения Красный Яр муниципального района Красноярский постановляет:

1. Назначить ответственным за обеспечение безопасности персональных данных в администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области главного специалиста Коневу Ирину Николаевну.

2. Утвердить прилагаемые:

2.1. Инструкцию ответственного за обеспечение безопасности персональных данных;

2.2. Инструкцию пользователя информационной системы персональных данных;

2.3. Инструкцию по организации парольной защиты в информационных системах персональных данных;

2.4. Инструкцию по организации антивирусной защиты в информационных системах персональных данных.

3. Контроль за исполнением настоящего постановления оставляю за собой.

Глава администрации **А.Г. Бушов**

исп. Конева И.Н.
тел. (884657) 2-20-81

Утверждена
постановлением администрации
сельского поселения Красный Яр
муниципального района Красноярский
от _____ № _____

ИНСТРУКЦИЯ
ответственного за обеспечение безопасности персональных данных

I. Общие положения

1.1. Данная инструкция регламентирует действия ответственного за обеспечение безопасности персональных данных, определяет основные цели, функции и права ответственного за обеспечение безопасности персональных данных в администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области (далее – администрации).

1.2. Для разработки и осуществления мероприятий по обеспечению безопасности персональных данных при их обработке в информационных системах в соответствии с п.14 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства РФ от 1 ноября 2012 года №1119, распоряжением администрации назначается должностное лицо, ответственное за обеспечение персональных данных, из числа работников, имеющих опыт работы по основной деятельности или в области защиты информации.

1.3. Непосредственное руководство работой ответственного за обеспечение безопасности персональных данных осуществляет Глава администрации поселения.

1.4. В своей работе ответственный за обеспечение безопасности персональных данных руководствуется законодательными и иными нормативными актами Российской Федерации в области обеспечения безопасности персональных данных, распоряжениями Главы администрации и другими руководящими документами по обеспечению безопасности персональных данных.

II. Основные функции ответственного за обеспечение безопасности персональных данных

Основными функциями ответственного за обеспечение безопасности персональных данных являются:

2.1. Проведение единой технической политики, организация и координация работ по обеспечению безопасности персональных данных в администрации.

2.2. Проведение мероприятий по организации обеспечения безопасности

персональных данных, включая определение уровней защищенности информационных систем персональных данных.

2.3. Проведение мероприятий по техническому обеспечению безопасности персональных данных при их обработке, как в информационных системах персональных данных, так и вне их, в том числе:

- мероприятия по размещению, охране, организации режима допуска в помещения, где ведется обработка персональных данных;
- мероприятия по закрытию технических каналов утечки персональных данных при их обработке;
- мероприятия по защите от несанкционированного доступа к персональным данным;
- мероприятия по выбору средств защиты персональных данных при их обработке.

2.4. Проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным или передачи их лицам, не имеющим права доступа к такой информации.

2.5. Своевременное обнаружение фактов несанкционированного доступа к персональным данным.

2.6. Обеспечение возможности восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

2.7. Постоянный контроль за обеспечением уровня защищенности персональных данных.

2.8. Разработка организационных распорядительных документов по обеспечению безопасности персональных данных в администрации.

2.9. Организация в установленном порядке расследования причин и условий появления нарушений в безопасности персональных данных и разработка предложений по устранению недостатков и предупреждению подобного рода нарушений, а также осуществление контроля за устранением этих нарушений.

2.10. Разработка предложений, участие в проводимых работах по совершенствованию системы безопасности персональных данных в администрации.

2.11. Проведение периодического контроля эффективности мер защиты персональных данных в администрации. Учет и анализ результатов контроля.

2.12. Организация повышения осведомленности руководства и сотрудников администрации по вопросам обеспечения безопасности персональных данных.

2.13. Подготовка отчетов о состоянии работ по обеспечению безопасности персональных данных в администрации.

III. Права

Ответственный за обеспечение безопасности персональных данных имеет право:

3.1. Запрашивать и получать необходимые материалы для организации и проведения работ по вопросам обеспечения безопасности персональных данных.

3.2. Разрабатывать проекты организационных и распорядительных документов по обеспечению безопасности персональных данных.

3.3. Готовить предложения о привлечении к проведению работ по защите информации на договорной основе организаций, имеющих лицензии на право проведения работ в области защиты информации.

3.4. Контролировать деятельность структурных подразделений администрации в части выполнения ими требований по обеспечению безопасности персональных данных.

3.5. Вносить предложения Главе администрации о приостановке работ в случае обнаружения несанкционированного доступа, утечки (или предпосылок для утечки) персональных данных.

3.6. Привлекать в установленном порядке необходимых специалистов из числа сотрудников администрации для проведения исследований, разработки решений, мероприятий и организационно-распорядительных документов по вопросам обеспечения безопасности персональных данных.

IV. Ответственность

4.1. Ответственный за обеспечение безопасности персональных данных несет персональную ответственность за:

– правильность и объективность принимаемых решений;

– правильное и своевременное выполнение распоряжений Главы администрации по вопросам, входящим в возложенные на него функции;

– выполнение возложенных на него обязанностей, предусмотренных настоящей инструкцией;

– соблюдение трудовой дисциплины, охраны труда;

– качество проводимых работ по обеспечению безопасности персональных данных в соответствии с функциональными обязанностями;

– за разглашение сведений ограниченного распространения, ставших известными ему по роду работы, согласно действующему законодательству Российской Федерации.

Утверждена
постановлением администрации
сельского поселения Красный Яр
муниципального района
Красноярский
от _____ № _____

Инструкция
пользователя информационной системы персональных данных

I. Общие положения

1.1. Пользователь информационной системы персональных данных (далее - ИСПДн) осуществляет обработку персональных данных в ИСПДн.

1.2. Пользователем является каждый сотрудник Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области (далее - администрации), участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

1.3. Пользователь несет персональную ответственность за свои действия.

1.4. Пользователь в своей работе руководствуется настоящей инструкцией, Концепцией информационной безопасности, Политикой информационной безопасности, руководящими и нормативными документами ФСТЭК России и регламентирующими документами администрации.

1.5. Методическое руководство работой пользователя осуществляется ответственным за обеспечение защиты персональных данных.

II. Должностные обязанности пользователей ИСПДн

Пользователь обязан:

2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

2.2. Выполнять на автоматизированном рабочем месте (АРМ) только те процедуры, которые определены для него в должностной инструкции.

2.3. Знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности ПДн, а также руководящих и организационно-распорядительных документов.

2.4. Соблюдать требования парольной политики.

2.5. Соблюдать правила при работе в сетях общего доступа и (или) международного обмена - Интернет и других.

2.6. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

2.7. Обо всех выявленных нарушениях, связанных с информационной безопасностью администрации, а также для получения консультаций по вопросам информационной безопасности, необходимо обратиться к лицу ответственному за обеспечение информационной безопасности ИСПДн.

2.8. Для получения консультаций по вопросам работы и настройке элементов ИСПДн необходимо обращаться к специалисту по информационным технологиям.

2.9. Пользователям запрещается:

- разглашать защищаемую информацию третьим лицам;

- копировать защищаемую информацию на внешние носители без разрешения своего руководителя;

- самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;

- несанкционированно открывать общий доступ к папкам на своей рабочей станции;

- запрещено подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства;

- отключать (блокировать) средства защиты информации;

- обрабатывать на автоматизированном рабочем месте (далее – АРМ) информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к ИСПДн;

- сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн;

- привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с ответственным за обеспечение защиты персональных данных.

2.10. При отсутствии визуального контроля за рабочей станцией: доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировка>.

2.11. Принимать меры по реагированию в случае возникновения внештатных ситуаций и аварийных ситуаций с целью ликвидации их последствий, в пределах, возложенных на него функций.

III. Правила работы в сетях общего доступа и (или) международного обмена

3.1. Работа в сетях общего доступа и (или) международного обмена (сети Интернет и других) (далее - Сеть) на элементах ИСПДн должна проводиться при служебной необходимости.

3.2. При работе в Сети запрещается:

- осуществлять работу при отключенных средствах защиты (антивирус и других);
- передавать по Сети защищаемую информацию без использования средств шифрования;
- запрещается скачивать из Сети программное обеспечение и другие файлы;
- запрещается посещение сайтов сомнительной репутации (порно сайты, сайты, содержащие нелегально распространяемое ПО и другие);
- запрещается нецелевое использование подключения к Сети.

Утверждена
постановлением администрации
сельского поселения Красный Яр
муниципального района
Красноярский
от _____ № _____

Инструкция
по организации парольной защиты в информационных системах персональных данных

Настоящая Инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационных системах персональных данных (далее – ИСПДн) Администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области (далее – администрации), а также контроль за действиями пользователей и обслуживающего персонала ИСПДн при работе с паролями.

1. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн администрации и контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями возлагается на ответственного за организацию обработки ПДн, являющегося специалистом по защите информации.

2. Личные пароли выбираются пользователями автоматизированной системы самостоятельно либо могут генерироваться и распределяться централизованно с учетом следующих требований:

- длина пароля должна быть не менее 6 символов;

- в числе символов пароля обязательно должны присутствовать буквы латинского алфавита в верхнем и нижнем регистрах и цифры, а также могут использоваться специальные символы (@, #, $, &, *, % и т.п.);

- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии пользователей, наименования АРМ, учетные записи и т.д.), а также общепринятые сокращения (USER, PASSWORD, MANAGER и т.п. и производные от них);

- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 3 позициях.

3. Владельцы паролей должны быть ознакомлены под роспись с настоящей инструкцией по форме согласно приложению и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

4. При наличии (в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т.п.) технологической необходимости

использования имен и паролей некоторых сотрудников в их отсутствие, такие сотрудники обязаны сразу же после смены своих паролей их новые значения (вместе с именами соответствующих учетных записей) в запечатанном конверте передавать на хранение ответственному за организацию обработки ПДн. Опечатанные конверты (пеналы) с паролями исполнителей должны храниться в сейфе.

5. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в месяц.

6. Внеплановая смена личного пароля или удаление учетной записи пользователя информационной системы в случае прекращения его полномочий (увольнение, переход на другую работу) должна производиться ответственным за организацию обработки ПДн, ответственным за организацию парольной защиты, немедленно после окончания последнего сеанса работы данного пользователя с системой.

7. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение и другие обстоятельства) ответственного за организацию обработки ПДн, ответственного за организацию парольной защиты, и других сотрудников, которым по роду служебной деятельности были предоставлены полномочия по управлению парольной защитой ИС.

8. В случае компрометации личного пароля пользователя информационной системы должны быть немедленно предприняты меры в соответствии с пунктом 4 или пунктом 5 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

9. Хранение сотрудником значений своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у Ответственного за организацию обработки ПДн, ответственного за организацию парольной защиты, или начальника отдела в опечатанном виде.

10. Каждый пользователь несет ответственность за неразглашение личного пароля третьим лицам и сохранность персонального идентификатора.

11. Повседневный контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на начальников отделов, периодический контроль возлагается на ответственного за организацию обработки ПДн, ответственного за организацию парольной защиты.

Приложение к Инструкции по организации парольной защиты в информационной системе персональных данных, утвержденной постановлением администрации сельского поселения Красный Яр муниципального района Красноярский
от _____ №___

Лист ознакомления сотрудников
с инструкцией по организации парольной защиты в информационной системе персональных данных администрации сельского поселения Красный Яр муниципального района Красноярский

С инструкцией ознакомлен(ы):

№ п/п	Фамилия сотрудника	Дата ознакомления	Роспись в ознакомлении
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			

Утверждена
постановлением администрации
сельского поселения Красный Яр
муниципального района Красноярский
от _____ № _____

Инструкция
по организации антивирусной защиты в информационных системах персональных данных администрации сельского поселения Красный Яр муниципального района Красноярский Самарской области (далее – администрации)

I. Общие положения

1.1. Настоящая Инструкция определяет требования к организации защиты объектов информатизации от разрушающего воздействия компьютерных вирусов и устанавливает ответственность сотрудников администрации, эксплуатирующих и сопровождающих информационные системы персональных данных (далее – ИСПДн), за их выполнение. Инструкция распространяется на автоматизированные системы, предназначенные для обработки информации ограниченного распространения (персональных данных). Для отдельных автоматизированных систем могут быть разработаны свои инструкции, учитывающие особенности их работы.

1.2. К использованию в ИСПДн допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств и прошедшие в установленном порядке процедуру оценки соответствия требованиям по безопасности.

1.3. Установка и настройка средств антивирусного контроля, контроль за состоянием антивирусной защиты в ИСПДн осуществляется специалистом по информационным технологиям Муниципального бюджетного учреждения «Хозяйственно-эксплуатационная служба» (далее – специалист по информационным технологиям).

1.4. Установка средств антивирусного контроля производится в программную папку «C:\Program Files\Kaspersky Lab\».

1.5. После установки и настройки средств антивирусного контроля специалистом по информационным технологиям в обязательном порядке должно быть произведено тестирование системы антивирусной защиты.

1.6. Ответственность за ежедневный антивирусный контроль в процессе эксплуатации ИСПДн и своевременное информирование специалиста по информационным технологиям в случае обнаружения действий вредоносных программ возлагается на пользователей ИСПДн.

II. Применение средств антивирусного контроля

2.1. Ежедневно в начале работы при загрузке компьютеров в

автоматическом режиме должен проводиться антивирусный контроль всех электронных носителей информации ИСПДн.

Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных носителях.

Настройка средств антивирусной защиты должна реализовывать следующие функции:

− непрерывный автоматический мониторинг информационного обмена в ИСПДн с целью выявления программно-математического воздействия (далее – ПМВ);

− автоматическая проверка на наличие вредоносных программ или последствий ПМВ при импорте в ИСПДн всех программных модулей (прикладных программ), которые могут содержать вредоносные программы, по их типовым шаблонам и с помощью эвристического анализа;

− реализация механизма автоматического блокирования обнаруженных вредоносных программ путем их удаления из программных модулей или уничтожения;

− автоматическая проверка критических областей автоматизированных рабочих мест и серверов, таких как системная память, загрузочные секторы дисков, объекты автозапуска, каталоги операционной системы «system» и «system32» при каждом запуске операционной системы;

− полная автоматическая проверка носителей информации всех автоматизированных рабочих мест и серверов не реже одного раза в неделю;

− регулярное обновление антивирусных баз и программных модулей средств антивирусной защиты;

− автоматическое документирование состояния системы антивирусной защиты ИСПДн.

2.2. Пользователи ИСПДн при работе со съемными носителями информации (flash-накопители, дискеты 3,5”, CD/DVD диски, жесткие диски USB и т.д.) обязаны перед началом работы осуществить их проверку на предмет отсутствия вредоносных программ, выполнив следующие действия:

− подключить съемный носитель информации;

− открыть значок Рабочего стола «Мой компьютер»;

− установить курсор мыши на имя выбранного носителя;

− по правой клавише мыши открыть контекстное меню Microsoft Windows и выбрать пункт, запускающий антивирусную проверку электронного носителя информации.

2.3. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

2.4. Устанавливаемое (изменяемое) программное обеспечение должно

быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера, специалистом по информационным технологиям также должна быть выполнена антивирусная проверка электронных средств обработки персональных данных.

2.5. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, появление сообщений о системных ошибках и т.п.) пользователь ИСПДн самостоятельно или вместе со специалистом по информационным технологиям должен провести внеочередной антивирусный контроль рабочей станции.

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

Пользователи ИСПДн обязаны:

- приостановить работу в ИСПДн;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов специалиста по информационным технологиям и других сотрудников, использующих эти файлы в работе;
- совместно со специалистом по информационным технологиям провести анализ необходимости дальнейшего использования зараженных файлов;

Специалист по информационным технологиям обязан провести лечение зараженных файлов или их гарантированное удаление.