АДМИНИСТРАЦИЯ ПЕТРОПАВЛОВСКОГО РАЙОНА
АЛТАЙСКОГО КРАЯ

ПОСТАНОВЛЕНИЕ

10.10.2014 № 351 с. Петропавловское

Об утверждении Положения об обеспечении безопасности общедоступной информации в информационных системах Администрации Петропавловского района и ее структурных подразделениях

На основании Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

ПОСТАНОВЛЯЮ:

1. Утвердить прилагаемое Положение об обеспечении безопасности общедоступной информации в информационных системах Администрации Петропавловского района и её структурных подразделениях.

2. Опубликовать данное постановление в Сборнике муниципальных правовых актов муниципального образования Петропавловский район Алтайского края и разместить на официальном сайте Администрации района.

3. Контроль за выполнением настоящего постановления возложить на первого заместителя главы Администрации района Толстых В. А.

Глава Администрации района С.В. Козликин

УТВЕРЖДЕНО
постановлением
Администрации района от
10.10.2014 № 351

ПОЛОЖЕНИЕ
об обеспечении безопасности общедоступной информации в информационных системах Администрации Петропавловского района и ее структурных подразделениях

1. Общие положения

1.1. Положение об обеспечении безопасности общедоступной информации в информационных системах Администрации Петропавловского района и ее структурных подразделениях (далее – Положение) разработано в соответствии с Конституцией Российской Федерации, Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и другими нормативными правовыми актами Российской Федерации, регулирующими отношения, связанные с обработкой и защитой информации.

1.2. Настоящее Положение устанавливает требования к обеспечению безопасности общедоступной информации в информационных системах Администрации района и ее структурных подразделениях (далее – ИС), доступ к которой не ограничен федеральными законами.

Под ИС понимается совокупность информации, содержащейся в базах данных, и обеспечивающих ее обработку информационных технологий, технических средств Администрации Петропавловского района (далее – Администрация) и ее структурных подразделений.

ИС используются для хранения, обработки и передачи информации в соответствии с функциями организации.

ИС включают в себя рабочие станции, сетевое оборудование, периферийное оборудование (принтеры, сканеры и т.п.) и другое специализированное оборудование организации.

1.3. Безопасность общедоступной информации при ее обработке в ИС обеспечивается применением организационных мер и технических средств защиты информации, реализующих требования нормативных правовых актов Российской Федерации.

1.4. Требования настоящего Положения и других документов, разработанных для их реализации, являются обязательными для исполнения всеми лицами, получившими доступ к общедоступной информации в ИС, и должны быть доведены до их сведения.

1.5. Решение о необходимости внесения изменений в Положение

принимается на основании:

изменения нормативных правовых актов Российской Федерации, регулирующих отношения, связанные с обработкой и защитой информации;

результатов анализа инцидентов информационной безопасности в ИС;

изменения технологии хранения и обработки информации.

1.6. Все изменения положения до их ввода в действие подлежат предварительной оценке на соответствие нормативным правовым актам и нормативным методическим документам Российской Федерации, регулирующим отношения, связанные с обработкой и защитой информации.

2. Цель защиты информации и основные виды угроз безопасности

2.1. Основной целью Положения является обеспечение принятия организационных и технических мер, направленных на:

обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, распространения, а также от иных неправомерных действий в отношении такой информации;

реализацию права на доступ к информации.

2.2. На основании Положения устанавливаются требования к:

разграничению доступа к общедоступной информации, порядку и условиям такого доступа;

порядку хранения и обработки информации;

передаче информации другим лицам по договору или на ином установленном законом основании;

2.3. Основными видами угроз безопасности общедоступной информации в ИС являются:

противоправные и (или) ошибочные действия пользователей ИС и третьих лиц;

отказы, сбои программного обеспечения и технических средств ИС, приводящие к модификации, блокированию, уничтожению, а также нарушению правил эксплуатации рабочих станций;

стихийные бедствия, техногенные аварии, сбои и отказы технических средств ИС.

3. Методы и способы защиты общедоступной информации в ИС

3.1. Для достижения основной цели защиты информации системы безопасности должны обеспечивать эффективное решение следующих задач:

предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к ней;

своевременное обнаружение фактов несанкционированного доступа;

предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

создание возможности незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

постоянный контроль за обеспечением защищенности информации.

3.2. При выполнении требований настоящего Положения Администрация руководствуется:

инструкцией по проведению антивирусного контроля в ИС (Приложение № 1);

инструкцией по организации парольной защиты в ИС (Приложение № 2);

инструкцией по организации обслуживания и ремонта технических средств ИС (Приложение № 3);

инструкцией по работе пользователей в ИС (Приложение № 4);

инструкцией по организации резервного копирования информации в ИС (Приложение № 5).

3.3. Охрана помещений, в которых ведется обработка информации и организация режима безопасности в этих помещениях, должна обеспечивать сохранность технических средств ИС, носителей информации и средств защиты информации, а также исключение возможности неконтролируемого пребывания посторонних лиц в этих помещениях.

4. Обязанности

4.1. Заведующий отделом по информационным технологиям Администрации района:

организует защиту общедоступной информации, расположенной в ИС;

определяет порядок доступа к общедоступной информации, расположенной в ИС;

осуществляет методическое руководство и внесение предложений по организации и совершенствованию систем защиты информации;

отвечает за соблюдение в ИС требований по обеспечению безопасности информации;

отвечает за своевременное обнаружение фактов несанкционированного доступа к ИС;

осуществляет администрирование ИС;

сопровождает функционирование программного обеспечения рабочих станций ИС;

в случае необходимости удаленно контролирует состояние рабочих станций;

организует и обеспечивает работы по проведению антивирусного контроля ПЭВМ.

осуществляет резервное копирование и восстановление информации, расположенной в ИС:

организует обслуживание технических средств ИС, периферийного и другого специализированного оборудования;

обеспечивает анализ и устранение неисправностей технических средств и ПО, предпринимает необходимые действия по их предупреждению.

4.2. Пользователь ИС – сотрудник, допущенный к работе в ИС:

отвечает за соблюдение установленного порядка использования программного обеспечения, а также применение технических и программных средств ИС;

соблюдает требования нормативных документов по обеспечению безопасности информации, обрабатываемой в ИС;

соблюдает разрешительную систему доступа к техническим средствам ИС и информации, обрабатываемой в ней;

не имеет права на изменение компонентов рабочих станций, отключение или изменение настроек антивирусной защиты.

5. Ответственность

5.1. Ответственность за реализацию и соблюдение требований Положения пользователями ИС возлагается на заведующего отделом по информационным технологиям Администрации района и руководителей структурных подразделений Администрации района.

5.2. Нарушение требований Положения влечет ответственность в соответствии с действующим законодательством Российской Федерации.

Приложение 1
к Положению об обеспечении безопасности общедоступной информации в информационных системах Администрации Петропавловского района и ее структурных подразделениях

ИНСТРУКЦИЯ
по проведению антивирусного контроля в информационных системах Администрации и ее структурных подразделениях

1. Общие положения

1.1. Инструкция по проведению антивирусного контроля в информационных системах Администрации и ее структурных подразделениях (далее – Инструкция) предназначена для пользователей информационных систем Администрации и ее структурных подразделений.

1.2. В целях обеспечения антивирусной защиты в информационных системах Администрации и ее структурных подразделениях производится антивирусный контроль.

1.3. Ответственность за поддержание установленного в Инструкции порядка возлагается на администратора информационной безопасности ИС.

1.4. К применению в ИС допускается лицензионное антивирусное программное обеспечение.

2. Порядок проведения антивирусного контроля в ИС

2.1. Антивирусный контроль должен осуществляться на рабочих станциях в постоянном режиме.

2.2. Пользователи ИС при работе с носителями информации обязаны перед началом работы осуществить их проверку на предмет наличия вредоносного программного обеспечения.

2.3. Администратор информационной безопасности ИС осуществляет контроль обновления антивирусных баз и функционирования антивирусной защиты информации.

2.4. Администратор информационной безопасности ИС проводит периодическое тестирование установленного программного

обеспечения на предмет наличия вирусов.

2.5. При обнаружении вредоносного программного обеспечения пользователь ИС обязан немедленно поставить в известность администратора информационной безопасности ИС и прекратить какие-либо действия в ИС.

2.6. Администратор информационной безопасности ИС проводит в случае необходимости лечение зараженных файлов с помощью антивирусного программного обеспечения и после этого вновь проводит антивирусный контроль.

2.7. В случае обнаружения на носителе информации вредоносного программного обеспечения, неподдающегося лечению, Администратор информационной безопасности ИС обязан запретить использование данного носителя информации, а также обязан поставить в известность руководителя подразделения или лицо, ответственное за обеспечение информационной безопасности, запретить работу в ИС и принять меры по восстановлению работоспособности ИС.

Приложение 2
к Положению об обеспечении безопасности общедоступной информации в информационных системах Администрации Петропавловского района Алтайского края и ее структурных подразделениях

ИНСТРУКЦИЯ
по организации парольной защиты в информационных системах Администрации и ее структурных подразделениях

1. Общие положения

1.1. Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационных системах Администрации и ее структурных подразделениях, а также контроль за действиями пользователей и обслуживающего персонала ИС при работе с парольной защитой.

1.2. Идентификация и аутентификация пользователей в ИС осуществляется посредством использования персональных учетных записей пользователей ИС и периодически сменяемых паролей. Пароли пользователей ИС должны содержать не менее шести символов, состоять из букв и цифр, а также при смене пароля отличаться от прежнего минимум на 3 символа.

1.3. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИС, а также контроль за действиями пользователей и обслуживающего персонала ИС при работе с паролями возлагается на администратора информационной безопасности ИС.

1.4. Временный пароль, задаваемый при создании учетной записи или смене забытого пароля, должен передаваться способом, исключающим доступ к нему других лиц, и быть изменен пользователем при первом обращении к ИС. Пароли, предустановленные производителем программного обеспечения, средства защиты информации и т.д. должны изменяться до начала их эксплуатации.

2. Порядок генерации, смены и прекращения действия и резервирования паролей

2.1. В целях предотвращения несанкционированного доступа посторонних лиц к ресурсам ИС пользователями осуществляется периодическая (не реже раза в шесть месяцев) замена пароля в ручном режиме в вычислительной сети и по возможности в другом программном обеспечении ИС. Замена пароля осуществляется пользователем ИС самостоятельно или с привлечением администратора информационной безопасности ИС.

2.2. В случае прекращения полномочий пользователя ИС (увольнение, переход на другую работу и т.п.) подразделение или лицо, ответственное за кадровое обеспечение организации должно уведомить об этом администратора информационной безопасности ИС.

Администратор информационной безопасности ИС должен произвести блокирование или удаление учетной записи пользователя ИС незамедлительно после получения такого уведомления.

2.3. Внеплановая смена паролей всех пользователей ИС должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и другие обстоятельства) администратора информационной безопасности ИС и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой ИС.

2.4. В случае компрометации личного пароля пользователя ИС проводится внеплановая смена пароля, которая выполняется лично или администратором информационной безопасности ИС устанавливается временный пароль.

2.5. Повседневный контроль за действиями пользователей и обслуживающего персонала ИС при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на руководителей структурных подразделений организации, администратора информационной безопасности ИС.

2.6. По решению руководителя структурного подразделения, может применяться резервирование паролей ключевых пользователей, таких, как Администратор информационной безопасности ИС, отдельных пользователей, выполняющих ключевые функции, а также пользователей, обеспечивающих работу отдельных сетевых сервисов.

2.7. Для резервирования пароля выполняются следующие действия:

пароль записывается на лист бумаги;

лист с записью пароля вкладывается владельцем в конверт. Конверт не должен допускать просмотр записи пароля на просвет. Если конверт недостаточно плотный, в него может быть вложен лист темной бумаги. Конверт заклеивается, при необходимости - опечатывается;

на конверте владелец пароля указывает свою должность,

фамилию и инициалы, наименование информационного средства, доступ к которому защищается этим паролем, текущую дату и время, при необходимости – другие данные, и заверяет запись личной подписью;

конверт передается на хранение руководителю структурного подразделения или лицу, им для этого назначенным;

конверты с паролями хранятся у руководителей структурных подразделений или у администратора информационной безопасности ИС в условиях, исключающих бесконтрольный доступ к ним. Указанные должностные лица обязаны проверять наличие конвертов с паролями, не реже раза в квартал;

при замене пароля конверт передается владельцу пароля, который уничтожает лист с резервным паролем. Новый резервный пароль подготавливается к хранению так, как указано выше;

вскрытие конверта с паролем производится по решению руководителя структурного подразделения в случае необходимости использования прав доступа его владельца в отсутствие самого владельца. О вскрытии конверта составляется акт, утверждаемый руководителем подразделения, который по окончании работы хранится в деле подразделения;

при появлении владельца пароля, после факта вскрытия конверта, пароль заменяется на новый и вновь сохраняется его копия, как описано выше.

3. Запрещается:

сообщать свой пароль другим лицам или записывать его на материальных носителях, доступных для других лиц (кроме предусмотренных случаев сохранения паролей ключевых пользователей ИС);

сохранять пароль в программно-технических средствах в открытом виде или использовать средства его автоматического ввода;

использовать учетные записи других лиц.

Приложение 3
к Положению об обеспечении безопасности общедоступной информации в информационных системах Администрации Петропавловского района Алтайского края и ее структурных подразделениях

ИНСТРУКЦИЯ
по организации обслуживания и ремонта технических средств в информационных системах Администрации и ее структурных подразделениях

1. Общие положения

Данная инструкция определяет общие принципы организации технического обслуживания и ремонта технических средств в информационных системах Администрации и ее структурных подразделениях.

Инструкция регламентирует порядок обслуживания и ремонта оборудования, сопровождения программного обеспечения, устранения неисправностей программного обеспечения и технических средств ИС.

2. Обслуживание и ремонт технических средств ИС

Обслуживание технических средств ИС выполняется для обеспечения работоспособности ИС, предотвращения ее неисправностей.

При проведении технического обслуживания (далее – «ТО») и ремонта необходимо руководствоваться следующими принципами:

выполнение регламентных работ для технических средств ИС осуществляется в соответствии с технической документацией производителя;

проведение ТО и ремонт должно осуществлять отдел по информационным технологиям, а также привлекаемые специалисты;

выполнять меры по защите информации, в случае выполнения работ сторонней организацией за пределами контролируемой зоны, защищаемая информация должна быть удалена с передаваемых носителей информации;

соблюдать требования поставщика технических средств для выполнения гарантийных обязательств.

Ответственность за своевременное проведение ТО и ремонта возла-

гается на отдел по информационным технологиям.

3. Сопровождение программного обеспечения

При сопровождении программного обеспечения (далее - ПО) необходимо руководствоваться следующими принципами:

проводить регламентные работы по сопровождению ПО должен администратор информационной безопасности ИС или привлекаемые специалисты в присутствии администратора информационной безопасности ИС;

выполнять требования лицензионного соглашения на использование ПО в соответствии с законодательством Российской Федерации;

руководствоваться технической документацией производителя при сопровождении ПО;

принимать меры по исключению несанкционированного доступа к защищаемой информации при сопровождении ПО сторонними организациями;

исключить возможность изменения пользователем состава ПО.

4. Устранение неисправностей технических средств и программного обеспечения

Заведующий отелом по информационным технологиям, обеспечивает анализ и устранение неисправностей технических средств и ПО, предпринимает необходимые действия по их предупреждению.

После выявления неисправности должны выполняться необходимые работы по восстановлению работоспособности ИС, технических средств и ПО.

Приложение 4
к Положению об обеспечении безопасности общедоступной информации в информационных системах Администрации Петропавловского района Алтайского края и ее структурных подразделениях

ИНСТРУКЦИЯ
по работе пользователей в информационных системах Администрации и ее структурных подразделениях

1. Общие положения

1.1. Данная инструкция определяет общие принципы работы пользователей в информационных системах Администрации и ее структурных подразделениях. Пользователи ИС несут персональную ответственность за свои действия.

1.2. Допуск пользователей для работы в ИС осуществляется в соответствии с их должностными обязанностями после ознакомления с документами по работе в ИС.

1.3. Доступ пользователей в ИС обеспечивает администратор информационной безопасности ИС.

2. Порядок работы пользователей в ИС

2.1. Пользователь имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ИС, присвоенными администратором информационной безопасности ИС. При этом для хранения информации ограниченного доступа разрешается использовать только учтенные носители информации (дискеты, компакт-диски, USB Flash-накопители, жесткие диски и т.д.), учтенные по журналу учета и выдачи машинных носителей информации, предназначенных для обработки и хранения информации ограниченного доступа.

2.2. Пользователь ИС отвечает за правильность включения и выключения ПЭВМ, входа/выхода в/из ИС и действия при работе в ней.

2.3. Вход пользователя в ИС осуществляется на основе ввода (по запросу системы) имени (идентификатора), присвоенного при регистрации администратором информационной безопасности ИС, и

пароля. Требования к сложности пароля и периодичности его замены установлены в инструкции по организации парольной защиты в ИС.

2.4. В случае отказа ИС в идентификации пользователя, либо не подтверждения личного пароля следует немедленно обратиться к администратору безопасности ИС.

2.5. Резервное копирование, уничтожение и восстановление защищаемой информации осуществляются пользователем в рамках выделенных полномочий, либо администратором информационной безопасности ИС, в соответствии с инструкцией по организации резервного копирования информации в ИС.

2.6. Перед началом работы с носителями информации пользователь ИС обязан проверить их на наличие вредоносного программного обеспечения с использованием антивирусного программного обеспечения, установленного в ИС, в соответствии с инструкцией по проведению антивирусного контроля в ИС. В случае обнаружения вредоносного программного обеспечения на носителе информации пользователь обязан немедленно сообщить администратору информационной безопасности ИС.

3. В процессе работы пользователю запрещается:

3.1. использовать для хранения и обработки защищаемой информации носители, не учтенные соответствующим образом;

3.2. осуществлять попытки неправомерного доступа к ресурсам ИС других пользователей;

3.3. пытаться подменять функции администратора информационной безопасности ИС по перераспределению времени работы и полномочий доступа к ресурсам ИС;

3.4. оставлять рабочую станцию с незавершенным сеансом. При отсутствии визуального контроля за рабочей станцией, доступ к ней должен быть заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировка>;

3.5. допускать посторонних лиц к рабочей станции;

3.6. сообщать (или передавать) посторонним лицам атрибуты доступа к ресурсам ИС;

3.7. самостоятельно устанавливать, тиражировать или модифицировать программное обеспечение, изменять установленный алгоритм функционирования технических средств или программного обеспечения;

3.8. открывать общий доступ к папкам на рабочей станции;

3.9. продолжать работать при обнаружении неисправности;

3.10. самостоятельно вносить изменения в конфигурацию, размещение рабочей станции и другие узлы ИС.

4. Ответственность

4.1. Ответственность за допуск пользователя к ресурсам и установленные ему полномочия несет руководитель структурного подразделения.

4.2. Пользователи ИС, нарушившие требования данной инструкции, несут ответственность в соответствии с действующим законодательством и внутренними организационно-распорядительными документами.

Приложение 5
к Положению об обеспечении безопасности общедоступной информации в информационных системах Администрации Петропавловского района Алтайского края и ее структурных подразделениях

ИНСТРУКЦИЯ
по организации резервного копирования информации в информационных системах Администрации и ее структурных подразделениях

1. Общие положения

1.1. Данная инструкция определяет порядок организации резервного копирования информации, обрабатываемой в информационных системах Администрации и ее структурных подразделениях, меры поддержания непрерывности работы ИС и восстановления их работоспособности.

1.2. Задачей данной инструкции является:

определение необходимых мероприятий по защите ИС от потери информации;

определение необходимых действий по восстановлению информации ИС в случае ее потери.

1.3. Действие настоящей инструкции распространяется на администратора информационной безопасности ИС, а в его отсутствие на замещающих его лиц и всех пользователей ИС.

1.4. Пересмотр настоящей инструкции осуществляется по мере необходимости руководителем подразделения или лицом, ответственным за обеспечение информационной безопасности.

1.5. Ответственность за обеспечение мероприятий по предотвращению инцидентов, приводящих к потере информации, возлагается на администратора информационной безопасности ИС.

1.6. Контроль за реагированием на инциденты безопасности, приводящие к потере защищаемой информации, возлагается на администратора информационной безопасности ИС.

2. Порядок резервирования информации

2.1. Система резервного копирования и хранения данных должна

обеспечивать сохранность информации на носителях информации, не участвующих в ее обработке.

2.2. Резервное копирование данных должно осуществляться на периодической основе:

для обрабатываемой информации – не реже одного раза в неделю;

для технологической информации – не реже одного раза в 6 месяцев.

Администратор информационной безопасности ИС должен контролировать наличие резервных копий не реже одного раза в месяц.

2.3. Для обеспечения возможности восстановления данных резервные копии должны храниться не менее недели.

2.4. Для защиты от неисправностей носителей информации на рабочих станциях, осуществляющих обработку и хранение информации, могут применяться технические средства, основанные на RAID-технологии (кроме RAID-0), в которой применяется дублирование информации.

2.5. Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИС, сетевое и коммуникационное оборудование, а также рабочие станции должны подключаться к сети электропитания через источники бесперебойного питания. В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

локальные источники бесперебойного электропитания для защиты отдельных рабочих станций;

источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения.

3. Реагирование на инцидент

3.1. Под инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании ИС, предоставляемых пользователям ИС, а также потеря информации.

3.2. Инцидент может произойти:

в результате непреднамеренных действий пользователей ИС;

в результате преднамеренных действий пользователей ИС или третьих лиц;

в результате нарушения правил эксплуатации технических средств ИС;

в результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.

3.3. В сроки, не превышающие 3 рабочих дня, администратором информационной безопасности ИС применяются меры по восстановлению работоспособности ИС. Предпринимаемые меры в

случае необходимости согласуются с первым заместителем главы Администрации района.

4. Восстановление информации из резервных копий

4.1. Работы по восстановлению данных из резервных копий производятся администратором информационной безопасности ИС.

4.2. Восстановление данных из резервных копий происходит в случае ее исчезновения или нарушения вследствие несанкционированного доступа в ИС, воздействия вредоносного программного обеспечения, ошибок программного обеспечения, ошибок пользователей ИС и аппаратных сбоев.

4.3. Восстановление программного обеспечения производится с носителей, входящих в комплект поставки, или их резервных копий в соответствии с технической документацией на данное программное обеспечение.