Р А С П О Р Я Ж Е Н И Е
АДМИНИСТРАЦИИ МУНИЦИПАЛЬНОГО РАЙОНА "ЧЕРНЯНСКИЙ РАЙОН" БЕЛГОРОДСКОЙ ОБЛАСТИ

23 апреля 2013 г. № 279-р

Об утверждении инструкций пользователя и администратора безопасности информации по обеспечению безопасности информации в автоматизированных системах ИСПДн «Кадровый учет» и ИСПДн «Бухгалтерский учет» администрации Чернянского района

В целях исполнения Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных»

1. Утвердить инструкции пользователя и администратора безопасности информации по обеспечению безопасности информации в автоматизированных системах ИСПДн «Кадровый учет» и ИСПДн «Бухгалтерский учет» администрации Чернянского района (прилагается).

2. Контроль исполнения постановления оставляю за собой.

Глава администрации
Чернянского района **И.В. Гапотченко**

Утверждена

распоряжением администрации
муниципального района
«Чернянский район»

от 23 апреля 2013 г. № 279-р

ИНСТРУКЦИИ
пользователя и администратора безопасности информации по обеспечению безопасности информации в автоматизированных системах ИСПДн «Кадровый учет» и ИСПДн «Бухгалтерский учет» администрации Чернянского района

Общие положения

Настоящие Инструкции определяют функции, права и обязанности администратора безопасности информации и пользователей автоматизированных систем (АС) информационных систем персональных данных (ИСПДн) администрации муниципального района «Чернянский район» Белгородской области (далее «АС ИСПДн») по вопросам обеспечения информационной безопасности при подготовке и исполнении конфиденциальных документов.

Настоящие Инструкции являются дополнением к действующим нормативным документам по вопросам обеспечения безопасности информации и защите информации, и не исключают обязательного выполнения их требований.

Инструкция администратора безопасности информации

Администратор безопасности информации в администрации муниципального района «Чернянский район» Белгородской области (далее – администрация района) назначается постановлением администрации района.

Администратор безопасности информации обеспечивает правильность использования и нормальное функционирование системы защиты информации (СЗИ) на объекте информатизации.

Основные функции администратора безопасности информации в администрации района:

– контроль за выполнением требований действующих нормативных документов по вопросам обеспечения режима конфиденциальности, при проведении работ в «АС ИСПДн»;

– настройка и сопровождение в процессе эксплуатации подсистемы управления доступом в «АС ИСПДн»;

– контроль доступа лиц в помещение «АС ИСПДн»;

– контроль за проведением периодической смены паролей для доступа пользователей в «АС ИСПДн»;

– настройка и сопровождение подсистемы регистрации и учета действий пользователей при работе в «АС ИСПДн»;

– сопровождение подсистемы обеспечения целостности информации в «АС ИСПДн»;

– сопровождение подсистемы защиты информации от утечки за счет ПЭМИН, контроль соблюдения требований по размещению и использованию технических средств и систем, указанных в Предписании на эксплуатацию;

– анализировать данные журналов аудита «АС ИСПДн» с целью выявления возможных нарушений требований защиты;

– оценивать возможность и последствия внесения изменений в состав «АС ИСПДн» с учетом требований по защите, подготавливать свои предложения;

– контролировать физическую сохранность средств и оборудования «АС ИСПДн»;

– своевременно анализировать журналы учета событий, регистрируемых средствами защиты, с целью выявления возможных нарушений;

– в период профилактических работ на рабочих станциях «АС ИСПДн» снимать при необходимости средства защиты информации с эксплуатации с обязательным обеспечением сохранности информации;

–периодически предоставлять сотруднику, ответственному за обеспечение безопасности персональных данных отчет о состоянии защиты «АС ИСПДн» и о нештатных ситуациях и допущенных пользователями нарушений установленных требований по защите информации.

Администратор безопасности информации в администрации района имеет право:

– участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа;

– требовать прекращения обработки информации в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации;

– блокировать учетные записи пользователей, осуществивших несанкционированный доступ к защищаемым ресурсам;

– участвовать в любых проверках в «АС ИСПДн»;

– запрещать устанавливать на серверах и рабочих станциях нештатное программное и аппаратное обеспечение;

– вести контроль за процессом резервирования и дублирования важных ресурсов «АС ИСПДн»;

– участвовать в приемке новых программных средств;

– уточнять в установленном порядке обязанности пользователей «АС ИСПДн» по поддержанию уровня защиты;

– вносить предложения по совершенствованию уровня защиты «АС ИСПДн»;

– запрещать и немедленно блокировать попытки изменения программно-аппаратной среды «АС ИСПДн» без согласования порядка ввода новых (отремонтированных) технических и программных средств и средств защиты информации;

– запрещать и немедленно блокировать применение пользователям «АС ИСПДн» программ, с помощью которых возможны факты несанкционированного доступа к ресурсам «АС ИСПДн»;

– незамедлительно докладывать ответственному за обеспечение безопасности персональных данных обо всех попытках нарушения защиты «АС ИСПДн»;

– анализировать состояние защиты «АС ИСПДн» и ее отдельных подсистем;

– контролировать состояние средств и систем защиты информации и их параметры и критерии;

– контролировать правильность применения пользователями средств защиты информации;

– оказывать помощь пользователям в части применения средств защиты;

– не допускать установку, использование, хранение и размножение в «АС ИСПДн» программных средств, не связанных с выполнением функциональных задач;

– осуществлять контроль за соблюдением установленных правил и параметров регистрации и учета бумажных носителей информации;

– контролировать установленный порядок и правила антивирусной защиты информации;

– контролировать отсутствие на машинных носителях остаточной информации по окончании работы;

– не допускать к работе на рабочих станциях «АС ИСПДн» посторонних лиц.

Администратор безопасности информации в администрации района обязан:

– знать в совершенстве применяемые информационные технологии;

– участвовать в контрольных и тестовых испытаниях и проверках «АС ИСПДн»;

– знать права доступа пользователей по обработке, хранению и передаче защищаемой информации;

– обеспечивать функционирование и поддерживать работоспособность средств и систем защиты информации в пределах возложенных функций;

– проводить инструктаж пользователей по правилам работы на в «АС ИСПДн»;

– в случае отказа средств и систем защиты информации принимать меры по их восстановлению;

– докладывать сотруднику, ответственному за обеспечение безопасности персональных данных о неправомерных действиях пользователя, приводящих к нарушению требований по защите информации;

– вести документацию в «АС ИСПДн», в соответствии с требованиями нормативных документов;

– настраивать только те параметры системы, которые определяют права доступа пользователей к информации;

– производить периодическое тестирование всех реализованных программно-техническими средствами функций и требований по обеспечению информационной безопасности;

– в соответствии с постановлением администрации района и разрешительной системой доступа осуществлять добавление, блокирование, удаление и назначение прав доступа пользователям в системе;

– определить начальное значение паролей пользователя;

– восстанавливать настройки средств защиты информации при сбоях;

– хранить журналы аудита средств защиты информации на весь срок исковой давности действий и 5 лет после его окончания.

При выявлении факта несанкционированного доступа администратор безопасности информации в администрации района обязан:

– блокировать доступ к конфиденциальной информации;

– проанализировать характер несанкционированного доступа

– доложить ответственному за обеспечение безопасности персональных данных служебной запиской о факте несанкционированного доступа, его результате (успешный, неуспешный) и предпринятых действиях;

– принять меры к защите от несанкционированного доступа;

– по решению ответственного за обеспечение безопасности персональных данных возобновить работу.

Администратору безопасности информации в администрации района запрещается:

– производить действия по настройке параметров системного и специального программного обеспечения;

– устанавливать срок действия учетной записи пользователя более 1 (одного) года; по истечении указанного срока в соответствии с разрешительной системой доступа производится продление действия учетной записи либо определение прав на такое продление;

– производить установку прикладного и специального программного обеспечения;

– фиксировать учетные данные пользователя (пароли, идентификаторы, ключи и др.) на твердых носителях, а также сообщать их кому бы то ни было, кроме самого пользователя.

При возникновении ситуаций, не описываемых руководящими документами, решение принимает администратор безопасности информации, руководствуясь Положением по организации и проведению работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных.

Ответственность за сохранность конфиденциальной информации несет администратор безопасности информации, действия которого фиксируются в протоколах аудита.

Администратор безопасности информации несет ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования этих учетных записей.

При нарушениях администратором безопасности информации правил, связанных с информационной безопасностью, он несет ответственность, установленную действующим законодательством Российской Федерации.

Инструкция по работе пользователей в автоматизированной системе

Допуск пользователей для работы в «АС ИСПДн» осуществляется в соответствии с постановлением администрации района и разрешительной системой доступа.

Пользователь имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам компьютера. При этом для хранения файлов, содержащих конфиденциальную информацию, разрешается использовать только специально выделенные каталоги на несъемных носителях информации, а также соответствующим образом учтенные съёмные носители информации.

Присвоение пользователю полномочий доступа к ресурсам компьютера, состав необходимого системного и прикладного программного обеспечения для решения поставленных задач и определение возможного времени работы пользователя в «АС ИСПДн» осуществляется при первичной регистрации пользователя администратором безопасности информации.

Пользователь отвечает за правильность включения и выключения технических средств и систем, входа в систему и все действия при работе в «АС ИСПДн»

Вход пользователя в систему осуществляется на основе ввода имени, присвоенного при первичной регистрации и ввода личного пароля. Требования к парольной защите определяется инструкцией по парольной защите.

В целях предотвращения несанкционированного доступа посторонних лиц к ресурсам пользователя осуществляется периодическая (раз в месяц) замена пароля постоянного пользователя. Замена личного пароля осуществляется пользователем самостоятельно.

При работе со съемными носителями информации пользователь каждый раз перед началом работы обязан проверить их на наличие вирусов с использованием установленных антивирусных программ, в соответствии с Инструкцией по антивирусной защите.

Пользователь обязан:

– знать и строго выполнять установленные правила и обязанности по доступу к защищаемым ресурсам и соблюдению принятого режима информационной безопасности;

– обеспечить правильность вводимых данных;

– своевременно сообщать администратору безопасности об изменениях статуса пользователя;

– незамедлительно сообщить администратору безопасности факты выявления инцидентов с доступом к конфиденциальной информации.

В процессе работы пользователю запрещается:

– использовать для постоянного хранения и обработки конфиденциальной информации каталоги несъемных носителей информации, за исключением выделенных каталогов;

– осуществлять попытки несанкционированного доступа к ресурсам операционной системы;

– в рамках выделенных ресурсов и полномочий доступа к ним обрабатывать информацию с уровнем конфиденциальности, выше заявленного при регистрации;

– пытаться подменять функции администратора по перераспределению времени работы и полномочий доступа к ресурсам компьютера;

– покидать помещение с не заблокированной учетной записью;

– отключать установленные средства защиты информации;

– использовать машинные носители без их предварительной проверки антивирусными средствами;

– устанавливать программное обеспечение;

– менять параметры конфигурации ранее установленных программных средств;

– использовать пароль, предоставленный администратором безопасности для первоначального доступа в качестве постоянного рабочего пароля;

– использование различными пользователями одной и той же учетной записи, даже если пользователи имеют одинаковые полномочия по доступу;

– запрещается передавать в любом виде или сообщать идентификаторы и пароли для доступа другим лицам, в том числе и своим руководителям;

– хранение пароля на любых твердых носителях, позволяющих другим лицам получить информацию о пароле;

– использовать информацию, полученную в результате доступа к БД, в целях, не предусмотренных его функциональными обязанностями.

Ответственность за сохранность и правильное использование информации, ставшей известной в процессе обработки конфиденциальной информации несет пользователь.

Возможность получения технического доступа к конфиденциальной информации не дает права пользователям обработки такой информации, если им не предоставлены права доступа к этой информации. Такие действия рассматриваются как попытки несанкционированного доступа.

При выявлении инцидентов с доступом к конфиденциальной информации доступ пользователей к ней может быть ограничен до окончания расследования инцидента, о чем пользователь уведомляется в кратчайшие сроки. По результатам служебного расследования нарушитель может быть лишен прав доступа к конфиденциальной информации, материалы расследования могут быть направлены в соответствующие службы для привлечения нарушителя к ответственности.

Пользователь несет ответственность за все действия, совершенные от имени его учетной записи, если не доказан факт несанкционированного использования этой учетной записи.

При нарушениях пользователем правил, связанных с информационной безопасностью, он несет ответственность, установленную действующим законодательством Российской Федерации.

Инструкция по парольной защите

Данная инструкция призвана регламентировать организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в автоматизированной системе, а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах «АС ИСПДн» и контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на администратора безопасности.

Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями автоматизированной системы самостоятельно с учетом следующих требований:

– длина пароля должна быть не менее 8 символов;

– в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);

– пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, номера телефонов и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);

– при смене пароля новое значение должно отличаться от предыдущего не менее чем в 8 позициях;

– личный пароль пользователь не имеет права сообщать никому.

Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

Для генерации «стойких» значений паролей могут применяться специальные программные средства.

При наличии технологической необходимости использования имен и паролей некоторых сотрудников (исполнителей) в их отсутствие (например, в случае возникновении нештатных ситуаций, форс-мажорных обстоятельств и т.п.), такие сотрудники обязаны сразу же после смены своих паролей их новые значения (вместе с именами своих учетных записей) в запечатанном конверте или опечатанном пенале передавать на хранение администратору безопасности.

Опечатанные конверты с паролями исполнителей должны храниться в сейфе. Для опечатывания конвертов должны применяться личные печати владельцев паролей.

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

Внеплановая смена личного пароля или удаление учетной записи пользователя автоматизированной системы в случае прекращения его

полномочий должна производиться администратором безопасности немедленно.

Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий администраторов и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой.

В случае компрометации личного пароля пользователя автоматизированной системы должны быть немедленно предприняты меры по внеплановой смене паролей.

Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

Инструкция по антивирусной защите

Ответственность за поддержание установленного в настоящей Инструкции порядка проведения антивирусного контроля возлагается на администратора безопасности информации «АС ИСПДн».

К применению в «АС ИСПДн» допускаются сертифицированные ФСБ и ФСТЭК России антивирусные средства.

В «АС ИСПДн» запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации.

Пользователи «АС ИСПДн» при работе со съемными носителями информации обязаны перед началом работы осуществить их проверку на предмет отсутствия компьютерных вирусов.

Ярлык для запуска антивирусной программы должен быть вынесен в окно «Рабочий стол» операционной системы Windows.

Администратор безопасности информации осуществляет периодическое обновление антивирусных пакетов и контроль их работоспособности.

Администратор безопасности информации проводит периодическое тестирование всего установленного программного обеспечения на предмет отсутствия компьютерных вирусов.

При обнаружении компьютерного вируса пользователь обязан сообщить об этом факте администратору безопасности.

В случае обнаружения на сменных носителях информации нового вируса, не поддающегося лечению, администратор безопасности информации обязан запретить (приостановить) использование этих носителей до обезвреживания вируса, передать вирус в компанию производитель применяемого антивирусного средства и сообщить об этом факте ответственному за обеспечение безопасности персональных данных.

Начальник отдела
информатизации и электронного
межведомственного взаимодействия
администрации Чернянского района **В. Черкесов**

Лист ознакомления с инстукции пользователя и администратора безопасности информации по обеспечению безопасности информации в автоматизированных системах ИСПДн «Кадровый учет» и ИСПДн «Бухгалтерский учет» администрации Чернянского района

«Ознакомлен»	Инициалы и фамилия	Личная подпись