

**АДМИНИСТРАЦИЯ**

**БЕЛОВСКОГО РАЙОНА КУРСКОЙ ОБЛАСТИ**

Р А С П О Р Я Ж Е Н И Е

от 14.08.2020 г. № 115-р

**307910 Курская область, сл. Белая**

|  |
| --- |
| **Об утверждении Комплекта инструкций администраторам системы и пользователям по обеспечению безопасности информации в автоматизированной информационной системе Администрации Беловского района** |

В соответствии с Федеральным законом от 27.07.2006 г. №152-ФЗ «О персональных данных» (с последующими изменениями и дополнениями), во исполнение постановления Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» с последующими изменениями и дополнениями), приказом Федеральной службы по техническому и экспортному контролю от 18.02.2013 г. №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (с последующими изменениями и дополнениями):

1. Утвердить Комплект инструкций администраторам системы и пользователям по обеспечению безопасности информации в информационных системах Администрации Беловского района Курской области.
2. Контроль за выполнением настоящего распоряжения возложить на Управляющего делами Администрации Беловского района А.В. Шепелева.
3. Распоряжение вступает в силу со дня его подписания

Глава Беловского района

Курской области Н.В. Волобуев

УТВЕРЖДЁН распоряжением Администрации Беловского района от 14.08.2020 г. № 115-р

**Комплект инструкций**

**администраторам системы и пользователям по обеспечению безопасности информации в государственной информационной системе Администрации Беловского района Курской области**

## ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая Инструкция определяет функции, права и обязанности администратора безопасности информации и пользователей информационной системы в Администрации Беловского района Курской области (далее ГИС) и ИСПДн в её составе по вопросам обеспечения информационной безопасности при работе с информацией ограниченного доступа.

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

## ИНСТРУКЦИЯ АДМИНИСТРАТОРУ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Администратор безопасности информации назначается постановлением Администрации Беловского района Курской области.

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

Основные функции администратора:

* контроль за выполнением требований действующих нормативных документов по вопросам обеспечения режима конфиденциальности, при проведении работ в ГИС;
* настройка и сопровождение в процессе эксплуатации подсистемы управления доступом в ГИС;
* контроль доступа лиц в помещение ГИС;
* контроль за проведением периодической смены паролей для доступа пользователей в ГИС;
* настройка и сопровождение подсистемы регистрации и учета действий пользователей при работе в ГИС;
* сопровождение подсистемы обеспечения целостности информации в ГИС;
* сопровождение подсистемы защиты информации от утечки, контроль соблюдения требований по размещению и использованию технических средств и систем;
* анализировать данные журналов аудита ГИС с целью выявления возможных нарушений требований защиты;
* оценивать возможность и последствия внесения изменений в состав ГИС с учетом требований по защите, подготавливать свои предложения;
* контролировать физическую сохранность средств и оборудования ГИС;
* своевременно анализировать журналы учета событий, регистрируемых средствами защиты, с целью выявления возможных нарушений;
* в период профилактических работ на рабочих станциях ГИС снимать при необходимости средства защиты информации с эксплуатации с обязательным обеспечением сохранности информации;
* периодически предоставлять Главе Администрации Беловского района Курской области отчет о состоянии защиты ГИС и о нештатных ситуациях и допущенных пользователями нарушений установленных требований по защите информации.

Администратор безопасности информации 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 ГИС;
* запрещать устанавливать на серверах и рабочих станциях нештатное программное и аппаратное обеспечение;
* вести контроль за процессом резервирования и дублирования важных ресурсов ГИС;
* участвовать в приемке новых программных средств;
* уточнять в установленном порядке обязанности пользователей ГИС по поддержанию уровня защиты;
* вносить предложения по совершенствованию уровня защиты ГИС;
* запрещать и немедленно блокировать попытки изменения программно-аппаратной среды ГИС без согласования порядка ввода новых (отремонтированных) технических и программных средств и средств защиты информации;
* запрещать и немедленно блокировать применение пользователями ГИС программ, с помощью которых возможны факты несанкционированного доступа к ресурсам ГИС;
* незамедлительно докладывать Главе Администрации Беловского района Курской области обо всех попытках нарушения защиты ГИС;
* анализировать состояние защиты ГИС 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 ГИС программных средств, не связанных с выполнением функциональных задач;
* осуществлять контроль за соблюдением установленных правил и параметров регистрации и учета бумажных носителей информации;
* осуществлять контроль уничтожения (стирание) информации на машинных носителях при их передаче между пользователями и в сторонние организации;
* 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 ГИС посторонних лиц.

Администратор безопасности информации обязан:

* знать в совершенстве применяемые информационные технологии;
* участвовать в контрольных и тестовых испытаниях и проверках ГИС;
* 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 в ГИС;
* в случае отказа средств и систем защиты информации принимать меры по их восстановлению;
* докладывать Главе Администрации Беловского района Курской области о неправомерных действиях пользователя, приводящих к нарушению требований по защите информации;
* вести документацию в ГИС, 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 распоряжением главы Администрации Беловского района Курской области и разрешительной системой доступа осуществлять добавление, блокирование, удаление и назначение прав доступа пользователям в системе;
* определять начальное значение паролей пользователя;
* восстанавливать настройки средств защиты информации при сбоях;

При выявлении факта несанкционированного доступа администратор безопасности информации обязан:

* блокировать доступ к информации ограниченного доступа;
* проанализировать характер несанкционированного доступа;
* доложить Главе Администрации Беловского района Курской области запиской о факте несанкционированного доступа, его результате (успешный, неуспешный) и предпринятых действиях;
* принять меры к защите от несанкционированного доступа;
* по решению Главы Администрации Беловского района Курской области возобновить работу.

Администратору безопасности информации 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 стороннего 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 действующим законодательством РФ.

Ответственность за сохранность информации ограниченного доступа несет администратор безопасности информации, действия которых 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, они несут ответственность, установленную действующим законодательством Российской Федерации.

## ИНСТРУКЦИЯ ПО РАБОТЕ ПОЛЬЗОВАТЕЛЕЙ В ГИС

Допуск пользователей для работы в ГИС осуществляется в соответствии с распоряжением Главы Администрации Беловского района Курской области 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 информацию ограниченного доступа, 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 ГИС 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 ГИС.

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.

При передаче съемных носителей информации между пользователями либо в сторонние организации для ремонта или утилизации пользователь производит уничтожение (стирание) информации ограниченного доступа на таких машинных носителях, после чего осуществляет контроль уничтожения (стирания) информации. Уничтожение (стирание) информации производится внедренными в ГИС сертифицированными средствами защиты информации с использованием механизмов очистки остаточной информации в соответствии с эксплуатационной документацией на такие средства защиты. Уничтожение (стирание) информации ограниченного доступа при передаче между пользователями может не производиться пользователем только при условии предварительного шифрования такой информации средствами криптографической защиты информации, если таковые внедрены в ГИС.

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 информации ограниченного доступа.

В процессе работы пользователю запрещается:

* использовать для постоянного хранения и обработки информации ограниченного доступа 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 незаблокированной 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 информации ограниченного доступа несет пользователь.

Возможность получения технического доступа к информации ограниченного доступа 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 информации ограниченного доступа 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 информации ограниченного доступа, 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 организации, 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 ГИС 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) передавать на хранение администратору безопасности.

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 ГИС.

К применению в ГИС допускаются сертифицированные ФСБ и ФСТЭК России антивирусные средства.

В ГИС запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации.

Пользователи ГИС 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 Главе Администрации Беловского района Курской области.

## ИНСТРУКЦИЯ ПО УЧЕТУ И МАРКИРОВАНИЮ СЪЕМНЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ (ПЕРСОНАЛЬНЫХ ДАННЫХ)

С целью реализации режима ограниченного доступа к персональным данным в Администрации Беловского района Курской области и недопущению бесконтрольного использования машинных носителей, содержащих персональные данные, вводится их маркирование и поэкземплярный учет.

При маркировании на машинный носитель должна быть нанесена следующая информация:

* Администрация Беловского района Курской области;
* надпись «Содержит персональные данные» (в случае наличия);
* учетный/инвентарный номер.

Организация и контроль за выполнением учета машинных носителей, содержащих персональные данные, возлагается на лицо, ответственное за обеспечение безопасности персональных данных в информационной системе в Администрации Беловского района Курской области.

Учет машинных носителей, содержащих персональные данные, осуществляется по Журналу учета машинных носителей информации:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № п/п | Метка съемного носителя (учетный номер) | Ответственный за хранение | Дата регистрации | Подпись | Примечание <\*> |
| 1. |  |  |  |  |  |
| 2. |  |  |  |  |  |
| ... |  |  |  |  |  |