



АДМИНИСТРАЦИЯ МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ
СЕВЕРСКИЙ РАЙОН

РАСПОРЯЖЕНИЕ

от 18.09.2023

станция Северская

№ 144-12

Об утверждении Правил доступа и работы
в информационных системах в администрации
муниципального образования Северский район

Во исполнение положений Федеральных законов от 27 июля 2006 года № 149-ФЗ "Об информации, информационных технологиях и о защите информации", от 27 июля 2006 года № 152-ФЗ "О персональных данных", постановлении Правительства Российской Федерации от 21 марта 2012 года № 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами":

1. Утвердить Правила доступа и работы в информационных системах в администрации муниципального образования Северский район (далее – Правила доступа и работы) согласно приложению к настоящему распоряжению.
2. Управлению информатизации и информационной безопасности администрации муниципального образования Северский район (Сергиевская) ознакомить под роспись начальников структурных подразделений администрации с настоящими Правилами доступа и работы.
3. Управлению кадровой политики (Галицкий) обеспечить согласование заявок на предоставление доступа к информационным системам в соответствии с должностными обязанностями сотрудников администрации.
4. Контроль за исполнением настоящего распоряжения возложить на заместителя главы администрации М.Н.Чернову.
5. Распоряжение вступает в силу со дня его подписания.

Глава муниципального образования
Северский район

А.В.Дорошевский



ПРИЛОЖЕНИЕ

УТВЕРЖДЕНЫ
распоряжением администрации
муниципального образования

Северский район
от 18.09.2023 № 144-12

ПРАВИЛА

доступа и работы в информационных системах в
администрации муниципального образования Северский район

1. Общие положения

Настоящие правила доступа и работы в информационных системах в администрации муниципального образования Северский район (далее – Правила) определяют порядок предоставления доступа сотрудникам структурных подразделений администрации муниципального образования Северский район (далее – администрации) к локальным и государственным информационным системам и основные организационные правила работы в них. Выполнение данных правил нацелено на предотвращение угрозы несанкционированного доступа к информационным системам.

2. Основные понятия, термины и сокращения

Информационная система (далее – ИС) - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

Доступ к информации в ИС - возможность получения информации в ИС и ее использования;

пользователь ИС – сотрудник, получивший доступ к информации в ИС, идентифициция пользователя – это процесс, при котором пользователь сообщает ИС свое уникальное имя (логин, идентификатор);

аутентификация пользователя (проверка подлинности) - процесс, позволяющий ИС убедиться в том, что субъект, сообщивший свой идентификатор, действительно тот, за кого себя выдает;

обработка информации - любое действие (операция) или совокупность действий (операций), совершаемых в ИС, включая чтение, запись, изменение, извлечение, импорт (выгрузка) в другую ИС или в транспортный файл, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение данных;

конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

предоставление информации - действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;

распространение информации - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

блокирование данных - временное прекращение обработки данных (за исключением случаев, если обработка необходима для уточнения данных);

уничтожение данных - действия, в результате которых становится невозможным восстановить содержание данных в информационной системе и (или) в результате которых уничтожаются материальные носители данных;

электронная подпись (далее - ЭП) - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию;

сертификат ключа проверки электронной подписи - электронный документ и документ на бумажном носителе, выданные удостоверяющим центром и подтверждающие принадлежность ключа проверки ЭП владельцу ЭП; **владелец электронной подписи** - сотрудник администрации, наделенный правом использования собственной ЭП при обмене информацией от имени администрации (или подразделения администрации) с другой организацией - участником электронного взаимодействия.

3. Жизненный цикл информационных систем

3.1. Любая ИС проходит 3 этапа жизненного цикла:
ввод в эксплуатацию ИС;
эксплуатация ИС;
вывод ИС из эксплуатации.

3.2. Ввод в эксплуатацию. Данный этап может разделяться на 2 под-этапа: тестовая (опытная) эксплуатация. На данном этапе происходит испытание ИС в части проверки полноты функционирования. В ИС может размещаться недостоверная, тестовая информация.

промышленная (продуктивная) эксплуатация. На данном этапе в ИС размещается только достоверная, актуальная информация.

Этап ввода ИС в эксплуатацию должен сопровождаться изданием нормативного документа, в котором определяется:

дата начала эксплуатации ИС;

подразделение или сотрудник администрации, ответственный за техническое сопровождение данной ИС;

сотрудники подразделений администрации, являющиеся администраторами ИС, ответственные за предоставление, разграничение доступа к информации в данной ИС, если это предусмотрено возможностями ИС;

сотрудники подразделений администрации, ответственные за обработку информации в данной ИС с указанием конкретных прав (ролей), если это предусмотрено возможностями конкретной ИС, в том числе условий использования ЭП (если это предусмотрено возможностями конкретной ИС).

3.3. Эксплуатация ИС. На данном этапе сотрудники могут получить доступ к ИС, выполнять обработку информации (данных) в ИС.

3.4. Вывод ИС из эксплуатации.

Этап вывода ИС из эксплуатации должен сопровождаться изданием нормативного документа, в котором определяется необходимость дальнейшего хранения информации, размещенной в данной ИС. В случае такой необходимости необходимо определить:

электронный носитель (HDD, диск CD-R или DVD-R) архивной информации;

место хранения данного носителя;

срок хранения данной архивной информации;

сотрудника или подразделения, ответственных за хранение данного носителя;

порядок уничтожения информации (носителя) по истечению срока хранения.

4. Предоставление и прекращение доступа к ИС

4.1. Доступ к ИС предоставляется конкретному сотруднику на период исполнения им должностных обязанностей, требующих доступа к конкретной ИС.

4.2. Необходимость предоставления доступа сотрудников к ИС определяется руководителем структурного подразделения администрации на основании задач и полномочий, решаемых данным структурным подразделением и должностных обязанностей сотрудников.

4.3. При наличии в ИС возможности разграничения прав доступа (ролей) руководитель структурного подразделения администрации распределяет роли сотрудников в ИС согласно должностных обязанностей сотрудников.

4.4. Право доступа (роль) сотрудника определяется по принципу минимальной необходимости:

сотрудник должен обладать правом, позволяющим ему полностью исполнять свои должностные обязанности, но не должен иметь права доступа к информации, выходящей за их пределы.

4.5. Доступ сотруднику предоставляется посредством создания управления информатизации и информационной безопасности для него в ИС личной учетной записи на основании предоставленного распоряжения администрации, в котором указаны:

основание (полномочия, нормативный документ, иные документы), определяющие необходимость внесения информации в ИС данным структурным подразделением;

наименование информационной системы;

ответственного руководителя структурного подразделения, курирующего внесение информации в данную ИС; фамилия, имя, отчество, должность ответственного сотрудника администрации;

полномочия сотрудника (внесение данных, подготовка ответов на заявление, контроль правильности и актуальности информации, подписание информации, ответов и другие).

4.6. Учетная запись пользователя ИС состоит из двух параметров: имени и пароля пользователя (далее - логин).

Имя пользователя создается в ИС на основании требований конкретной ИС. Имя пользователя является уникальным для данной ИС и не подлежит изменению. Уникальность и постоянство логина пользователя ИС позволяет определять авторство каждому действию с информацией, совершаемому в ИС.

Пароль предоставляется администратором ИС, назначенным из числа сотрудников управления информатизации и информационной безопасности. Замена пароля производится в соответствии с инструкцией по парольной защите и актуальными требованиями по защите информации.

4.7. ИС ведут протоколирование всех действий, производимых пользователями над информацией, размещаемой в данной ИС. Достоверность аудита обеспечивается идентификацией (доступ только определенному кругу лиц) и аутентификацией (учетная запись определяет конкретного пользователя) пользователей.

4.8. Доступ предоставляется на основании заявки руководителя структурного подразделения (согласно приложению к Правилам), направленной администратору ИС, с отметкой сотрудника управления кадровой политики о наличии данных обязанностей в должностных обязанностях у сотрудника подразделения.

При изменении должностных обязанностей сотрудника подразделения, повлекших за собой изменение роли в ИС или прекращение необходимости доступа в ИС, начальник структурного подразделения администрации информирует об этом администратора ИС служебной запиской.

5. Работа с электронной подписью

5.1. Назначение лиц, наделенных правом владения и использования собственной ЭП в электронном взаимодействии от имени администрации, производится на основании распоряжения администрации муниципального образования Северский район и предоставленной копии доверенности, выданной главой муниципального образования Северский район на проведение мероприятий в ИС: внесение данных, изменений в размещенную ранее информацию, подписание документов, отправку сведений, подписанных ЭП сотрудника и другие действия, которые глава муниципального образования Северский район доверяет производить сотруднику администрации – владельцу ЭП, действующему в ИС от имени администрации).

5.2. В целях признания юридической силы электронных документов в распоряжении о назначении ответственных лиц, наделенных правом ЭП при электронном взаимодействии, указывается:

полное наименование информационной системы; права (роль) данного сотрудника в данной ИС, название отчетной формы, документа, на подписание которой сотрудник предоставляется право подписи.

6. Обязанности пользователей ИС

6.1. Обязанности пользователей ИС:

6.1.1. Пользователь ИС совершает обработку данных, используя личную учетную запись (имя пользователя, учетное имя) с паролем.

6.1.2. Все действия, выполняемые в системе под учетной записью пользователя ИС, считаются совершенными самим пользователем. Пользователь ИС обязан предпринимать меры, не допускающие возможности разглашения своего пароля. Недопустимо сообщать свой пароль другим лицам, записывать его на общедоступных носителях. При подозрении на компрометацию пароля, (то есть утраты его секретности) пользователь ИС обязан проинформировать о данном факте начальника структурного подразделения администрации и обратиться к администратору ИС для его изменения или блокирования учетной записи.

6.2. Обязанности руководителя структурного подразделения администрации:

6.2.1. Назначает дублирующих сотрудников на каждую роль ИС, организует работу в ИС таким образом, чтобы отсутствие отдельных сотрудников (в периоды отпусков, болезни, командировки и прочее) не влияло на своевременность выполнения задач структурного подразделения, исполнения работы в ИС.

6.2.2. Контролирует и пресекает факты передачи учетной записи одного пользователя ИС другому.

6.2.3. В случае возникновения или подозрения на возникновение угрозы компрометации учетной записи пользователя ИС, влекущей за собой возможность уничтожения, блокирования, искажения информации в ИС оперативно (в течение 1 рабочего дня) информирует администратора ИС о необходимости прекращения доступа сотруднику к ИС (блокировки учетной записи).

6.3. Обязанности администратора ИС:

6.3.1. Администратор ИС обязан своевременно, в течение 1 рабочего дня, выполнять заявки начальников структурных подразделений администрации на предоставление доступа к ИС.

6.3.2. При необходимости проведения служебного расследования предоставлять руководителю протокол совершенных действий, имеющийся в ИС.

6.3.3. Периодически получать информацию из управления кадровой политики о припятьх, увольненных и переведенных сотрудников администрации, на основании которой проводить аудит работы данных пользователей в ИС.

6.3.4. Незамедлительно докладывать заместителю главы администрации, курирующему данное направление, о выявленных фактах использования логина уволенного сотрудника.

6.4. Сотрудники администрации, наделенные правом использования ЭП в ИС обязаны:

6.4.1. Обеспечивать конфиденциальность ключей ЭП, в частности не допускать использование принадлежащих им ключей ЭП без их согласия.

6.4.2. Уведомлять администратора ИС и удостоверяющий центр, выдавший сертификат ключа проверки ЭП, и иных участников электронного взаимодействия о нарушении конфиденциальности ключа ЭП в течение не более чем одного рабочего дня со дня получения информации о таком нарушении.

6.4.3. Не использовать ключ ЭП при наличии оснований, полагать, что конфиденциальность данного ключа нарушена.

6.4.4. Контролировать срок действия ЭП и заблаговременно предпринимать меры по своевременной замене ЭП.

6.4.5. Руководитель структурного подразделения, сотрудники которого наделены правом использования ЭП, при увольнении данного сотрудника, изменения его обязанностей, своевременно уведомляет администратора ИС о прекращении действия ЭП данного сотрудника.

6.4.6. Администратор ИС делает заявку в удостоверяющий центр, выдавший сертификаты ключей проверки ЭП, о прекращении действия электронного сертификата сотрудника ИС.

7. Ответственность пользователей ИС

7.1. Все пользователи ИС, получившие доступ к ИС, несут ответственность за предотвращение угроз, приводящих к нарушению конфиденциальности ПДн (копированию, или несанкционированному распространению), искажению, уничтожению, блокированию информации.

7.2. Нарушение правил доступа в ИС, порядка сбора, хранения, использования или распространения служебной информации, повлекшее уничтожение, блокирование, модификацию, копирование, распространение охраняемой законом информации, влечет административную или уголовную ответственность в соответствии с действующим законодательством.

Начальник управления информатизации и информационной безопасности

Н.Н.Сергиевская



ПРИЛОЖЕНИЕ

к Правилам доступа и работы в информационных системах в администрации муниципального образования Северский район

ЗАЯВКА
на предоставление доступа к информационной системе

Дата заполнения « » 202_ год

Для выполнения должностных обязанностей прошу предоставить доступ к автоматизированной (информационной) системе следующему (им) сотруднику (ам):

№п/п	Должность	ФИО	Роль(права)

Начальник / Подпись ФИО
Наименование структурного подразделения

СОГЛАСОВАНО:

Запрашиваемый доступ к ИС сотрудников соответствует их должностным обязанностям и отвечает принципу минимизации необходимых прав.

Сотрудник управления кадровой политики / Подпись ФИО

ОТМЕТКА ОБ ИСПОЛНЕНИИ ЗАЯВКИ АДМИНИСТРАТОРОМ ИС О ПРЕДОСТАВЛЕНИИ ДОСТУПА:

Заявка получена « » 202_ год

Заявка выполнена « » 202_ год

В доступе отказано
указывается причина отказа предоставления доступа

Примечания:

1. Если заявка занимает более одной страницы, она распечатывается с двух сторон листа.
2. В заявке на доступ указываются исчерпывающие права пользователя ИС.
3. Последующая заявка на доступ к ИС отменяет предыдущую заявку.

Начальник управления информатизации и информационной безопасности

Н.Н.Сергиевская

