АДМИНИСТРАЦИЯ МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ ПАВЛОВСКИЙ РАЙОН

ПОСТАНОВЛЕНИЕ

от 13.06.2017 № 730

ст-ца Павловская

Об утверждении правил доступа и работы в информационных системах

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", постановления 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" п о с т а н о в л я ю:

1. Утвердить Правила доступа и работы в информационных системах в подразделениях администрации муниципального образования Павловский район (приложение).

2. Отделу кадров управления правового обеспечения и муниципальной службы администрации муниципального образования Павловский район (Мохно) ознакомить под роспись сотрудников администрации и её структурных подразделений с настоящими правилами.

3. Контроль за выполнением данного постановления возложить на первого заместителя главы муниципального образования Павловский район Ю.Ю. Шулико.

4. Постановление вступает в силу с даты его подписания.

Глава муниципального образования
Павловский район В.В. Трифонов

ПРИЛОЖЕНИЕ
к постановлению администрации
муниципального образования
Павловский район
от 13.06.2017 № 730

Правила
доступа и работы в информационных системах в подразделениях
администрации муниципального образования Павловский район

1. Общие положение

Настоящие правила определяют порядок предоставления доступа сотрудникам подразделений администрации муниципального образования Павловский район (далее – администрация) к локальным и государственным информационным системам и основные организационные правила работы в них. Выполнение данных правил нацелено не предотвращение угроз 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;

идентификация 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 (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 электронной подписи владельцу электронной подписи;

владелец электронной подписи – сотрудник администрации, наделенный правом использования собственной ЭП при обмене информацией от имени администрации (или подразделения администрации) с другой огранизацией – участником электронного взаимодействия.

3. Жизненный цикл информационных систем

Любая информационная система проходит 3 этапа жизнедеятельности:

- ввод в эксплуатацию ИС;
- эксплуатация ИС;
- вывод ИС из эксплуатации.

3.1. 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 размещаться только достоверная 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 электроной подписи (если это предусмотрено возможностями конкретной ИС).

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

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

3.3. 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 (Диск CD-R или DVD-R) архивной информации;
- место хранения данного носителя;
- срок хранения данной архивной информации;
- сотрудника или подразделение, ответственных за хранение данного носителя;
- порядок уничтожения информации (носителя) по истечению срока хранения.

4. Предоставление и прекращение доступа к ИС

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

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

При наличии в ИС возможности разграничения прав доступа (ролей) начальник подразделения распределяет роли сотрудников в ИС согласно должностных обязанностей сотрудников.

Право доступа (роль) сотрудника определяется по принципу минимальной необходимости: сотрудник должен обладать правом, позволяющим ему полноценно исполнять свои должностные обязанности, но не должен иметь права доступа к информации, выходящей за их пределы.

Доступ сотруднику предоставляется посредством создания для него в ИС личной учетной записи. Учетная запись пользователя состоит из двух параметров: имени и пароля пользователя (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 позволяет определять авторство каждому действию с информаций, совершаемому в ИС.

Пароль придумывает и хранит непосредственно сам пользователь.

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

Доступ предоставляется на основании заявки руководителя подразделения (форма приведена в приложении №1), направленной администратору ИС,

с отметкой сотрудника кадровой службы о наличии данных обязанностей у сотрудника.

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

5. Работа с электронной подписью

5.1. Назначение лиц, наделяемых правом владения и использования собственной электронной подписи в электронном взаимодействии от имени администрации, производится на основании распоряжения главы муниципального образования Павловский район.

5.2. Назначение лиц, наделяемых правом владения и использования собственной электронной подписи в электронном взаимодействии от имени подразделения администрации, являющегося самостоятельным юридическим лицом, производится на основании распоряжения руководителя данного подразеделния администрации.

5.3. В распоряжении о назначении ответственных лиц, наделенных правом электронной подписи при электронном взаимодействии в целях признания юридической силы электронных документов указывается: полное наименование информационной системы; права (роль) данного сотрудника в данной ИС; название отчетной формы, на подписание которой сотруднику предоставляется право подписи.

6. Обязанности сотрудников

6.1. Обязанности пользователей.

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

Пароль к собственному учетному имени придумывает и хранит непосредственно пользователь ИС. Пароль должен быть достаточно сложным для предотвращения подбора случайным образом. При составлении паролей рекомендуется придерживаться следующих правил:

- пароль должен содержать не менее шести символов;
- в состав пароля могут входить цифры, латинские буквы, пробелы и специальные символы («.», «,», «?», «!», «<», «>». «-» и др.);
- рекомендуется составлять пароль из смешанного набора цифровых и буквенных (прописных и строчных) символов.

Все действия, выполненные в системе под учетной записью пользователя, считаются совершенными самим пользователем. Пользователь 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, (т.е. утраты его секретности) пользователь обязан проинформировать о данном факте начальника подразделения и обратиться к администратору ИС для его изменения или блокирования учетной записи.

6.2. Обязанности руководителя подразделения.

Руководитель подразделения путем назначения 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 подразделения, исполнения работы в ИС. Начальник подразделения контролирует и пресекает факты передачи учетной записи одного пользователя другому.

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

6.3. Обязанности администратора информационной системы.

Администратор информационной системы обязан своевременно, в течении 1 рабочего дня, выполнять заявки начальников подразделений администрации на предоставление доступа или прекращение доступа к ИС.

При необходимости проведения служебного расследования предоставлять руководителю протокол совершенных действий, имеющийся в информационной системе.

Периодически получать информацию из отдела кадров об уволенных и переведенных сотрудниках, на основании которой проводить аудит работы данных пользователей в ИС. О выявленных фактах использования логина уволенного сотрудника докладывать заместителю главы, курирующему данное направление.

6.4. Обязанности сотрудников, наделенных правом использования электронной подписи.

Владельцы электронных подписей обязаны:

- обеспечивать конфиденциальность ключей электронных подписей, в частности не допускать использование принадлежащих им ключей электронных подписей без их согласия;

- уведомлять удостоверяющий центр, выдавший сертификат ключа проверки электронной подписи, и иных участников электронного взаимодействия о нарушении конфиденциальности ключа электронной подписи в течение не более чем одного рабочего дня со дня получения информации о таком нарушении;

- не использовать ключ электронной подписи при наличии оснований полагать, что конфиденциальность данного ключа нарушена;

- контролировать срок действия ЭП и заблаговременно предпринимать меры по своевременной замене ЭП;

- руководитель подразделения, сотрудники которого наделены правом использования ЭП, при увольнении данного сотрудника, изменении его обязанностей, своевременно направляет Заявление о прекращении действия ЭП

данного сотрудника в удостоверяющий центр, выдавший сертификаты ключей проверки электронных подписей.

7. Ответственность сотрудников

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

Нарушение правил доступа в информационные системы, 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 отдела информатизации
управления организационной работы
администрации муниципального образования
Павловский район Т.Н. Аула

ПРИЛОЖЕНИЕ
к Правилам доступа и работы в
информационных системах

Заявка
на предоставление доступа к АС (ИС)_____

Дата заполнения "___" _____ 20___ г.

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

№ п/п	Должность	ФИО	Роль (права)

Начальник _____ _____/_____
наименование подразделения Подпись (Ф.И.О.)

«Согласовано»

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

_____ _____ / _____
сотрудник отдела кадров подпись Ф.И.О.

Отметка об исполнении заявки администратором доступа к АС:

Заявка получена «___» _____ 20__ г. _____ / _____

Выполнена «___» _____ 20___ г. _____/ _____
Ф.И.О. Подпись

Примечания:
1. Если заявка занимает более одной страницы, она распечатывается с двух сторон листа.
2. В заявке на доступ указываются исчерпывающие права пользователя; последующая заявка на АС отменяет предыдущую заявку.

Начальник отдела информатизации
управления организационной работы
администрации муниципального образования
Павловский район Т.Н. Аула