Приложение № 4

УТВЕРЖДЕНО
распоряжением
администрации
от 23.04.2021 № 82

ПОЛОЖЕНИЕ

о разрешительной системе доступа к персональным данным, обрабатываемым в информационных системах персональных данных администрации муниципального образования «Бугровское сельское поселение» Всеволожского муниципального района Ленинградской области

1. Общие положения

Настоящее Положение о разрешительной системе доступа разработано на основании нормативно-методических документов ФСТЭК России и определяет порядок и правила доступа сотрудников администрации муниципального образования «Бугровское сельское поселение» Всеволожского муниципального района Ленинградской области к информационным ресурсам информационной системы персональных данных (ИСПДн) администрации муниципального образования «Бугровское сельское поселение» Всеволожского муниципального района Ленинградской области (далее – Администрация).

Доступ сотрудников к информационным ресурсам ИСПДн предоставляется на основании распоряжения администрации.

К работе в ИСПДн допускаются сотрудники, ознакомившиеся с настоящим Положением, Положением об обеспечении безопасности персональных данных в администрации, Политикой администрации в отношении обработки персональных данных, в порядке, установленном Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», Перечнем персональных данных, обрабатываемых в администрации.

Сотрудники, допущенные к работе с персональными данными, несут дисциплинарную, гражданско-правовую, административную и уголовную ответственность в соответствии с требованиями законодательных, правовых актов, нормативно-распорядительных документов Российской Федерации и Администрации.

Логический алгоритм и положение о разрешительные системы доступа пользователей к ИСПДн распространяется на все информационные системы Администрации.

2. Разграничение доступа к информации в ИСПДн

Разграничение доступа к информации основывается на должностных обязанностях сотрудников, осуществляющих обработку такой информации, с учетом требований, предъявляемых к её защите.

К техническим средствам, обеспечивающим разграничение доступа, относятся программные и аппаратно-программные средства защиты информации.

Предоставление, изменение или ограничение доступа к информации осуществляется путем создания и удаления учетных записей пользователей, управления полномочиями учетных записей пользователей и поддержания правил разграничения доступа к информации.

Разграничение доступа к информационной системе осуществляется администратором ИСПДн с учетом требований к ее защите.

Учетная запись нового сотрудника (пользователя) с соответствующими правами доступа создается администратором ИСПДн по представлению начальника структурного подразделения сотрудника, заверенного курирующим данную область заместителем главы администрации.

Контроль доступа сотрудников (пользователей) структурных подразделений администрации к информационным ресурсам ИСПДн и обеспечение информационной безопасности при работе с информационными ресурсами ИСПДн возлагается на Администратора ИСПДн.

3. Правила и процедуры идентификации и аутентификации пользователей

Процедура идентификации и аутентификации пользователя обеспечивается с применением соответствующих средств защиты информации. Все процессы по получению доступа к системе регламентируются эксплуатационной и технической документацией на эти средства.

Имя учетной записи (идентификатор) выдается пользователю системы администратором автоматизированной информационной системой (далее - ИСПДн) и используется пользователям для входа в систему.

Администратор ИСПДн выполняет функции по управлению идентификаторами в ИСПДн (в том числе создание, присвоение, уничтожение идентификаторов), а также ответственный за хранение, выдачу, инициализацию, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации. Администратор ИСПДн формирует идентификатор пользователя ИСПДн по определенному формату имени и выдает идентификатор пользователю. При увольнении сотрудника администратором ИСПДн выполняется блокировка идентификатора пользователя. Блокировка идентификатора может выполнятся с использованием функций средств защиты информации.

Администратор ИСПДн выполняет изменение аутентификационной информации (средств аутентификации), заданных их производителями и (или) используемых при внедрении системы защиты информации информационной системы, генерирует начальную аутентификационную информацию и выдает средства аутентификации пользователям.

Администратором ИСПДн устанавливаются требуемые характеристики пароля для учетных записей пользователей ИСПДн:

- длина пароля должна быть не менее 8-ми буквенно-цифровых символов;

- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, дни рождения и другие памятные даты, номера телефонов, автомобилей, адреса места жительства, наименования автоматизированной системы, общепринятые сокращения, и другие данные, которые могут быть подобраны злоумышленником путем анализа информации об ответственном исполнителе;

- не использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;

- не использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре;

- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;

- в числе символов пароля, обязательно должны присутствовать буквы в верхнем и нижнем регистрах, а также цифры;

- не использовать ранее использованные пароли.

Требуемые характеристики пароля задаются в параметрах средств защиты информации выполняющие процедуры по идентификации и аутентификации пользователей.

При возникновении нештатных ситуаций при работе с учетными данными, подозрений на компрометацию учетных данных пользователь немедленно сообщает об этом ответственному за обеспечение безопасности информации и следует его инструкциям.

При организации парольной защиты запрещается:

- сообщать устно или письменно другим лицам личные имена учётных записей и пароли к ним;

- осуществлять ввод паролей, допуская возможность ознакомления с ними посторонних лиц;

- хранить пароли на любых носителях (как бумажных, так и электронных);

- производить подбор пароля других пользователей.

4. Правила и процедуры управления установкой (инсталляцией) компонентов программного обеспечения

Установка (инсталляция) ПО выполняется только администраторами информационных систем персональных данных (далее - администратор ИСПДн).

Установка ПО должна включать только компоненты устанавливаемого ПО, необходимые для реализации целей использования данного ПО.

Компоненты ПО, необходимые для обеспечения выполнения задач ИСПДн, определяются до момента установки ПО на основании эксплуатационной документации на данное ПО.

Компоненты, не относящиеся к функционалу устанавливаемого ПО, должны быть отменены в процессе настройки параметров установки.

После установки ПО, администратор ИСПДн выполняет проверку правильности установки ПО (состав компонентов, параметры установки, конфигурация компонентов). В случае обнаружения несоответствия параметров компонентов ПО определенному до момента установки, администратор в ИСПДн проводит корректировку параметров (состав компонентов, параметры установки, конфигурация компонентов).

Установка обновлений проводится администраторами ИСПДн. При контроле установки обновлений осуществляются проверки соответствия версий общесистемного, прикладного и специального программного (микропрограммного) обеспечения, включая программное обеспечение средств защиты информации, установленного в информационной системе и выпущенного разработчиком, а также наличие отметок в эксплуатационной документации (формуляр или паспорт) об установке (применении) обновлений. Периодичность проведения контроля установки обновлений устанавливается администраторами в ИСПДн с учетом особенностей функционирования ИСПДн и требований по периодичности, устанавливаемых в рамках сопровождения ИСПДн.