АДМИНИСТРАЦИЯ

ГОРОДСКОГО ОКРУГА МЫТИЩИ

МОСКОВСКОЙ ОБЛАСТИ

РАСПОРЯЖЕНИЕ

11.04.2024 № 79-р

Об утверждении Регламента управления

учетными записями в едином каталоге пользователей

Администрации городского округа Мытищи

В целях обеспечения безопасности информации в государственных информационных системах в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации, руководствуясь Уставом городского округа Мытищи Московской области:

1. Утвердить Регламент управления учетными записями в едином каталоге пользователей Администрации городского округа Мытищи (далее - Регламент) (прилагается).
2. Администрации городского округа Мытищи Московской области руководствоваться Регламентом при создании, изменении и блокировке учетных записей в едином каталоге пользователей.
3. Настоящее распоряжение подлежит размещению на официальном сайте органов местного самоуправления городского округа Мытищи.
4. Контроль за выполнением настоящего распоряжения возложить на первого заместителя Главы городского округа Мытищи Л.С. Иванову.

И.о. Главы городского округа Мытищи О.А. Сотник

|  |  |
| --- | --- |
|  | УТВЕРЖДЕН  распоряжением Администрации городского округа Мытищи  от 11.04.2024 г № 79-р |

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

РЕГЛАМЕНТ

УПРАВЛЕНИЯ УЧЕТНЫМИ ЗАПИСЯМИ В ЕДИНОМ КАТАЛОГЕ

ПОЛЬЗОВАТЕЛЕЙ АДМИНИСТРАЦИИ ГОРОДСКОГО ОКРУГА МЫТИЩИ МОСКОВСКОЙ ОБЛАСТИ

Администрация городского округа Мытищи Московской области

РЕГЛАМЕНТ

УПРАВЛЕНИЯ УЧЕТНЫМИ ЗАПИСЯМИ В ЕДИНОМ КАТАЛОГЕ

ПОЛЬЗОВАТЕЛЕЙ АДМИНИСТРАЦИИ ГОРОДСКОГО ОКРУГА МЫТИЩИ МОСКОВСКОЙ ОБЛАСТИ

ПЕРЕЧЕНЬ

ИСПОЛЬЗУЕМЫХ СОКРАЩЕНИЙ

|  |  |
| --- | --- |
| ЕИТО АГОМ | Единственная инфраструктура технологического обеспечения Администрации городского округа Мытищи |
| ЕКП | Единый каталог пользователей Администрации городского округа Мытищи |
| ЕСЭП | Единая система электронной почты Администрации городского округа Мытищи |
| ЛВС | Локальная вычислительная сеть |
| МСЭД | Межведомственная система электронного документооборота |
| НСД | Несанкционированный доступ |
| ОМСУ | Орган местного самоуправления |
| АГОМ | Администрация городского округа Мытищи |
| СТП | Служба технической поддержки (Отдел информационных технологий и связи) |
| УЗ | Учетная запись |
| VPN | Доступ к ЛВС с использованием технологии виртуальной частной сети |

ПЕРЕЧЕНЬ

ИСПОЛЬЗУЕМЫХ ОПРЕДЕЛЕНИЙ

|  |  |
| --- | --- |
| Контактное лицо | Сотрудник организации, с которым СТП оператора осуществляет взаимодействие по вопросам управления учетными записями ЕКП |
| Объект | Структурная единица ЕКП (учетная запись компьютера, группа, контакт, организационная единица, групповая политика) |
| Организация | Орган местного самоуправления и другая организация |
| Пользователь | Сотрудник, для которого требуется Управление учетной записью ЕКП |
| Уполномоченное лицо | Сотрудник ОМСУ и подведомственного учреждения, уполномоченный на внесение изменений в ЕКП. |
| Управление учетной записью | Создание, изменение или блокировка учетной записи ЕКП |
| Учетные данные | Логин и пароль учетной записи ЕКП |
| Оператор | АГОМ |

1. Общие положения

1.1. Настоящий регламент управления учетными записями в едином каталоге пользователей Администрации городского округа Мытищи Московской области (далее - Регламент) разработан на основании Федерального [закона](https://login.consultant.ru/link/?req=doc&base=LAW&n=464157&date=25.03.2024) от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" и [политики](https://login.consultant.ru/link/?req=doc&base=MOB&n=235177&date=25.03.2024&dst=100011&field=134) парольной защиты информационных систем центральных исполнительных органов государственной власти Московской области и государственных органов Московской области, утвержденной распоряжением Министерства государственного управления, информационных технологий и связи Московской области от 1 декабря 2015 г. N 10-33/РВ.

1.2. Регламент определяет порядок управления учетными записями ЕКП.

1.2.1. Регламент распространяется в форме электронного документа, размещенного на сайте оператора в сети Интернет (www.mytyshi.ru).

1.2.2 ОМСУ и другие организации, присоединившиеся к Регламенту, соглашаются с ним и принимают дальнейшие изменения (дополнения), вносимые в Регламент, в соответствии с условиями Регламента.

1.3. Положения Регламента должны учитываться при организации доступа сотрудников ОМСУ и других организаций к ЕКП в части управления учетными записями, блокировки учетных записей, включая вопросы генерации и распределения парольной информации указанных учетных записей, а также порядка работы с объектами ЕКП.

1.4. В ЕКП для сотрудников существует три вида учетных записей, отличающихся функциональными возможностями:

1.4.1. Учетная запись пользователя позволяет пользователю проходить проверку подлинности (аутентификация и авторизация) на устройствах домена mytyshi.ru и получать доступ к различным ресурсам и сервисам ЕИТО АГОМ.

1.4.2. Учетная запись пользователя ЕСЭП - наличие у пользователя помимо полномочий, указанных в [п. 1.4.1](#Par94) (при необходимости [п. 1.4.2](#Par95)), почтового ящика в ЕСЭП АГОМ.

1.5. Контроль за соблюдением требований Регламента осуществляет оператор.

2. Порядок управления и распределения учетных записей ЕКП

сотрудников ОМСУ, подведомственных

и подрядных им организаций

2.1. Управление учетными записями и объектами ЕКП ОМСУ, подведомственных и подрядных им организаций выполняется уполномоченными лицами этих организаций. С целью организации контроля и обоснованности внесения изменений в ЕКП ОМСУ необходимо определить (назначить внутренним нормативным правовым актом) в организации уполномоченных лиц, список которых необходимо предоставить в адрес оператора посредством МСЭД.

2.2. Уполномоченные лица ОМСУ осуществляют Управление учетными записями и объектами ЕКП своего ведомства.

2.3. Если для управления учетными записями сотрудников ОМСУ, подведомственных и подрядных им организаций в ЕКП требуется привлечение оператора, то соответствующие запросы оператор обрабатывает на основании одного из следующих документов:

2.3.1. Служебной записки, направленной уполномоченным лицом ведомства на адрес электронной почты itsupport@mytyshi.ru с приложением заполненного шаблона (приложение 1) и обоснованием необходимости, в теме письма указать "Учетная запись ЕКП".

2.3.2. Письма, направленного в адрес оператора через МСЭД, за подписью руководителя или заместителя руководителя ведомства с приложением заполненного шаблона (приложение 1) и обоснованием необходимости, в кратком содержании указать "Учетная запись ЕКП".

2.4. Обработка запросов на управление учетными записями и объектами ЕКП АГОМ оператором возможна не ранее чем через один рабочий день с момента получения списка уполномоченных лиц АГОМ либо изменений в данном списке.

2.5. Оператор в течение одного рабочего дня регистрирует поступивший запрос, рассматривает его и исполняет, либо отклоняет запрос.

2.6. Причинами для отклонения запроса на управление учетной записью ЕКП могут быть:

2.6.1. Поступление запроса от сотрудника, не являющегося уполномоченным лицом ведомства.

2.6.2. Отсутствие обоснования потребностей в управлении учетной записью ЕКП или некорректное заполнение шаблона на управление учетной записью ЕКП.

2.7. После выполнения запроса оператор направляет уполномоченному лицу на электронную почту уведомление о результатах выполнения запроса.

2.8. Учетные данные передаются уполномоченному лицу способом, исключающим получение к ним несанкционированного доступа.

2.9. Уполномоченное лицо, ответственное за управление учетными записями ЕКП в ведомстве, обеспечивает доведение учетных данных до пользователя способом, исключающим получение к ним несанкционированного доступа.

2.10. Учетная запись является персональной независимо от ее вида, создается для определенного пользователя и не может быть передана иным лицам. Совместное использование персональных учетных записей не допускается.

3. Порядок управления и распределения учетных записей ЕКП

сотрудников АГОМ и других организаций

3.1. Оператор обрабатывает заявки по управлению учетными записями сотрудников организации в ЕКП на основании письменного запроса, направленного в адрес оператора через МСЭД с обоснованием необходимости в создании, изменении или блокировке учетных записей ЕКП. Письмо должно быть подписано квалифицированной электронной подписью руководителя или заместителя руководителя организации, к нему должен быть приложен заполненный шаблон (приложение 1). В письме необходимо указать номер рабочего телефона и адрес электронной почты контактного лица, в кратком содержании указать "Учетная запись ЕКП".

3.2. Оператор в течение трех рабочих дней регистрирует поступивший запрос, рассматривает его и исполняет либо отклоняет.

3.3. Причинами для отклонения запроса на управление учетной записью ЕКП могут быть:

3.3.1. Отсутствие или некорректное заполнение шаблона на управление учетной записью ЕКП.

3.3.2. Отсутствие обоснования потребностей в управлении учетной записью ЕКП.

3.3.3. Несоответствие запроса требованиям, указанным в [п. 3.1](#Par121) Регламента.

3.4. После выполнения запроса оператор направляет контактному лицу на электронную почту уведомление о результатах запроса.

3.5. Учетные данные передаются контактному лицу способом, исключающим получение к ним несанкционированного доступа.

3.6. Контактное лицо обеспечивает доведение учетных данных до пользователя способом, исключающим получение к ним несанкционированного доступа.

4. Порядок блокирования учетных записей ЕКП

4.1. Решение о необходимости блокирования учетных записей ЕКП принимается уполномоченным лицом, руководителями (заместителями руководителей) ОМСУ и других организаций городского округа Мытищи либо оператором.

4.2. Уполномоченное лицо, руководитель (заместитель руководителя) ОМСУ и других организаций Московской области в течение одного рабочего дня с момента наступления любого из событий, указанных в [п. 4.3.1](#Par136), [4.3.2](#Par137), обязаны направить оператору заявку о необходимости блокирования учетной записи ЕКП в соответствии с порядком, указанным в [п. 2.3](#Par105) и [3.1](#Par121) соответственно.

4.3. Заявка о необходимости блокирования учетной записи ЕКП подается в случае:

4.3.1. Наличия любых сведений о компрометации паролей либо о факте передачи парольной информации соответствующей учетной записи третьими лицами.

4.3.2. Прекращения (полного либо временного) полномочий пользователя соответствующей учетной записи, в том числе его увольнения.

Заявка оператору должна содержать необходимую информация для блокировки учетной записи, в комментарии к заявке указать "Блокировка учетной записи ЕКП".

4.4. Блокирование учетной записи ЕКП может осуществляться оператором в случае:

4.4.1. Наличия у оператора любых сведений о компрометации паролей либо о факте передачи парольной информации соответствующей учетной записи третьим лицам.

4.4.2. Наличия у оператора информации о попытках НСД со стороны пользователя соответствующей учетной записи ЕКП к ресурсам, доступ к которым для данного пользователя запрещен.

4.4.3. Наличия у оператора информации о том, что авторизация под учетными данными в ЕКП выполнялась 3 месяца назад и более.

4.4.4. Если учетная запись не соответствует требованиям, указанным в [п. 6.5](#Par210) Регламента.

4.5. После блокирования учетной записи ЕКП в случаях, указанных в [п. 4.4](#Par139), СТП оператора в течение одного рабочего дня уведомляет уполномоченное лицо, контактное лицо или руководителя организации путем направления информации по электронной почте либо через МСЭД о блокировке с указанием причины блокирования учетной записи ЕКП.

4.6. Не допускается передача учетных записей ЕКП и связанной с ними парольной информации после их блокирования третьими лицами за исключением случаев, когда это необходимо для проведения служебных проверок и расследования инцидентов информационной безопасности с использованием учетной записи ЕКП.

4.7. Блокировка УЗ осуществляется при увольнении сотрудника с обязательным уведомлением оператора отделом (службы) кадров в письменном виде через МСЭД

5. Требования к паролям учетных записей ЕКП,

их генерации, использованию, хранению и смене

5.1. Требования к паролям.

5.1.1. Минимальная длина пароля должна быть не менее восьми цифр (или переходим на символы?).

5.1.3. Пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии и другие), а также общепринятые сокращения и любые другие данные, которые можно определить исходя из информации о пользователе (даты рождения родственников, клички домашних животных и подобные).

5.1.4. Пароль не должен включать в себя последовательности из более чем 3 символов, расположенных рядом на клавиатуре (например, 1234, gwer и другие).

5.1.5. Пароль не должен состоять из одного и того же повторяющегося символа либо повторяющейся комбинации из нескольких символов (например, 222999, psqpsq).

5.1.6. При смене пароля новое значение должно отличаться от предыдущего не менее чем на 3 символа (если такое позволяет AD).

5.1.7. При смене пароля новое значение не должно совпадать с 5 предыдущими значениями паролей данного пользователя (если такое позволяет AD).

5.2. Порядок генерации паролей.

5.2.1. Генерация паролей осуществляется при создании учетной записи ЕКП либо при необходимости плановой или внеплановой смены пароля.

5.2.2. Генерация пароля при создании учетной записи осуществляется на основании запроса уполномоченного лица или организации о необходимости управления учетной записью ЕКП, направленного оператору в соответствии с [п. 2.3](#Par105), [3.1](#Par121) Регламента.

5.3. Правила использования паролей.

5.3.1. При использовании паролей пользователь обязан соблюдать положения должностных инструкций, методических документов по информационной безопасности, а также требования Регламента.

5.3.2. Ввод пароля должен осуществляться с учетом регистра, в котором пароль был задан.

5.3.3. При вводе паролей необходимо исключить возможность его просмотра посторонними лицами или техническими средствами (фото-, видеокамеры и другие средства).

5.3.4. Пользователь не имеет права сообщать личный пароль другим сотрудникам и допускать их к работе под своей учетной записью в ЕКП.

5.3.5. При утере, компрометации, несанкционированном изменении пароля пользователь обязан немедленно сообщить о данном факте Уполномоченному лицу либо оператору, после чего дальнейшее использование соответствующей учетной записи не допускается до смены пароля и передачи учетных данных пользователю в порядке, описанном [п. 2.8](#Par114) и [3.5](#Par128) Регламента.

5.4. Правила хранения паролей.

5.4.1. При хранении пароля пользователем должны быть приняты все возможные меры по минимизации возможности компрометации либо утери пароля.

5.4.2. Запрещается записывать пароли в файлах, электронных записных книжках, других электронных носителях информации.

5.4.3. Запрещается сообщать пароль каким-либо образом третьим лицам.

5.5. Смена пароля осуществляется самостоятельно владельцем УЗ по всем требованиям п.5 Регламента

6. Порядок работы с учетными записями и объектами в ЕКП

6.1. Данный порядок определяет принципы работы с учетными записями и объектами ЕКП для сотрудников СТП оператора и уполномоченных лиц, ответственных за управление учетными записями ЕКП в организационной единице ЦИОГВ и ГО.

6.2. ЕКП представляет собой иерархическую структуру, в корне которой находятся следующие организационные единицы:

6.2.1. Computers (в данной организационной единице находятся учетные записи компьютеров, которые помещаются в нее по умолчанию при вводе компьютера в домен dp.mosreg.ru).

6.2.2. Users (в данной организационной единице находятся системные группы безопасности (security groups) и распространения (distribution groups).

Добавление объектов, не относящихся к данной категории, в указанную организационную единицу запрещено.

6.2.3. Органы местного самоуправления (в данной организационной единице находятся объекты городского округа).

6.2.4. Подведомственные организации (в данной организационной единице находятся объекты различных муниципальных учреждений, являющихся подведомственными ОМСУ организациями).

6.2.5. Подрядные организации (в данной организационной единице находятся учетные записи представителей подрядных организаций, имеющих договорные отношения с АГОМ).

6.2.6. Служебное (в данной организационной единице находятся объекты, используемые для служебных нужд оператором mytyshi.ru).

6.3. Типовая иерархическая структура организации должна иметь вид, представленный на рисунке 1:

- Contacts (почтовые контакты);

- Groups (группы, включает в себя дочерние организационные единицы с группами безопасности и распространения);

- Servers (учетные записи серверов организации);

- Services (служебные учетные записи организации);

- Users (учетные записи пользователей, включает в себя дочерние организационные единицы структурных подразделений в соответствии с организационно-штатной структурной организации);

- Workstations (учетные записи компьютеров организации).

6.4. Наименования объектов ЕКП должны отвечать определенным правилам. Объектами регулирования правил являются:

- учетные записи пользователей;

- учетные записи серверов;

- учетные записи компьютеров;

- группы безопасности;

- адреса электронной почты.

Для наименования объектов используются:

- латинские символы;

- кириллические символы;

- цифры;

- дефис;

- специальные символы (при необходимости).

Латинские написания фамилий, инициалов, адресов электронной почты, названий организаций образуются с использованием правил транслитерации. Общая длина имени объекта не должна превышать 20 символов.

6.5. Именование учетных записей пользователей.

6.5.1. Имена учетных записей пользователей формируются на основе фамилии и других инициалов (имя и отчество) пользователя. Формат: фамилия (полностью), первая буква имени, первая буква отчества, без пробелов и иных символов.

6.5.2. В случае если логин уже существует, требуется добавлять к нему следующие по порядку буквы имени или отчества до достижения уникальности. К примеру, логин у сотрудника Салтинов Роман Анатольевич может иметь вид sаltinovra или sulral.

6.5.3. В случае если у пользователя отсутствует отчество, используется один имеющий инициал. В случае если пользователь имеет составную фамилию, имя или отчество, состоящее из двух и более слов, используется первое слово. Допускается произвольное сокращение фамилий, состоящих более чем из 10 символов.

6.5.4. Если инициал транслитерируется в более чем один латинский символ, то используется только первый латинский символ.

6.5.5. При заведении учетной записи пользователя необходимо в обязательном порядке заполнять следующие поля:

- имя;

- фамилия;

- выводимое имя;

- комната;

- номер рабочего телефона;

- адрес местонахождения организации (дом, улица, город, область, почтовый индекс, страна);

- должность;

- структурное подразделение;

- организация.

6.10. Именование адресов электронной почты.

Имена адресов электронной почты формируются по следующему принципу: <логин учетной записи пользователя>@<mytyshi.ru>. Использование адресов электронной почты, состоящих их первых букв фамилии, имени и отчества, запрещено. К примеру, адрес электронной почты у сотрудника Салтинов Роман Анатольевич может иметь вид sаltinovra @mytyshi.ru.

6.11. Для управления учетными записями и объектами ЕКП предусмотрена возможность делегирования оператором соответствующих полномочий уполномоченным лицам, право управления предоставляется на следующие категории:

- объекты службы каталогов, расположенные в разделе домена mytyshi.ru соответствующего ОМСУ;

- групповые политики, распространяющиеся на объекты, расположенные в разделе домена mytyshi.ru соответствующего ОМСУ;

- учетные записи компьютеров, расположенные в организационной единице Computers (в данной организационной единице находятся учетные записи компьютеров, которые помещаются в нее по умолчанию при вводе компьютера в домен mytyshi.ru);

- компьютеры (делегируются права локального администратора, данные права будут доступны только после того, как учетные записи компьютеров будут перенесены в организационную единицу Workstations ОМСУ);

- сервера (делегируются права локального администратора, данные права будут доступны только после того, как учетные записи серверов будут перенесены в организационную единицу Servers соответствующего ОМСУ).

6.12. Делегирование указанных полномочий осуществляется путем назначения необходимых прав на группу безопасности, включающего в себя учетные записи уполномоченных лиц ОМСУ. Именование группы безопасности формируется по следующему принципу: <сокращенное наименование организации кириллическими символами>-Admins.

7. Ответственность за выполнение требований Регламента

7.1. Участники информационного взаимодействия, указанные в Регламенте, несут ответственность за выполнение возложенных на них функций, в том числе за свои действия в ЕКП, в соответствии с законодательством Российской Федерации.

|  |  |  |
| --- | --- | --- |
| **Приложение №1**  **Данные сотрудника**  (пользователя сетевой инфраструктуры Администрации городского округа Мытищи) | | |
| Подразделение (Управление, отдел) | |  | | --- | |  | |  | |  | | |
| Ф.И.О. (полностью) | |  | | --- | |  | | |
| Должность | |  | | --- | |  | | |
| Номера | |  |  |  | | --- | --- | --- | |  |  |  | | корпус / кабинет | телефон | добавочный | | |
| Сгенерированный логин и пароль (старый) | |  |  | | --- | --- | |  |  | | логин | пароль | | |
| Технические характеристики ПК (описание) | |  |  |  | | --- | --- | --- | |  |  |  | | CPU | RAM | Инвентарный № | | |
| Имя ПК | |  | | --- | |  | | |
| Номера розеток | |  |  |  |  | | --- | --- | --- | --- | |  | Общая сеть □  Локальная сеть □ |  | Подключение □ | | сеть | | телефон | | | |
| Комплектность | |  |  |  |  | | --- | --- | --- | --- | | Монитор | ЖК □  ЭЛТ □ | Принтер | ЧБ □  ЦВ □ | | ИБП □ | | Колонки □ | | | |
| Примечание (смежные столы) | |  | | --- | |  | |  | | |
| Сгенерированный логин и пароль (новый) | |  |  | | --- | --- | |  |  | | логин | пароль | | |
| Логин и пароль пользователя должны оставаться личными и конфиденциальными. Передача или сообщение другому лицу закрепленного за пользователем логина и пароля строго запрещены. Любое нарушение этого запрета приведет к немедленному прекращению доступа к сетевой инфраструктуре Администрации, а также к возложению на пользователя ответственности за любой ущерб, причиненный таким нарушением. Ответственность за защиту пароля от неправомочного использования, а также за любые нарушения, повлекшие за собой незапланированные расходы, связанные с Вашим паролем, возлагается исключительно на Вас. | | С правилами ознакомлен,  логин и пароль получил  Подпись  Расшифровка |