

**КГУ «Управление архитектуры, градостроительства и земельных
отношений города Нур-Султан»**

УТВЕРЖДЕНО

**Директор ТОО
«АстанаГорАрхитектура» города
Нур-Султан**

_____ Кенжебеков Н. К.



« 19 » октября 2020 г.

УТВЕРЖДЕНО

**Руководитель Управления
архитектуры, градостроительства и
земельных отношений города
Нур-Султан**

_____ Уранхаев Н. Т.



« 19 » октября 2020 г.

**Правила организации процедуры аутентификации
Информационной системы «Геоинформационный портал
города Нур-Султан»
ГПГ.СМИБ.ПР.10.r02.20**

**г. Нур-Султан
2020 г.**

1. Область применения

Целью настоящего документа является описание правил организации процедуры аутентификации, и определение порядка действий ответственных сотрудников Организации, а также определение ответственности при проведении этих мероприятий или нарушении требований настоящего Документа.

Настоящий документ обязателен для исполнения в рамках проекта ИС.

2. Нормативные ссылки

Настоящий документ содержит указания к практическому исполнению требований, изложенных в нормативных документах согласно п. 3 Нормативные ссылки действующей Политики информационной безопасности.

3. Термины, определения и сокращения

В настоящем документе используются термины и сокращения, принятые в действующей Политике информационной безопасности.

4. Общие положения

Доступ к электронной почте предоставляется всем сотрудникам проекта ИС, на рабочем месте которых установлен персональный компьютер, подключенный к сети Интернет, согласно утверждённым политикам и процедурам ИБ.

Доступ к сети Интернет и службам Интернет-сообщений предоставляется по заявке, согласованной с СОИБ в порядке и по форме согласно утвержденной Политике информационной безопасности.

При этом обоснование доступа к сети Интернет должно содержать указание на необходимость постоянной оперативной работы.

5. Аутентификация

Регистрация пользователей

Функционал ИС обеспечивает:

- а) использование уникальных ID (идентификаторов или имен) пользователей, таким образом, чтобы действия в системе можно было бы соотнести с пользователями и установить ответственных;
- б) проверку того, что пользователь имеет авторизацию от владельца системы на использование информационной системы или сервисов;
- с) проверка того, что уровень предоставленного доступа соответствует производственной необходимости, а также учитывает требования политики безопасности ИС;
- д) предоставление пользователям письменного документа, в котором указаны их права доступа;

- е) требование того, чтобы пользователи подписывали документ о том, что они понимают условия предоставления доступа;
- ф) обеспечивает не предоставление доступа, пока процедура авторизации не завершена;
- г) ведение формализованного учета в отношении всех лиц, зарегистрированных для использования информации ИС;
- h) немедленную отмену прав доступа пользователей, у которых изменились должностные обязанности или уволившихся из организации;
- і) периодическую проверку и удаление избыточных пользовательских ID и учетных записей;
- ј) обеспечение того, что избыточные пользовательские учетные записи не были переданы другим пользователям.

Права пользователей объединены в роли и описаны в Матрице доступа.

При аутентификации применяются следующие меры обеспечения ИБ:

- а) идентифицировать привилегии доступа в отношении каждого системного продукта ИС: ОС, сервер приложений, средства защиты, СУБД;
- б) используемые привилегии ограничены только теми, которые необходимы пользователю для работы;
- с) привилегии не предоставляются до завершения процесса авторизации, учитываются и регистрируются в ИС;
- д) на усмотрение ответственного за обеспечение ИБ могут быть автоматизированы функции системного администратора при помощи мобильного кода, вместо предоставления дополнительных привилегий;
- е) на усмотрение ответственного за обеспечение ИБ могут быть автоматизированы функции системного администратора при помощи специальных утилит, вместо предоставления дополнительных привилегий;
- ф) следует использовать различные идентификаторы (ID) пользователей при работе в обычном режиме и с использованием привилегий.
- г) ИС должна вести электронный журнал регистрации пользователей.

Идентификация и аутентификация пользователя

Необходимо, чтобы все пользователи имели уникальный идентификатор (пользовательский ID) для их единоличного использования с тем, чтобы их действия могли быть проанализированы ответственным лицом.

Эти требования по мониторингу и контролю доступа в Интернет должны применяться для всех типов пользователей.

Идентификаторы пользователей должны быть использованы для отслеживания деятельности ответственного лица. Мероприятия с

пониженными привилегиями нельзя проводить с привилегированными учетными записями.

Для идентификации сотрудников в процессе подключения к серверам ИС, используются криптографические ключи.

Система управления паролями

Системы управления паролями в компонентах ИС и на рабочих станциях сотрудников проекта обеспечивают высокую надежность паролей и удовлетворяют утвержденные требования к политике паролей согласно Приложению 1.

Система управления паролями должна:

- а) предписывать использование индивидуальных паролей для обеспечения установления ответственности;
- б) позволять пользователям выбирать и изменять их собственные пароли, а также включать подтверждающую процедуру для учета ошибок ввода при необходимости;
- с) предписывать выбор высококачественных паролей в соответствии настоящим документом;
- д) принуждать их к изменению паролей;
- е) там, где пользователи выбирают пароли, обеспечивать изменение временных паролей при первой регистрации;
- ф) поддерживать хранение истории предыдущих пользовательских паролей (за предыдущий год) и предотвращать их повторное использование;
- г) не отображать пароли на экране при их вводе;
- h) хранить пароли отдельно от данных прикладных систем в зашифрованном виде;
- i) хранить и передавать пароли в зашифрованной форме.
- ж) в случаях, когда от пользователей требуется управление собственными паролями, обеспечивается предоставление безопасного первоначального временного пароля, который пользователя принуждают сменить при первой регистрации в ИС;
- к) обеспечение безопасного способа выдачи временных паролей пользователям нарочно в запечатанном конверте с подписанием акта передачи;
- л) подсистема аутентификации должна хранить только слепки-паролей или зашифровывать пароли методам не поддерживающими расшифровку, но однозначного определяющих зашифрованный пароль;
- м) временные пароли должны быть индивидуальными, не подвержены легкому угадыванию или повторению, иметь длину не менее 6 символов, состоять из латинских строчных и прописных букв, цифр и печатных символов (\$, #).

Управление паролями пользователей

Предоставление паролей определяется Правилами организации процедуры аутентификации.

Процесс управления паролями включает следующие требования:

- а) подписание пользователями документа о необходимости соблюдения полной конфиденциальности личных паролей;
- б) в случаях, когда от пользователей требуется управление собственными паролями, обеспечивается предоставление безопасного первоначального временного пароля, который пользователя принуждают сменить при первой регистрации в ИС;
- в) установить процедуры, чтобы проверить идентичность пользователя (ввода действующего пароля) до обеспечения нового, замены или временного пароля;
- г) обеспечение безопасного способа выдачи временных паролей пользователям нарочно в запечатанном конверте с подписанием акта передачи;
- д) временные пароли должны быть индивидуальными, не подвержены легкому угадыванию или повторению, иметь длину не менее 6 символов, состоять из латинских строчных и прописных букв, цифр и печатных символов (\$, #);
- е) пользователи подтверждают получение паролей, подписанием акта;
- ж) пароли хранятся в ИС в зашифрованном виде; пользователям запрещено записывать или сохранять пароли, а также включать пароли в автоматизированные процессы регистрации, например, с использованием хранимых макрокоманд или функциональных клавиш;
- з) заданные по умолчанию пароли поставщиков должны быть измененными после установки системы или программного обеспечения;
- и) принудительная смена паролей пользователей и сотрудников проекта каждые 30 дней;
- й) недопущение использования одних и тех же паролей.

В ИС, помимо паролей, возможно применение более надежной системы авторизации при помощи ЭЦП НУЦ РК в соответствии с требованиями законодательства РК.

В случае возникновения инцидента ИБ или подозрения ставящего под сомнение конфиденциальность аутентификационных данных учетной записи пользователя или компрометирующего, их пользователь или сотрудник проекта должен обратиться к администратору ИС или системному администратору проекта, соответственно, для немедленной блокировки учетной записи и изменению аутентификационных данных.

Администратор ИС и системный администратор проекта обязаны уведомлять ответственного за обеспечение ИБ о компрометации аутентификационных данных учетных записей или о подозрениях о возможности такого инцидента ИБ.

6. Аутентификация пользователей для внешних соединений

Аутентификация удаленного доступа к серверам для их обслуживания достигается путем использования средств криптографии с использованием виртуальной частной сети (VPN).

Аутентификация серверов ИС происходит по их уникальному IP-адресу.

Сотрудникам проекта запрещено автоматизировать ввод паролей, ключей и других идентификаторов при подключении к серверам ИС.

7. Ответственность

СОИБ несет ответственность за:

- a) контроль исполнения требований настоящего документа,
- b) исполнение настоящей Инструкции.

Сотрудники проекта ИС:

- a) исполнение настоящей Инструкции.

Пользователи ИС:

- a) исполнение настоящей Инструкции.

Требования к формированию пароля:

- пароль должен содержать не менее 8 символов;
- в пароле должны присутствовать прописные и заглавные буквенные символы, а также цифры и (или) специальные символы (#, \$, @ и др.);
- пароль не должен включать легко вычисляемые последовательности символов, такие как общепринятые сокращения (например, admin, system, user, sys, god, root, webadmin, adm, sysop, operator и т. п., включая их аналоги на казахской и русской раскладках клавиатуры), а также личные и иные общедоступные сведения (например, даты, имена, названия);
- пароль не должен включать группы символов, последовательность расположения которых на клавиатуре легко вычисляется (например, 1234, qWerty, qwerty123, 321369, 123456, !Q@W#E\$R%T^Y и т. п., включая их аналоги на казахской и русской раскладках клавиатуры);
- при смене пароля новое значение должно отличаться от предыдущего не менее, чем в 4 позициях.