ПРАВИЛА
ОРГАНИЗАЦИИ ПРОЦЕДУРЫ АУТЕНТИФИКАЦИИ ДЛЯ СОТРУДНИКОВ ОТДЕЛА ИТ

Астана

2023 г.

1. Термины и сокращения

В данных Правилах используются следующие основные понятия и термины:

Системный администратор – лицо, представляющее услуги системного администрирования и технической поддержки ИС.

В целях идентификации, аутентификации и соблюдения принципа персональной ответственности за свои действия, системным администратором ИС, пользователю должны быть присвоены персональные уникальные имена (учетная запись) с паролями.

Организационное и техническое обеспечение процессов использования, смены и прекращения действия паролей пользователей возлагается на системного администратора ИС.

Информационные ресурсы – электронная систематизированная информация (база данных), содержащаяся в информационных системах, объединенная соответствующим программным обеспечением;

Компрометация пароля – утечка или разглашение пароля;

Пользователь ИС – субъект, обращающийся к ИС за получением необходимых ему электронных информационных ресурсов, требующих авторизации;

Организация – ОЮЛ Ассоциация ВИЭ “Qazaq Green”

2. Общие положения

В целях идентификации, аутентификации и соблюдения принципа персональной ответственности за свои действия, системного администратору и пользователям ИС должны быть присвоены персональные уникальные имена (учетная запись) с паролями.

Контроль над действиями пользователей, системного администратора ИС и работников при работе с паролями возлагается на специалиста по информационной безопасности, отвечающего за сопровождение ИС.

При приеме на работу нового системного администратора, специалист по информационной безопасности должен ознакомить системного администратора с нормативной документацией, связанной с функционированием и в области информационной безопасности ИС и осуществить передачу паролей для администрирования ИС (путем передачи информации о логинах и паролях в закрытом конверте). Системный администратор после получения вышеуказанной информации должен незамедлительно произвести смену паролей в соответствии с данными

Правилами, после чего передать новые пароли специалисту по информационной безопасности. Специалист по информационной безопасности информацию о новых логинах и паролях оформляет в закрытый конверт. Факты осуществления передачи паролей пользователей корпоративной сети должны фиксироваться в специально заведенном журнале согласно Приложению 1 к настоящим Правилам. Факты выдачи, смены паролей пользователей в соответствии с ролями ИС учитываются в электронном журнале выдача паролей ИС. Электронный журнал выдачи паролей должен содержать следующие поля: порядковый номер; кем выдан пароль, проводимая операция, дата и время проведения операции.

Удаление учетных записей пользователей, уволенных, переведенных в другое структурное подразделение, филиал, региональный центр должно производиться системный администратором немедленно с момента получения письменного уведомления из кадровой службы Организации.

В течение **3** часов после увольнения, перевода работника в другое структурное подразделение, филиал, региональный центр кадровая служба Организации должны известить системного администратора о состоявшемся приказе.

Аутентификация некоторых пользователей может быть обеспечена с использованием специальных защитных аппаратно-программных средств, рекомендованных к использованию информационной безопасности и централизованно закупленных Организацией у разработчиков (поставщиков) указанных средств.

3. Нормативные ссылки

В части правового обеспечения и оснований для разработки данного документа, использовались следующие документы:

1. Закон Республики Казахстан «Об информатизации» от 24 ноября 2015 года № 418-V ЗРК;
2. Закон Республики Казахстан «О техническом регулировании» от 9 ноября 2004 года;
3. СТ РК ИСО/МЭК 27001-2015 «Методы и средства обеспечения безопасности. Система менеджмента информационной безопасностью. Требования».

4. Правила формирования личного пароля

Личные пароли должны выбираться пользователями и системным администратором ИС самостоятельно с учетом следующих требований:

Пароль должен отвечать следующим требованиям:

- длина пароля должна быть не менее 8 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры или специальные символы;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименование автоматизированного рабочего места – АРМ и так далее), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.), также дни рождения;
- запрещается использовать в качестве пароля «пустой» пароль;
- при смене пароля новое значение должно отличаться от предыдущего не менее, чем в 3 позициях;
- пользователь не имеет права сообщать кому–либо личный пароль.
- запрещается выбирать пароли, которые уже использовались ранее;
- запрещается использовать один и тот же пароль для деловых и неделовых целей;
- пользователь не имеет права разглашать свои личные пароли
- запрещается при авторизации пользователя использовать только логин (имя пользователя) без пароля;
- рекомендуется использовать пароли случайного набора символов.

Для некоторых сотрудников в случае производственной необходимости допускается использование нескольких уникальных имен (учетных записей).

Перед получением временного пароля пользователю рекомендуется подписать обязательство о неразглашении личного пароля (Приложение 2).

Для получения временного пароля пользователь должен предоставить документ, удостоверяющий его личность, или служебное удостоверение.

Пользователь должен запомнить свой пароль самостоятельно, и ни в каком виде не должен его сохранять и передавать другим лицам.

Запрещается выдача паролей пользователям открытыми сообщениями электронной почты или передача их сообщениями электронной почты от третьей стороны в открытой форме.

Пользователь при получении пароля должен расписаться в журнале выдачи и приема пароля.

5. Ввод (доступ) пароля

Ввод пароля осуществляется с учётом регистра (верхний-нижний) и с учётом текущей раскладки клавиатуры (EN-RU и др.).

Во время ввода паролей, необходимо исключить возможность распознания его посторонними лицами или компрометации пароля посредством технических средств.

При вводе паролей происходит проверка правдоподобия логина и пароля. При неправильном вводе пароля вход в систему не производится.

6. Порядок смены паролей

При первом входе в систему пользователь обязан произвести смену временного пароля. При выборе пароля необходимо руководствоваться следующим требованиям 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), 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);

– при смене пароля новое значение должно отличаться от предыдущего не менее, чем в 4 позициях.

Владелец пароля несет персональную ответственность за сохранение в тайне основного пароля. Запрещается сообщать пароль другим лицам, в том числе работникам структурного подразделения, записывать его, а также пересылать открытым текстом в электронных сообщениях.

Пароль никогда не следует хранить в компьютерной системе в незащищенной форме. Владелец должен избегать делать записи (например, на бумаге, в файлах программного обеспечения или портативном устройстве) паролей, без гарантии их безопасного хранения и утверждения метода хранения.

Контроль блокирования учетных записей осуществляется системным администратором, в соответствии с записями журнала регистрации учетных записей.

Пользователь/администратор информационной системы Организации должен сменить основной пароль не реже чем один раз в месяц. Основной пароль может быть создан только самим пользователем или администратором

информационной системы Организации. Запрещается генерировать пароли компьютерными программами и сторонними лицами.

Администратор передает свои аутентификационные данные для доступа к информационным системам Организации на бумажном носителе в опечатанном конверте Представителю руководства по СУИБ, который в свою очередь хранит их в закрывающемся на ключ хранилище.

Пользователь ИС, утративший свои реквизиты доступа в систему, должен официально обратиться за помощью к системному администратору для установки другого пароля на основании письма в Организацию. Пользователь корпоративной сети, утративший свои реквизиты доступа в ИС, должен официально обратиться за помощью к системному администратору для установки другого пароля на основании заявки о выдачи пароля (Приложение 2). Системный администратор в случае необходимости может изменить пароль пользователю корпоративной сети и ИС в любое время (как при регистрации в системе, так и после определенного периода использования пароля).

Системный администратор должен производить проверку цикличного использования старых паролей и исключение повторного использования паролей. А также системный администратор ИС должен удалять неиспользуемые учетные записи (логины и пароли) пользователей.

Системный администратор определяет политику смены пароля, предусматривающую срок действия пароля, выдачу предупреждающего сообщения о необходимости сменить пароль и блокировку доступа к информационным ресурсам по истечению срока действия пароля в 45 дней.

Системный администратор ИС должен иметь возможность смены пароля в любое время. Смену пароля пользователя корпоративной сети осуществляет системный администратор.

7. Управление паролем

Система управления паролированием должна:

1) поддерживать хранение истории предыдущих пользовательских паролей, и предотвращать их повторное использование;

2) хранить и передавать пароли в защищенной форме (зашифрованной или хешированной).

8. Хранение пароля

Владельцам паролей запрещается:

1) сообщать другим пользователям личный пароль и регистрировать их в системе под своей учетной записью и паролем;

2) записывать пароли в электронной записной книжке, файле и других носителях информации, кроме бумажных носителей, при этом бумажные носители с записями паролей должны храниться в сейфе.

Пароли системного администратора ИС с именами учетных записей и датой установки паролей должны храниться в опечатанных конвертах в сейфе у непосредственного руководителя.

Системный администратор ИС и пользователи в течение 3-х часов после смены своих паролей должны передать их новые значения вместе с именами соответствующих учетных записей в запечатанном конверте руководителям соответствующего подразделения. При получении конверта с новыми паролями конверт со старыми паролями уничтожается.

Все пользователи, работающие в ИС, должны проходить безопасную аутентификацию, идентифицирующую их и исключающую возможность подбора пароля и перехвата данных при авторизации.

В случае компрометации пароля системного администратор ИС должен:

1) немедленно сменить свой пароль;
2) известить специалиста по информационной безопасности.

При возникновении производственной необходимости в срочном доступе к данным персонального компьютера временно отсутствующего пользователя разрешается:

1) системный администратору по указанию непосредственного специалиста по информационной безопасности отсутствующего сотрудника поменять пароль временного отсутствующего пользователя для использования компьютера. При выходе на работу пользователь обязан в течении суток сменить пароль. Данные операции фиксируются в журнале о выдачи паролей (Приложение 1);

2) при временно отсутствующем сотруднике специалисту информационной безопасности по указанию непосредственного руководителя, вскрыть конверт с паролем и использовать компьютер. При выходе на работу пользователь обязан в течение суток сменить пароль. Данные операции фиксируются в журнале о выдачи паролей (Приложение 1).

Все пользователи должны быть осведомлены о необходимости запрещения включения паролей в автоматизированный процесс регистрации, например, с использованием хранимых макрокоманд или функциональных клавиш.

Ответственность за разглашение полученного пароля и действия, произведенные на персональном компьютере, возлагается на лицо, получившее пароль после такого случая. По прибытию, временно

отсутствующий пользователь обязан сменить пароль при первом входе в систему.

Учетная запись пользователя, ушедшего в длительный отпуск (более 60 дней), должна блокироваться системным администратором ИС с момента получения письменного уведомления от кадрового подразделения организации.

Для восстановления забытого пароля на ПК необходимо обратиться к непосредственному руководителю для принятия решения о разблокировании учетной записи пользователя.

В случае компрометации пароля пользователь должен немедленно сменить свой пароль.

9. Ответственность при организации парольной защиты

Сотрудники, работающие с ИС, должны быть ознакомлены под роспись с требованиями настоящими Правилами и предупреждены об ответственности за использование паролей, не соответствующих предъявленным требованиям, а также за разглашение парольной информации.

Остальные пользователи системы несут ответственность за хранение учетных записей и паролей.

За разглашение парольной информации, которая представляет конфиденциальные сведения, работник привлекается к ответственности в соответствии с действующим законодательством РК.

Приложение 1
К ПРАВИЛАМ
ОРГАНИЗАЦИИ ПРОЦЕДУРЫ
АУТЕНТИФИКАЦИИ ДЛЯ
СОТРУДНИКОВ ОТДЕЛА ИТ
«__» _____ 202_ г. № __

Журнал о выдаче паролей

№	ФИО/ подпись системного администратора	ФИО/подпись сотрудника	Проводимая операция	Дата
1				

Приложение 2
К ПРАВИЛАМ
ОРГАНИЗАЦИИ ПРОЦЕДУРЫ
АУТЕНТИФИКАЦИИ ДЛЯ
СОТРУДНИКОВ ОТДЕЛА ИТ
«__» _____ 202_ г. № __

ЗАЯВКА
на выдачу пароля

Наименование структурного подразделения

_____

ФИО пользователя корпоративной сети, должность

_____

Причина для выдачи пароля:

_____
_____
_____
_____
_____
_____
_____
_____

Дата и подпись

«____»_____ _____

ЛИСТ ОЗНАКОМЛЕНИЯ

№	Фамилия, имя, отчество	Должность	Личная подпись	Дата
1	**2**	**3**	**4**	**5**
1				
2				
3				
4				
5				
6				
7				
8				
9				