

Инструкция
по организации парольной защиты в информационных системах государственного автономного учреждения дополнительного профессионального образования Иркутской области «Институт развития образования Иркутской области»

1. Общие положения

1.1. Настоящая инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационных системах государственного автономного учреждения дополнительного профессионального образования Иркутской области «Институт развития образования Иркутской области» (далее – ИС ГАУ ДПО ИРО), требования к содержанию паролей, а также контроль за действиями пользователей автоматизированной системы при работе с идентификаторами и персональными паролями.

1.2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей в ИС ГАУ ДПО ИРО и контроль за данными действиями возлагается на администратора информационной безопасности ГАУ ДПО ИРО – администратора средств защиты, содержащих механизмы идентификации и аутентификации (подтверждения подлинности) пользователей по значениям паролей.

1.3. Контроль за действиями пользователей ИС ГАУ ДПО ИРО при работе с паролями, соблюдением порядка их смены, хранения и за соответствие паролей требованиям настоящей инструкции возлагается на администратора информационной безопасности.

2. Правила формирования паролей

2.1. Персональные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями информационных систем самостоятельно с учетом следующих требований:

- 1) длина пароля должна быть не менее 9 символов;
- 2) в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры;
- 3) пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т. д.), последовательности символов и знаков (111, qwerty, abcd и т. д.), общепринятые сокращения (ADMIN, SECRET, USER и т. п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетания букв и знаков, которые можно угадать, основываясь на информации о пользователе;
- 4) использование трех и более подряд идущих на клавиатуре символов, набранных в одном регистре, недопустимо;
- 5) при смене пароля новое значение должно отличаться от предыдущего не менее чем в 3 позициях;
- 6) личный пароль пользователь не имеет права сообщать никому;
- 7) новый пароль не должен совпадать с одним из трех предыдущих паролей;
- 8) пользователь обязан сохранять в тайне свой личный пароль.

2.2. В случае если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на администратора информационной безопасности.

2.3. При технологической необходимости использования учетных данных некоторых сотрудников в их отсутствие (в случае возникновения нештатных ситуаций,

форс-мажорных обстоятельств и т. п.) администратором информационной безопасности по запросу от руководителя структурного подразделения ГАУ ДПО ИРО, в состав которого входит автоматизированное рабочее место ИС ГАУ ДПО ИРО, предоставляется одноразовый пароль на данную учетную запись. По возвращению сотрудник обязан сменить персональный пароль на все локальное программное обеспечение.

3. Порядок ввода пароля

3.1. В целях обеспечения информационной безопасности и противодействия попыткам подбора пароля в ИС ГАУ ДПО ИРО определены правила ввода пароля:

- 1) символы вводимого пароля не отображаются на экране в явном виде;
- 2) учёт всех попыток (успешных и неудачных) входа в систему.

3.2. При первоначальном вводе или смене пароля пользователя действуют следующие правила:

- 1) символы вводимого пароля не должны явно отображаться на экране;
- 2) для подтверждения правильности ввода пароля (с учетом первого правила) – ввод пароля необходимо проводить 2 раза.

3.3. Ввод пароля должен осуществляться непосредственно пользователем ИС ГАУ ДПО ИРО (владельцем пароля). Пользователю запрещается передавать пароль для ввода другим лицам. Передача пароля для ввода другим лицам является разглашением конфиденциальной информации и влечёт за собой ответственность согласно положениям данной Инструкции и в соответствии с действующим законодательством Российской Федерации.

3.4. Непосредственно перед вводом пароля для предотвращения возможности неверного ввода пользователь ИС ГАУ ДПО ИРО должен убедиться в правильности языка ввода (раскладки клавиатуры), проверить, не является ли активной клавиша CAPS LOCK (если это необходимо), а также проконтролировать расположение клавиатуры (клавиатура должна располагаться таким образом, чтобы исключить возможность увидеть набираемый текст посторонними).

3.5. При вводе пароля пользователю необходимо исключить произнесение его вслух, возможность его подсматривания посторонними лицами и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерами и т. п.).

4. Порядок смены личных паролей

4.1. Полная плановая смена паролей проводится регулярно, не реже одного раза в квартал.

4.2. При смене пароля администратором безопасности производится тестирование функций средств защиты информации от несанкционированного доступа путем ввода с клавиатуры заведомо ложного пароля, при наличии считывателя – предъявления стороннего идентификатора.

4.3. Внеплановая смена персонального пароля или удаление учетной записи пользователя ИС ГАУ ДПО ИРО в случае прекращения его полномочий (увольнение, переход на другую работу внутри предприятия и т.п.) должна производиться администратором информационной безопасности немедленно после окончания последнего сеанса работы данного пользователя с системой.

4.4. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри предприятия и т.д.) администратора информационной безопасности и других сотрудников, которым для выполнения их должностных обязанностей были предоставлены полномочия по управлению парольной защитой ИС ГАУ ДПО ИРО.

4.5. Временный пароль, заданный системным администратором при регистрации нового пользователя, следует изменить при первом входе в систему.

4.6. Работники, имеющие доступ к ИС ГАУ ДПО ИРО, в течение 3-х часов после смены своих паролей должны передать их новые значения вместе с именами соответствующих учетных записей в запечатанном конверте администратору информационной безопасности на хранение. При получении конверта с новыми паролями конверт со старыми паролями уничтожается.

4.7. Учетная запись пользователя, ушедшего в длительный отпуск (более 60 дней), должна блокироваться администратором информационной безопасности с момента получения письменного уведомления из отдела правового и кадрового обеспечения ГАУ ДПО ИРО.

4.8. Удаление учетных записей пользователей, уволенных, переведенных в другое структурное подразделение ГАУ ДПО ИРО должно производиться администратором информационной безопасности немедленно с момента получения письменного уведомления из отдела правового и кадрового обеспечения ГАУ ДПО ИРО.

4.9. Отдел правового и кадрового обеспечения ГАУ ДПО ИРО должен известить администратора информационной безопасности о состоявшемся приказе в течение 24 часов после увольнения, перевода сотрудника в другое структурное подразделение.

5. Порядок хранения пароля

5.1. Хранение работником зарегистрированных идентификаторов и значений своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе администратора информационной безопасности.

5.2. При возникновении производственной необходимости в срочном доступе в автоматизированную систему временно отсутствующего пользователя разрешается произвести смену пароля пользователя его непосредственным руководителем. При этом должен быть составлен акт о вскрытии конверта с паролем и о его повторном опечатывании с новым паролем.

5.3. Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации.

5.4. Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

6. Действия работника в случае утери и компрометации пароля

6.1. В случае возникновения необходимости в смене пароля в виду компрометации пользователь должен немедленно сменить свой пароль и известить администратора информационной безопасности.

6.2. В случае компрометации (утеря, передача парольной информации) персонального пароля пользователя ИС ГАУ ДПО ИРО должны быть немедленно предприняты меры в соответствии с пунктами 4.3, 4.4 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

7. Ответственность при организации парольной защиты

7.1. Владельцы паролей должны быть ознакомлены под расписку с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение информации о пароле.

7.2. Ответственность за организацию парольной защиты в ГАУ ДПО ИРО возлагается на администратора информационной безопасности.