?????????? ?
????????? ??????

- ИНСТРУКЦИЯ О ПАРОЛЬНОЙ ЗАЩИТЕ УЧРЕЖДЕНИЯ «SDU UNIVERSITY»

?????????? ? ????????? ?????? ??????????? «SDU UNIVERSITY»

СОДЕРЖАНИЕ

1. Общие положения

2. Правила формирования пароля

3. Ввод пароля

4. Порядок смены паролей

5. Хранение пароля

6. Ответственность при организации парольной защиты

????? ?????????

1 Настоящая Инструкция (далее - Инструкция) о парольной защите Учреждения SDU University» (далее – Университет) регламентирует организационно-ехническое обеспечение процессов генерации, использования, смены и рекращения действия личных паролей пользователей ПК и администраторов ıформационных систем (ИС), удаления учетных записей.

2 В данной Инструкции используются следующие основные понятия и термины:

ıформационные ресурсы - электронная систематизированная информация аза данных),

держащаяся в информационных системах, объединенная соответствующим рограммным

еспечением;

ɔмпрометация пароля - утечка или разглашение пароля;

ользователь - сотрудник Университета, использующий закрепленный за ним на емя выполнения

оих должностных обязанностей персональный компьютер, подключенный к окальной

ычислительной сети и располагающий определенными правами доступа к ыформационным

есурсам;

3 В целях идентификации, аутентификации и соблюдения принципа ерсональной ответственности

свои действия, пользователям присваиваются персональные уникальные имена четная запись) с

ролями.

4 Эффективность парольной защиты, выполнение требований к ее организации на рабочих станциях локальной вычислительной сети Университета выполняется Отделом информационно-технической поддержки (далее – ОИТП) и контролируется Системным администратором Университета.

5 Эффективность парольной защиты, выполнение требований к ее организации на серверах,

тевом оборудовании, базе данных ИС выполняется ОИТП и контролируется СИБ.

6 Контроль за исполнением политики парольной защиты возлагается на СИБ.

??????? ???????????? ??????

2.1 Требования к паролям:

- **Длина:** Пароль должен содержать не менее **8 символов**.
- **Состав:** В пароле обязательно должны использоваться заглавные и строчные буквы, цифры и специальные символы.
- **Авторизация:** Запрещается вход в систему с использованием только логина, без ввода пароля.
- **Конфиденциальность:** Пользователь не имеет права передавать или разглашать свой личный пароль третьим лицам.

- **Сложность:**
  - Запрещено использовать легкоугадываемые комбинации: личные данные (имена, даты рождения, номера телефонов, автономера) и стандартные последовательности клавиш (*qwerty*, *123456*, *zyxwvuts* и т.д.).
  - Рекомендуется использовать случайные наборы символов.
- **Правила смены пароля:**
  - Запрещается повторно использовать старые пароли.
  - Новый пароль должен отличаться от предыдущего минимум в **6 позициях**.
- **Срок действия и блокировка:**

> Срок действия пароля составляет **180 дней**. Пароль необходимо обновить до истечения этого срока. В противном случае доступ к сервисам, интегрированным с Active Directory (AD) — включая **Wi-Fi, Moodle** и другие ресурсы — будет ограничен.

???? ??????

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

.2 Во время ввода паролей, необходимо исключить возможность распознания го посторонними лицами или компрометации пароля посредством технических редств.

??????? ????? ???????

.1 Рабочие станции должны быть подключены к центральной системе.

.2 Изменение пароля рабочих станций является обязанностью пользователей

.3 Смена пароля на серверах и коммутаторах осуществляется системным дминистратором ОИТП не реже 1 раза в месяц.

.4 Смена пароля на базах данных ИС осуществляется администратором БД дин раз в 6 месяцев.

.5 Пользователи должны иметь возможность менять свои пароли. В связи с тим на платформе подготовлена или учетные записи пользователей ривязаны к телефонам с двухэтапной системой проверки. При регистрации в истеме пользователям выдается одноразовый пароль, который необходимо зменить. Пароли пользователей должны храниться в базе данных в ашифрованном виде.

???????? ??????

.1 Владельцам паролей запрещается:

- сообщать другим пользователям личный пароль и регистрировать их в системе под своей учетной записью и паролем;
- записывать пароли в электронной записной книжке, файле и других носителях информации, кроме бумажных носителей, при этом бумажные носители с записями паролей должны храниться в надежном и доступном только владельцу месте.

.2 Пароли пользователей рабочих станций с именами учетных записей и датой становки паролей должны храниться в электронном виде у системного дминистратора ОИТП.

.3 Пароли серверов, коммутаторов, базы данных запечатывается в бумажном иде в конверт, подписывается ректором Университета, и хранится в сейфе в ерверном помещении.

.4 В случае компрометации пароля сотрудник должен:

- известить ОИТП;
- известить СИБ;
- блокировать доступ пользователям, подключенным к ресурсам этой ИС, до смены пароля;

.5 При возникновении производственной необходимости в срочном доступе к анным персонального компьютера временно отсутствующего пользователя азрешается:

- непосредственному руководителю или другому сотруднику по указанию непосредственного руководителя, запросить ввод пароля системным администратором и использовать компьютер;
- произвести смену пароля (с помощью сотрудников ОИТП) пользователя его непосредственным руководителем.

тветственность за неразглашение полученного пароля и действия, роизведенные на персональном компьютере, возлагается на лицо, олучившее пароль после такого случая. По прибытию, временно тсутствующий пользователь обязан сменить пароль (с помощью ОИТП) при ервом входе в систему.

5.6 Учетная запись пользователя, ушедшего в длительный отпуск (более 60 ней), блокируется сотрудником ОИТП с момента получения письменного ведомления от кадровой службы Университета.

5.7 Удаление учетных записей пользователей, уволенных, переведенных в ругое структурное подразделение производится системным администратором ИТП с момента получения письменного уведомления из кадровой службы ниверситета.

течение 24 часов после увольнения, перевода работника в другое труктурное подразделение, кадровая служба Университета извещает ОИТП о остоявшемся приказе.

.8 Аутентификация некоторых пользователей может быть обеспечена с спользованием специальных защитных аппаратно-программных средств, екомендованных к использованию ОИТП.

?????????????? ??? ??????????? ????????? ??????

1 Сотрудники Университета должны быть ознакомлены под роспись с настоящей инструкцией и предупреждены об ответственности за использование паролей, не соответствующих предъявленным требованиям, а также за разглашение парольной информации.

2 За разглашение парольной информации, которая представляет конфиденциальные сведения Университета, сотрудник привлекается к дисциплинарной ответственности в соответствии с нормативными актами Университета.