

	<p>Государственное агентство гражданской авиации при Кабинете Министров Кыргызской Республики Высшее авиационное учебное заведение Кыргызский авиационный институт им.И.Абдраймова СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА</p>	<p>КАИ СМК И-023-02/1</p>
---	---	---------------------------

ОДОБРЕНО

Ученым Советом
Кыргызского авиационного
института им. И. Абдраймова
протокол № 9
от « 30 » 06 2015

УТВЕРЖДАЮ

Директор
Кыргызского авиационного
института им. И. Абдраймова



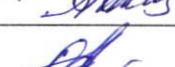
У.Э. Курманов

« 1 » 07 2025 г.
Приказ № 00 от « 1 » 07 2025 г.

**Инструкция
ПО ОРГАНИЗАЦИИ ПАРОЛЬНОЙ ЗАЩИТЫ
Кыргызского авиационного института им. И. Абдраймова**

Дата введения:

« 1 » 07 2025 г.

Должность	Ф.И.О. / Подпись	Дата
Разработано	зав.ЦУОП А.Д. Жунушалиева / 	1.07.2025,
Согласовано	Заместитель директора по УР О.А. Садовская / 	01.07.2025.
Согласовано	Зав. ОКБП и стандартов ИКАО Е.А.Деревянкина / 	1.07.2025

Бишкек – 2025



Государственное агентство гражданской авиации
при Кабинете Министров Кыргызской Республики
Высшее авиационное учебное заведение
Кыргызский авиационный институт
им.И.Абдраимова
СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА

КАИ СМК И-023-02/1

Лист регистрации изменений

Лист ознакомления

	<p>Государственное агентство гражданской авиации при Кабинете Министров Кыргызской Республики Высшее авиационное учебное заведение Кыргызский авиационный институт им.И.Абдраймова</p> <p>СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА</p>	<p>КАИ СМК И-023-02/1</p>
---	--	---------------------------

1. Общие положения

1.1. Настоящий документ регламентирует процессы генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационных системах персональных данных (далее – ИСПДн) Кыргызского авиационного института им. И.Абдраймова (далее – Авиаинститут) и разработан в соответствии нормативными документами по безопасности информации:

- Закон Кыргызской Республики от 14 апреля 2008 года № 58 «Об информации персонального характера». (В редакции Законов КР от 20 июля 2017 года № 129, 29 ноября 2021 года № 142, 30 июня 2022 года № 53, 12 июля 2022 года № 61);
- Указ Президента Кыргызской Республики от 12 мая 2023 года УП № 122 «О мерах по дальнейшему совершенствованию цифровой трансформации в сфере государственного управления» (В редакции Указов Президента КР от 5 апреля 2024 года УП № 90, 18 сентября 2024 года УП № 265);
- Указ Президента Кыргызской Республики от 5 апреля 2024 года УП № 90 «Об утверждении Концепции цифровой трансформации Кыргызской Республики на 2024-2028 годы»;
- Концепция Цифровой трансформации Кыргызской Республики на 2024-2028 годы <https://cbd.minjust.gov.kg/30-164/edition/6414/ru>;
- Закон Кыргызской Республики «О праве на доступ к информации» от 29 декабря 2023 года № 217 (Опубликован в газете "Эркин Too" от 12 января 2024 года № 3);
- Постановление от 21 ноября 2017 года № 762 «Об утверждении Требований к защите информации, содержащейся в базах данных государственных информационных систем» (В редакции постановления Правительства КР от 31 декабря 2019 года № 744, и Кабинета Министров КР от 31 января 2022 года № 45)

1.2. Настоящая инструкция устанавливает основные правила введения парольной защиты информационной системы AVN и персональных данных Авиаинститута. Инструкция регламентирует организационно-техническое обеспечение генерации, смены и прекращения действия паролей в информационной системе AVN

1.3. Осуществление процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИС AVN и контроль за действиями исполнителей и специалистов системы при работе с паролями возлагается на администратора безопасности ИСПДн

2. Термины и определения

AVN –название информационной системы в Авиаинституте

Информация – сведения (сообщения, данные) независимо от формы их представления.

Идентификация - присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

	<p>Государственное агентство гражданской авиации при Кабинете Министров Кыргызской Республики Высшее авиационное учебное заведение Кыргызский авиационный институт им.И.Абдрамова</p> <p style="text-align: center;">СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА</p>	<p>КАИ СМК И-023-02/1</p>
---	---	---------------------------

ИС – информационная система

ИСПДн — информационная система персональных данных- совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

Компрометация- факт доступа постороннего лица к защищаемой информации, а также подозрение на него.

Несанкционированный доступ - доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или ИС.

Персональные данные - это любая информация, используя которую человека можно прямо или косвенно узнать (идентифицировать).

Объект доступа - единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.

Пароль - секретная комбинация цифр, знаков, слов, или осмысленное предложение, служащие для защиты информации от несанкционированного доступа к информационным ресурсам;

Правила доступа - совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Субъект доступа - лицо или процесс, действия которого регламентируются правилами разграничения доступа.

ЦУОП- центр управления образовательным порталом.

2. Правила формирования паролей для входа в Информационную систему

AVN

2.1. Персональные пароли должны генерироваться специальными программными средствами информационной системы AVN и распределяются централизованно либо выбираются пользователями информационной системы самостоятельно с учетом следующих требований:

- пароль должен состоять не менее чем из восьми символов;
- в пароле обязательно должны присутствовать буквы из верхнего и нижнего регистров, цифры и специальные символы (@, #, \$, &, *, % и т. п.);
- 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 (ЭВМ, ЛВС, USER и т. п.), аббревиатуры, номера автомобилей, телефонов и другие значимые сочетания букв и знаков, которые можно угадать, основываясь на информации о пользователе;
- при смене пароля новый пароль должен отличаться от старого не менее чем — в шести позициях.

2.2. Допускается использование единого пароля для доступа субъекта доступа к различным информационным ресурсам одной ИСПДн объекта образования.

	<p>Государственное агентство гражданской авиации при Кабинете Министров Кыргызской Республики Высшее авиационное учебное заведение Кыргызский авиационный институт им.И.Абдраймова</p> <p style="text-align: center;">СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА</p>	<p>КАИ СМК И-023-02/1</p>
---	--	---------------------------

2.3. В случае если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на уполномоченных сотрудников центра управления образовательным порталом (ЦУОП).

3. Ввод пароля

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

3.2. При неверном вводе пароля более 3 раз, учетная запись пользователя блокируется.

4. Порядок смены паролей

4.2. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одно раза в месяц.

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

4.4. Полная внеплановая смена паролей всех пользователей должна производиться случае прекращения полномочий администраторов средств защиты или других сотрудников, которым по роду службы были предоставлены полномочия по управлению парольной защитой.

4.5. Полная внеплановая смена паролей должна производиться в случае компрометации личного пароля одного из администраторов ИСПДн.

4.6. В случае компрометации личного пароля пользователя надлежит немедленно ограничить доступ к информации с данной учетной записи, до момента вступления в силу новой учетной записи пользователя или пароля.

4.7. В случае прекращения полномочий пользователя (увольнение, переход на другую работу и т. п.) системный администратор должен немедленно удалить его учетную запись сразу после окончания последнего сеанса работы данного пользователя с системой.

5. Обязанности пользователей при работе с парольной защитой

5.1. При работе с парольной защитой пользователям запрещается:

- разглашать кому-либо персональный пароль и прочие идентифицирующие сведения;
- предоставлять доступ от своей учетной записи к информации, хранящейся в ИСПДн посторонним лицам;
- записывать пароли на бумаге, файле, электронных и прочих носителях информации.

5.2. Хранение пользователем своего пароля на бумажном носителе допускается только в личном владельцем.

5.3. При вводе пароля пользователь обязан исключить возможность его перехвата сторонними лицами и техническими средствами.

	<p>Государственное агентство гражданской авиации при Кабинете Министров Кыргызской Республики Высшее авиационное учебное заведение Кыргызский авиационный институт им.И.Абдраймова</p> <p>СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА</p>	<p>КАИ СМК И-023-02/1</p>
---	--	---------------------------

6. Случаи компрометации паролей

- 6.1. Под компрометацией следует понимать:
 - физическая потеря носителя с информацией;
 - передача идентификационной информации по открытым каналам связи;
 - проникновение постороннего лица в помещение физического хранения носителя парольной информации или алгоритма или подозрение на него (срабатывание сигнализации, повреждение устройств контроля НСД (слепков печатей), повреждение замков и т. п.);
 - визуальный осмотр носителя идентификационной информации посторонним лицом;
 - перехват пароля при распределении идентификаторов;
 - сознательная передача информации постороннему лицу.
- 6.2. Действия при компрометации пароля:
 - скомпрометированный пароль сразу же выводится из действия, взамен его вводятся запасной или новый пароль;
 - о компрометации немедленно оповещаются все участники обмена информацией.

Пароль вносится в специальные списки, содержащие скомпрометированные пароли и учетные записи.

7. Ответственность пользователей при работе с парольной защитой

- 7.1. Повседневный контроль за действиями сотрудников Авиаинститута при работе с паролями, соблюдением порядка их смены, хранения и использования, возлагается на системного администратора ИС AVN/
- 7.2. Владельцы паролей должны быть ознакомлены с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.
- 7.3. Ответственность за организацию парольной защиты возлагается на ответственного за систему защиты информации в информационной системе персональных данных.
- 7.4. Ответственность в случае несвоевременного уведомления ответственного за систему защиты информации в информационной системе персональных данных о случаях утери, кражи, взлома или компрометации паролей возлагается на владельца взломанной учетной записи.