Министерство образования Кузбасса

Государственное профессиональное образовательное учреждение «Прокопьевский аграрный колледж»

Приложение
УТВЕРЖДЕНО
Приказом директора ГПОУ ПАК
№ от «___»_____2026г.

# ПОЛОЖЕНИЕ
# О ПАРОЛЬНОЙ ПОЛИТИКЕ

Прокопьевский район
п. Школьный
2026

## СОДЕРЖАНИЕ

| | | |
|---|---|---|
| 1 | ОБЛАСТЬ ПРИМЕНЕНИЯ | 3 |
| 2 | НОРМАТИВНЫЕ ССЫЛКИ | 3 |
| 3 | ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ, ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ | 4 |
| 4 | ПОЛОЖЕНИЯ | 6 |
| 5 | ЛИСТ СОГЛАСОВАНИЯ | 13 |
| 6 | ЛИСТ ОЗНАКОМЛЕНИЯ | 14 |
| 7 | ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ | 16 |

## 1. ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1 Настоящее положение о парольной политике (далее Политика) определяет требования к процедуре обеспечения безопасности информации при управлении парольной информацией Государственного профессионального образовательного учреждения «Прокопьевский аграрный колледж» (далее Колледж), определяющую нормы по защите парольной информации (далее пароли) при работе с информационными ресурсами и (или) в информационных системах (далее ИТ-инфраструктура) колледжа, действующие во всех структурных подразделениях.

1.2 Политика предназначена для предотвращения возникновения недопустимых для Колледжа событий, влекущих за собой различные виды ущерба, которые могут произойти в результате компрометации паролей учетных записей пользователей и администраторов ИТ-инфраструктуры Колледжа.

1.3 Политика обязательна к применению всеми должностными лицами, являющимися работниками или обучающимися Колледжа и для которых в Колледже создана учетная запись в ИТ-инфраструктуре.

1.4 Политика направлена на противодействие компьютерным атакам или другим событиям, которые могут привести к компрометации паролей.

1.5 Решение задач обеспечения безопасности информации при управлении паролями в Колледже достигается применением организационных мер и использованием технических (программных) средств.

1.6 Организационные меры защиты парольной информации реализуются путем выполнения мероприятий в соответствии с требованиями, приведёнными в настоящей Политике.

1.7 Технические (программные) средства для защиты парольной информации должны реализовывать необходимые функции по обеспечению безопасности.

## 2. НОРМАТИВНЫЕ ССЫЛКИ

Настоящая Политика разработана на основании следующих нормативно-правовых документов:

- Федеральный закон от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон РФ от 27июля 2006 г. № 152-ФЗ «О персональных данных»;

- Постановление Правительства Российской Федерации от 06.07.2015 № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации»;
- Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Письмо Минобрнауки «О мерах по повышению защищенности информационной инфраструктуры РФ» от 19.03.2026 № МН-19/438.

## 3. ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ, ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

3.1 Термины и определения В настоящем положении используются следующие понятия и термины:

**Администратор** – лицо, использующее объекты ИТ-инфраструктуры колледжа для администрирования, обеспечения функционирования, настройки в ходе выполнения своих функциональных обязанностей или договорных обязательств.

**Аутентификация** – процедура проверки подлинности лица путем сравнения введенного им пароля с паролем, сохраненным в базе данных учетных записей ИТ-инфраструктуры колледжа.

**Информационная система** – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

**ИТ-инфраструктура колледжа** – совокупность информационных систем и (или) отдельных информационных ресурсов колледжа.

**Компрометация парол**я – факт доступа или возможность доступа постороннего лица к защищаемой парольной информации, а также подозрение на это действие.

Примерами компрометации паролей являются:

- перехват пароля при передаче пользователю незащищенным способом, нарушающим его конфиденциальность;

- физическая утеря носителя с парольной информацией;

- подбор пароля в результате компьютерной атаки;

- проникновение постороннего лица в помещение, где храниться парольная информация на физическом носителе в открытом виде, или подозрение на это действие (срабатывание сигнализации, повреждение устройств контроля НСД (слепков печатей), повреждение замков и т. п.);

- сознательная передача пароля постороннему лицу.

**Парольная информация (пароль)** – составная часть учетной записи, используемая в процедуре аутентификации. Пароли используются для подтверждения права доступа пользователя ИТ-инфраструктуры колледжа к информационным ресурсам и лежат в основе механизмов аутентификации, используемых при предоставлении доступа в ИТинфраструктуре Колледжа.

**Пользователь** – лицо, использующее объекты ИТ-инфраструктуры колледжа для обработки информации в ходе выполнения своих функциональных обязанностей или договорных обязательств, для которых создана учетная запись.

**Служба поддержки пользователей** – это служба, в которую пользователи могут обратиться за оказанием технической поддержки по решению возникшей проблемы, а также за получением дополнительной информации по интересующему вопросу (Информационно-вычислительный центр (ИВЦ), +7 (3846) 641-603.

**Технология единого входа** – информационная технология, при использовании которой пользователь переходит из одной информационной системы в другую (не связанную с первой системой) без повторной аутентификации.

**Учетная запись** – набор служебной информации, который содержит сведения, необходимые для идентификации пользователя при подключении к информационному ресурсу или информационной системе, а также информацию для авторизации и учета пользователя.

3.2 Обозначения и сокращения

**АРМ** – автоматизированное рабочее место – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

АС – автоматизированная система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

ИБ – информационная безопасность.

ИС – информационная система.

ИР – совокупность информационных объектов (информации и ее носителей), которые находятся в распоряжении Университета и могут быть использованы для осуществления деятельности Университета.

ЛВС – локальная вычислительная сеть.

НСД – несанкционированный доступ.

## 4. ПОЛОЖЕНИЯ

4.1 Общие положения

4.1.1 Обеспечение безопасности информации при управлении паролями предназначено для решения следующих задач:

4.1.1.1 определение видов паролей, используемых в Колледже;

4.1.1.2 определения правил формирования и использования паролей для обеспечения их стойкости;

4.1.1.3 определения правил обращения с паролями для соблюдения их безопасности (конфиденциальности).

4.1.2 Парольная аутентификация является одним из важнейших механизмов обеспечения защиты учетных записей пользователей от несанкционированного доступа.

4.1.3 В случае создания учетной записи Колледжа для лиц, не являющимися работниками или обучающими Колледжа, обязанность по выполнению Политики должна включаться в текст договоров с такими лицами или в правила проводимых конкурсов/мероприятий работниками структурных подразделений, организующими заключение договора или формирующими правила участия.

4.1.4 Настоящая Политика определяет требования к порядку создания, хранения, использования, смены и другим вопросам, связанным с применением механизмов парольной аутентификации в ИС Колледжа.

4.1.5 Целью настоящей Политики является минимизация рисков раскрытия или утраты конфиденциальных ИР, кражи интеллектуальной собственности и репутационных потерь.

4.1.6 Политикой не охватываются вопросы защиты ИС, предназначенных для обработки информации, содержащей сведения, составляющие государственную тайну.

4.1.7 Политика подлежит регулярному пересмотру с периодичностью достаточной и необходимой для приведения парольной защиты в соответствие реальным условиям. Также может проводиться внеплановый пересмотр Политики при изменении перечня решаемых задач, конфигурации технических и программных средств.

4.2 Правила обеспечения безопасности информации при управлении парольной информацией

4.2.1 Все должностные лица, создающие, передающие, получающие и использующие пароли в ИС, должны выполнять установленные Политикой требования.

4.2.2 Пароли должны быть защищены от доступа третьих лиц для соблюдения конфиденциальности пароля.

4.2.3 Процессы создания, передачи, получения и использования паролей должны выполняться в соответствии с правилами Политики.

4.2.4 Правила создания паролей:

В Колледже используются следующие виды паролей:

Пользовательские – создаются уполномоченными лицами из состава администраторов информационных систем и сервисов, передаются пользователям (владельцам учетной записи) способом, исключающим его компрометацию, и действуют в течение установленного срока действия первичного пароля в соответствии с правилами создания и использования паролей;

Пароли администраторов - создаются уполномоченными лицами, передаются пользователям (владельцам учетной записи), имеющим полномочия Администратора (установленные локальными нормативными актами Колледжа) способом, исключающим их компрометацию, действуют в течение установленного срока действия пароля в соответствии с правилами создания и использования паролей.

4.2.5 После окончания срока действия пароля учетная запись пользователя блокируется и для восстановления доступа к ИС или сервису пользователю необходимо обратиться в службу поддержки пользователей ИС Колледжа.

4.3 Правила создания и использования паролей

4.3.1 Правила создания и использования паролей для обеспечения их стойкости определены на основе следующих требований:

- к минимальной и максимальной длине пароля;
- к сложности пароля;
- к сроку действия пароля;
- к возможности использования паролей, использовавшихся ранее.

4.3.2 Правила создания и использования паролей, в зависимости от установленных требований, представлены в таблице 1.

Таблица 1.

| Установленное требование | Описание требования | Правила |
|---|---|---|
| К минимальной длине пароля | Минимальное количество символов, требуемое системой при создании пароля | Для пользователя: не менее 8 Для администратора: не менее 12 |
| К максимальной длине пароля | Максимальное количество символов, ограниченное системой при создании пароля | Не более 16 |
| К сложности пароля | Обязанность использования определенных символов при создании пароля с учетом требований к стойкости пароля | Заглавные и строчные буквы латинского алфавита, цифры и специальные символы |
| К сроку действия пароля | Минимальный и максимальный срок действия пароля в системе (при истечении требуется замена пароля) | От 60 дней до 90 дней |
| К возможности создания ранее использовавшихся паролей | При создании пароля ограничивается возможность использования паролей, использованных пользователем ранее в информационной системе | Не применимо |

4.3.3 Требования к стойкости пароля, при его формировании, заключаются в необходимости выполнение следующих правил и рекомендаций:

4.3.3.1 необходимо использовать сочетание букв верхнего и нижнего регистров латинского алфавита (А-Я, A-Z, а-я, a-z);

4.3.3.2 при использовании цифр необходимо использовать цифры из диапазона от 0 до 9;

4.3.3.3 при использовании специальных символов возможно использовать символы из следующего набора: !@#$%^&*()_+|~-=`{}[]:";'<>?,./;

4.3.3.4 пароль не должен являться словом на любом языке, диалекте, сленге, жаргоне, которое, в том числе:

- может содержаться в словарях (русских или иностранных);
- пароль не должен включать в себя легко вычисляемые сочетания символов, комбинаций соседних клавиш и словарных слов, а также общепринятые сокращения (abcde…, 12345…, ЭВМ, ЛВС, USER и т.п.);
- пароли от учетных записей на разных сервисах должны отличаться;
- не допускается использовать пароли «по умолчанию»;
- в пароле не должно быть персонифицированной информации (например фамилии, даты рождения, номера СНИЛС или ИНН, адреса или номера телефонов, имена друзей, коллег, вымышленных персонажей и т. д.);
- пароль не должен содержать компьютерные термины или названия, команды, названия сайтов, компаний, оборудования, программного обеспечения;
- пароль не должен содержать возможные названия «ПАК» или географические наименования, например "Moscow", "Kursk" или их производные.

4.4 Правила обращения с паролями

4.4.1 Пользователям запрещается предпринимать какие-либо действия по получению и использованию паролей других пользователей.

4.4.2 Пользователи должны выполнять правила по соблюдению конфиденциальности личного используемого пароля, при помощи которых можно исключить или снизить вероятность его компрометации.

4.4.3 Пользователям запрещается:

4.4.3.1 сообщать (передавать) личный пароль другим лицам, включая работников Колледжа;

4.4.3.2 озвучивать личный пароль голосом, в том числе находясь рядом с другими лицами;

4.4.3.3 сообщать кому-либо информацию о своих правилах формирования пароля;

4.4.3.4 указывать личный пароль в анкетах или различных «опросниках»;

4.4.3.5 записывать пароль и хранить его в открытом виде на рабочем месте (внутренности ящика стола, на мониторе, на обратной стороне клавиатуры и т.д.), на отдельных листах бумаги или записных книжках, для хранения которых не

используется хранилище, запираемое на ключ, т.е. в местах, где к ним могут получить доступ другие лица;

4.4.3.6 хранить пароль в файле в облачном сервисе, на компьютере, включая переносной, без использования шифрования.

4.4.4 При подозрении на компрометацию пароля пользователь должен незамедлительно прекратить использовать этот пароль и сменить его при помощи службы поддержки пользователей ИС Колледжа.

4.4.5 Первичные пароли должны передаваться (сообщаться) только пользователю, для которого этот пароль создан. Запрещается передавать (сообщать) первичные (временные) пароли через других работников Колледжа или каких-либо других третьих лиц.

4.4.6 В случае, если кто-либо требует сообщить личный пароль, пользователю необходимо отказать этому лицу, сославшись на этот документ.

Смена паролей:

Пароли системных учётных записей (администратора домена, администратора приложений и сетевого оборудования, локального администратора и т. д.) должны меняться не реже чем один раз в шесть месяцев, пароли пользовательских учётных записей (работников подразделений, преподавателей, студентов и т. д.) — не реже чем один раз в год.

Передача первоначального пароля — администратор ИС задаёт пользователю уникальный пароль, который передаётся лично на бумажном носителе. Не допускается передавать пароль в открытом виде по электронной почте и другим открытым каналам связи.

Обязательная смена пароля производится при первом входе в ИС, пользователь обязан сменить первоначальный пароль, заданный администратором (при наличии технической возможности).

Внеплановая смена пароля проводится в случае компрометации или утери пароля.

При смене пароля новое значение не должно совпадать ни с одним из пяти последних ранее используемых паролей.

Для обеспечения парольной безопасности в колледже могут использоваться, например:

- Механизмы, реализующие принудительное исполнение требований - в ИС, в базах данных, на серверах (при наличии технической возможности). Например,

механизмы для ограничения на минимальную длину пароля, периода действия пароля, запрета на повтор недавно используемых паролей, проверки паролей на сложность.

- Специализированное программное обеспечение - для автоматического создания паролей, которое должно удовлетворять всем требованиям, указанным в политике.
- Контроль подбора паролей - в ИС может быть установлено ограничение на количество неудачных попыток ввода неверного пароля, после которого доступ к ИС для данной учётной записи автоматически блокируется.

4.5 Документы, регламентирующие деятельность по управлению парольной информацией

4.5.1 Для организационной поддержки положений Политики в Колледже могут разрабатываться и вводятся в действие регламенты деятельности по обеспечению безопасности информации при управлении парольной информацией для определения границ зон ответственности участников процессов.

4.5.2 При необходимости в Колледже разрабатываются и вводятся в действие инструкции, памятки и методические рекомендации по указанному направлению, учитывающие особенности отдельных информационных процессов.

4.6 Контроль

4.6.1 В Колледже должен быть организован контроль выполнения установленных настоящей Политикой требований.

4.6.2 Контроль может проводиться как на плановой основе, так и по отдельному распоряжению директора колледжа.

4.6.3 Контроль за исполнением требований настоящей Политики возлагается на Информационно-вычислительный центр (ИВЦ), +7(3846) 641-603.

4.7 Ответственность

4.7.1 За несоблюдение Политики все лица, на которых распространяется ее действие, могут быть привлечены к ответственности в соответствии с законодательством Российской Федерации или положениями отдельных локальных нормативных актов Колледжа.

4.8 Исключения

4.8.1 Отдельные особенности применения Политики, при наличии уважительной причины к отклонению от ее условий, должны быть согласованы с

ИВЦ Колледжа посредством направления служебной записки по основным видам деятельности на имя директора колледжа либо установлены в отдельном локальном нормативном акте.

# ЛИСТ СОГЛАСОВАНИЯ

Ведущий юрисконсульт _____ О.А. Швец

подпись

«___» _____20___г.

Начальник ИВЦ _____ В.А.Лялин

подпись

«___» _____20___г.

## ЛИСТ ОЗНАКОМЛЕНИЯ

С положением Парольной политики ознакомлен:

| Фамилия, инициалы | Дата ознакомления | Подпись |
|---|---|---|
| | | |
| | | |
| | | |

| | | |
|---|---|---|
| | | |
| | | |
| | | |

# ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

| Номер изменения | Номера страниц | | | | Всего страниц | Дата | Основание для изменения и подпись лица, проводившего изменения |
|---|---|---|---|---|---|---|---|
| | измененных | замененных | аннулированных | новых | | | |
| | | | | | | | |
| | | | | | | | |
| | | | |