Министерство здравоохранения Республики Беларусь
Учреждение образования «Витебский государственный ордена Дружбы народов медицинский университет»

УТВЕРЖДЕНО
Ректором учреждения образования «Витебский государственный ордена Дружбы народов медицинский университет» А.Н.Чукановым

Политика о порядке генерации и смене аутентификационных данных пользователей (паролей)

31 декабря 2025 № 02-08/66

г. Витебск

ГЛАВА 1
ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Политика о порядке генерации и смене аутентификационных данных пользователей (паролей) определяет требования и порядок создания, использования, хранения и изменения паролей пользователей информационных систем и информационных ресурсов учреждения образования «Витебский государственный ордена дружбы народов медицинский университет» (далее – Университет).

1.2. Политика разработана в целях обеспечения защиты информации, предотвращения несанкционированного доступа к информационным ресурсам и выполнения требований законодательства Республики Беларусь в сфере информационной безопасности и защиты информации.

1.3. Действие Политики распространяется на всех работников Университета, а также иных лиц, которым предоставлен временный или постоянный доступ к информационным системам и ресурсам Университета (далее – Пользователи).

1.4. Требования настоящей Политики являются обязательными для выполнения всеми Пользователями.

1.5. Настоящая Политика разработана в соответствии с законодательством Республики Беларусь в части обеспечения информационной безопасности, международными стандартами в области информационной безопасности продуктов и систем информационных технологий.

ГЛАВА 2
ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. Информационная система – совокупность банков данных, информационных технологий и комплекса (комплексов) программно-технических средств (далее – ИС).

2.2. Информационный ресурс – организованная совокупность документированной информации, включающая базы данных, другие совокупности взаимосвязанной информации в информационных системах (далее – ИР).

2.3. Пользователь – физическое лицо, получившее в установленном порядке доступ к ИС, ИР и (или) информационной сети и пользующееся ими.

2.4. Учётная запись – совокупность данных, идентифицирующих пользователя в информационной системе и определяющих его права доступа.

2.5. Пароль – конфиденциальная символьная последовательность, используемая для аутентификации Пользователя при доступе к ИС и ИР.

2.6. Аутентификация – процесс проверки подлинности Пользователя по предъявляемым им аутентификационным данным.

2.7. Компрометация пароля – утрата конфиденциальности пароля, в том числе его раскрытие, утечка или подозрение на несанкционированное использование.

ГЛАВА 3
ОБЩИЕ ТРЕБОВАНИЯ К ПАРОЛЯМ

3.1. Пароль – это персональное средство аутентификации, не подлежащее передаче третьим лицам.

3.2. Все пароли пользователей, а также системные пароли должны соответствовать данной Политике.

3.3. Требования к паролям:

3.3.1. минимальная длина – не менее 8 символов;

3.3.2. должны включать следующие категории: прописные буквы, строчные буквы, цифры, специальные символы;

3.3.3. не должны являться часто употребляемыми словами; содержать фамилию, кличку животного, имена друзей, сотрудников, вымышленных персонажей и т. д. на любом языке, диалекте, сленге, жаргоне и т.д.

3.3.4. не должны содержать компьютерные термины и названия, команды, названия сайтов, организаций, оборудования, программного

обеспечения; содержат даты рождения и иную личную информацию, например, адреса и номера телефонов; слово или число по шаблону типа аааббб, qwerty, zyxwvuts, 12345 и т.д.

ГЛАВА 4
ПОРЯДОК ИСПОЛЬЗОВАНИЯ И ИЗМЕНЕНИЯ ПАРОЛЕЙ

4.1. Первичный пароль, полученный пользователем, подлежит обязательной смене при первом входе в систему, почтовый ящик.

4.2. Пользователь обязан обеспечивать конфиденциальность своего пароля и принимать меры по предотвращению его компрометации.

4.3. Рекомендуемый срок действия пароля – не более 90 календарных дней, если иное не установлено внутренними документами или техническими возможностями системы.

4.4. Пароль подлежит немедленной смене в случае подозрения на его компрометацию; выявления факта несанкционированного доступа; по требованию администратора.

ГЛАВА 5
ЗАПРЕТЫ И ОГРАНИЧЕНИЯ

5.1. Пользователям запрещается:

5.1.1. передавать свои пароли другим лицам; использовать один и тот же пароль для доступа к ИС, ИР, внешним ресурсам;

5.1.2. записывать пароли в открытом виде (на бумаге, в файлах без защиты и т.п.), хранить on-line;

5.1.3. передавать пароли при помощи почтовых сообщений либо иным другим открытым способом через Интернет;

5.1.4. использовать ранее применявшиеся в ИС и ИР пароли и пароли, используемые для личных целей (соцсети, email и т.д.).

ГЛАВА 6
ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЕЙ

6.1. Пользователь обязан:

6.1.1. соблюдать требования настоящей Политики;

6.1.2. использовать пароли в соответствии с установленными требованиями;

6.1.3. незамедлительно информировать администратора или ответственное лицо о компрометации или утрате пароля;

6.1.4. проходить инструктажи и обучение по вопросам информационной безопасности.

ГЛАВА 7
ОБЯЗАННОСТИ АДМИНИСТРАТОРОВ И ОТВЕТСТВЕННЫХ ЛИЦ

7.1. Администраторы информационных систем обязаны:

7.1.1. обеспечивать реализацию технических мер по защите паролей;

7.1.2. не допускать хранения паролей в открытом виде;

7.1.3. обеспечивать контроль соблюдения требований настоящей Политики;

7.1.4. при необходимости блокировать учётные записи пользователей.

7.2. Ответственное лицо за информационную безопасность обеспечивает актуализацию настоящего Политики и контроль ее исполнения.

ГЛАВА 8
ОТВЕТСТВЕННОСТЬ ЗА СОБЛЮДЕНИЕ ПОЛОЖЕНИЙ ПОЛИТИКИ

8.1. Пользователи несут персональную ответственность за конфиденциальность своих паролей.

8.2. Неисполнение или некачественное соблюдение пользователями информационных систем настоящей положений настоящей Политики может повлечь лишение доступа к информационным системам, а также применение к виновным административных мер воздействия, степень которых определяется установленным в Университете порядком либо требованиями действующего законодательства.

ГЛАВА 9
ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛИТИКИ

9.1. Контроль соблюдения требований настоящей Политики осуществляется в рамках системы внутреннего контроля (аудита) и мероприятий по обеспечению информационной безопасности.

9.2. Внесение изменений в настоящую Политику осуществляется на периодической и внеплановой основе:

9.2.1. периодическое внесение изменений в настоящую Политику должно осуществляться не реже одного раза в 12 месяцев;

9.2.2. внеплановое внесение изменений в настоящую Политику может производиться по результатам анализа инцидентов информационной безопасности, актуальности, достаточности и эффективности используемых мер обеспечения информационной безопасности, результатам проведения внутренних аудитов информационной безопасности и других контрольных мероприятий.

9.3. Ответственным за внесение изменений в настоящую Политику является начальник Центра информационных технологий.