МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВАСТОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
Временно исполняющий обязанности ректора
_____Д.В. Ярыгин
«__» _____ 20__ г.
№ 29-02-13/30
к приказу
от 07.05.2026 № 1073-п

ПАРОЛЬНАЯ ПОЛИТИКА

ФГАОУ ВО «Севастопольский государственный университет»

Севастополь

Содержание

1. Общие положения

1.1. Настоящая Парольная политика (далее – Политика) устанавливает единые требования к созданию, использованию и хранению паролей для доступа к информационным системам федерального государственного автономного образовательного учреждения «Севастопольский государственный университет» (далее – Университет) в целях обеспечения конфиденциальности, целостности и доступности информации.

1.2. Пароли обеспечивают защиту учетных записей пользователей. Неправильно выбранный пароль повышает потенциальный риск несанкционированного доступа к информационным системам.

1.3. Настоящая Политика распространяется на все элементы информационных систем и структурные подразделения Университета, а также на третьих лиц, использующих и/или обслуживающих информационные системы Университета.

1.4. Нормативная база.

Политика разработана в соответствии с:

– Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

– Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

– Приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

– Приказом ФСТЭК России от 11.04.2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений»;

– Методическим документом ФСТЭК России от 11.11.2025 «Методика оценки показателя состояния технической защиты информации в информационных системах и обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

1.5. Основные цели:

– обеспечение конфиденциальности персональных данных и иной информации, размещенных в информационных системах Университета;

– защита информационных систем от несанкционированного доступа;

– предотвращение возникновения событий, влекущих за собой различные виды ущерба, которые могут произойти в результате компрометации паролей учетных записей ИТ-инфраструктуры Университета;

– создание единых и обязательных для исполнения правил обработки и применения паролей.

Дирекция правового обеспечения и внутреннего контроля
А.В. Аброськин

1.6. В настоящей Политике используются следующие аббревиатуры, термины и определения:

Пользователь (владелец учётной записи) – физическое лицо, которому на законных основаниях предоставлено право доступа к информационным ресурсам, информационным системам, сервисам или данным организации с использованием учетной записи (учетных данных).

ОЗИ – Отдел защиты информации Дирекции информатизации и связи.

Административные пароли – пароли локальных администраторов, администраторов домена, администраторов приложений и активного сетевого оборудования, администраторов информационных систем.

Технологические пароли – пароли технологических, системных, служебных учетных записей и учетных записей администраторов.

Учетная запись – цифровой идентификатор пользователя или системы, состоящий из двух ключевых элементов: логин (уникальное имя для распознавания) и пароль или иной секретный ключ (для подтверждения прав на доступ).

ПО – программное обеспечение.

АРМ – автоматизированное рабочее место.

Аутентификация – процесс проверки личности пользователя или подлинности устройства при доступе к системе, сервису или данным.

Стойкие методы аутентификации – методы, которые обеспечивают высокий уровень безопасности, предотвращают несанкционированный доступ к ресурсам или данным. Виды стойких методов аутентификации: парольная, биометрическая, токенная, криптографическая и двухфакторная аутентификация.

2. Регламент парольной защиты

2.1. Основные положения

2.1.1. Все учетные записи (включая системные; служебные; учетные записи пользователей, учетные записи пользователей, имеющие административные привилегии, и администраторов) в системном и прикладном программном обеспечении, а также системы и средства защиты информации (включая доступ к BIOS и к управлению персональными межсетевыми экранами и антивирусным программным обеспечением) должны быть защищены стойкими методами аутентификации.

2.1.2. Пароль является средством защиты от несанкционированного доступа к информации или к средствам ее обработки, хранения, передачи и эффективен только при правильном его использовании.

Дирекция правового обеспечения
и внутреннего контроля
А.В. Аброськин

2.1.3. В информационных системах, в базах данных, на серверах, в других системах и устройствах Университета должны быть задействованы (при наличии технической возможности) механизмы, реализующие принудительное исполнение пользователями требований настоящей парольной политики:

- ограничения на минимальную длину пароля;

- периода действия пароля;

- запрета на повтор недавно используемых паролей;

- проверки паролей на сложность;

- блокирования учетной записи при превышении установленного числа попыток неправильного ввода пароля;

- обязательной смены пароля, установленного пользователю администратором системы, при первой регистрации пользователя в системе.

2.1.4. В случае отсутствия технической возможности выполнения требований пункта 2.1.3 Политики – должны применяться компенсирующие меры:

- проведение регулярных аудитов – проверка учётных записей на предмет использования слабых паролей (если есть доступ к хешам) или признаков компрометации;

- ручной анализ логов (администратор вручную просматривает компьютерный журнал (лог), куда записываются все попытки входа. Если он видит много ошибок ввода пароля подряд, он сам блокирует подозрительную учётную запись);

- памятки-инфографики (стикеры или обои) – визуальные напоминания правил безопасности, размещенные прямо на рабочих местах или экранах компьютеров.

2.1.5. Учётные записи могут быть индивидуальными и коллективными. Индивидуальная учётная запись принадлежит только одному пользователю и применяется для разграничения доступа в многопользовательских системах, а также для доступа к ресурсам индивидуального пользования. Коллективная – принадлежит нескольким пользователям, объединяемым в соответствующую группу, и применяется в многопользовательских системах для доступа к общим ресурсам и в системах с одной технически возможной учетной записью, если требуется обеспечить доступ к системе нескольких пользователей.

Дирекция правового обеспечения
и внутреннего контроля
А.В. Аброськин

2.1.6. Классификация по типу учетной записи:

– системные учетные записи – учетные записи, создаваемые и используемые операционной системой, службами, базовым ПО (например, СУБД) или виртуальными средами для функционирования и взаимодействия внутренних компонентов;

– служебные (функциональные) учетные записи – учетные записи, создаваемые администратором для запуска и работы конкретных прикладных служб, задач или процессов. Эти записи закреплены не за конкретным пользователем, а за функцией.

– учетные записи пользователей – учетные записи, однозначно идентифицирующие конкретное физическое лицо (в случае «индивидуальной учетной записи») или группу физических лиц (в случае коллективной учетной записи) в информационной системе для выполнения им своих трудовых или договорных функций;

– учетные записи пользователей, имеющие административные привилегии – подмножество учетных записей пользователей, которым в рамках их должностных обязанностей делегированы расширенные права в одной или нескольких информационных системах (например, права на установку ПО, управление сетевыми ресурсами, настройку параметров безопасности, управление другими учетными записями);

– учетные записи администраторов – специальные встроенные или предопределенные учетные записи, имеющие неограниченные (полные) права на управление всей информационной системой, ее компонентами или сетевым оборудованием (могут быть как коллективными, так и индивидуальными).

2.1.7. Типы паролей

2.1.7.1. По сроку действия:

- первоначальный (одноразовый) пароль – это пароль, устанавливаемый администратором или системой для выдачи пользователю (владельцу) учетной записи (не предназначен для постоянного использования, подлежит замене при первом входе);

- пароль (с ограниченным сроком действия) – пароль, применяемый при работе во всех информационных системах, а также с любым оборудованием. Частота смены таких паролей определена в разделе 2.4 настоящей Политики.

2.1.7.2. По функциональной принадлежности:

- пользовательские пароли – пароли учетных записей пользователей;

Дирекция правового обеспечения
и внутреннего контроля
А.В. Аброськин

- административные пароли – пароли локальных администраторов, администраторов домена, администраторов приложений и активного сетевого оборудования, администраторов информационных систем (с максимальными правами в рамках конкретного прикладного программного обеспечения);

- технологические пароли – пароли технологических, системных, служебных учетных записей и учетных записей администраторов, используемых для эксплуатации, настройки и ремонта средств вычислительной техники и ПО, устройств коммуникационной инфраструктуры (маршрутизатор, коммутатор, межсетевой экран, система бесперебойного питания, и т.п.).

2.1.8. Пароли являются конфиденциальной информацией. Запрещается:

- записывать пароли на бумажных носителях и оставлять их на рабочем месте;
- сохранять пароли в открытом виде в текстовых файлах, заметках или браузерах;
- передавать свои учетные данные третьим лицам;
- использовать один и тот же пароль для доступа к разным информационным ресурсам.

2.1.9. Пользователь должен принять все меры для того, чтобы исключить возможность компрометации принадлежащего ему пароля.

2.1.10. Работники Отдела защиты информации (ОЗИ) Дирекции информатизации и связи имеют право осуществлять проверку реализации требований Политики пользователями и администраторами информационных систем путем письменных опросов, запроса сведений. Запрос сведений в письменном виде осуществляется средствами системы электронного документооборота (СЭД) Университета, через служебную записку или через корпоративную электронную почту.

2.2. Генерация паролей

2.2.1. При предоставлении пользователю прав доступа в информационной системе администратор информационных систем Университета устанавливает для него первоначальный пароль, который является уникальным для каждого пользователя.

2.2.2. Первоначальный пароль передается пользователю безопасным способом (лично, через менеджер паролей, зашифрованные архивы и т.д.).

Дирекция правового обеспечения и внутреннего контроля
А.В. Аброськин

2.2.3. При первом входе в систему пользователь обязан сменить первоначальный пароль, заданный администратором с учетом соблюдения требований, указанных в разделе 3 настоящей Политики.

2.2.4. Все пароли, используемые в информационных системах Университета, должны отвечать требованиям сложности, указанными в разделе 3 настоящей Политики.

2.3. Использование паролей

2.3.1. Пользователи обязаны обеспечить конфиденциальность своих паролей (пункт 2.1.8 настоящей Политики). При вводе пароля пользователю необходимо исключить возможность его подсматривания посторонними лицами.

2.3.2. При покидании рабочего места пользователь обязан заблокировать свой компьютер.

2.3.3. Запрещается включение паролей в автоматизированный процесс регистрации (например, с использованием хранимых макрокоманд или функциональных клавиш) без применения дополнительных мер защиты.

2.3.4. Запрещается хранение паролей от ИС Университета в менеджерах паролей браузеров.

2.3.5. При использовании встроенных учетных записей на системных компонентах (серверы, СУБД, сетевое оборудование, средства виртуализации, прикладное программное обеспечение, средства защиты информации и т.п.) запрещено использовать пароли, установленные производителем по умолчанию.

2.3.6. Все пароли должны быть приведены к нечитаемому виду при передаче и хранении на всех системных компонентах с помощью алгоритмов надежной криптографии.

2.3.7. При неоднократных попытках неправильного ввода пароля учетная запись должна блокироваться. При этом разблокировка учетной записи должна выполняться:

- автоматически, но не ранее чем через 15 (пятнадцать) минут после ее блокировки;

- вручную администратором системы.

2.4. Изменение паролей

Дирекция правового обеспечения
и внутреннего контроля
А.В. Аброськин

2.4.1. Срок действия пользовательских паролей и паролей администраторов приложений не должен превышать 90 дней.

2.4.2. Внеплановая смена пользовательского пароля осуществляется в случае выявления факта компрометации пароля. Смена пароля должна производиться немедленно после выявления факта компрометации пароля.

2.4.3. Внеплановая смена пароля администраторов приложений и активного сетевого оборудования осуществляется в случае выявления факта компрометации пароля, а также в случае прекращения полномочий администратора системы (увольнение, переход на другую работу внутри Университета и другие обстоятельства). Смена пароля администраторов приложений и активного сетевого оборудования должна производиться немедленно после выявления факта компрометации пароля или прекращения полномочий администратора.

2.4.4. В случае утраты пароля пользователем пароль может быть изменен администратором системы с соблюдением следующих требований:

- смена пароля учётной записи пользователя администратором осуществляется при личном обращении пользователя с предъявлением документа, подтверждающего личность (пропуска или иного документа), либо обращении руководителя структурного подразделения посредством корпоративной почты. Обязательно прикладывается служебная записка с указанием причины утраты пароля;

- пароль, заданный администратором, передается пользователю согласно требованиям пункта 2.2 настоящей Политики;

- при первом входе в систему пользователь обязан сменить пароль, заданный администратором.

2.4.5. В случае компрометации пароля технологической учетной записи его смена должна быть проведена незамедлительно, новый пароль должен быть передан администраторам систем, использующих данную технологическую запись, безопасным способом в минимально короткие сроки.

3. Требования Парольной политики

3.1. Административные пароли должны соответствовать следующим требованиям:

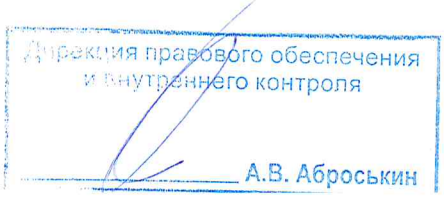
- изменяться не реже, чем 1 раз в 90 дней;
- содержать не менее двенадцати символов;

Дирекция правового обеспечения
и внутреннего контроля
А.В. Аброськин

- не являться словом, которое используется в словарях (русских или иностранных);
- содержать сочетания букв верхнего и нижнего регистров, цифры и спецсимволы:
  - буквы верхнего регистра (А-Я, A-Z);
  - буквы нижнего регистра (а-я, a-z);
  - цифры (0-9);
  - специальные символы (!, », №, %, *, / и др.);
- не содержать персонифицированную информацию (имя, адрес, дата рождения, телефон);
- храниться в зашифрованном виде в базе данных, доступ к которой ограничен;
- учитываться в журнале учета паролей административных учетных записей (далее – Журнал). Журнал является документом строгой отчетности, оформляется как документ «для служебного пользования», хранится в опечатываемом металлическом хранилище Отдела защиты информации.

3.2. Технологические пароли должны соответствовать следующим требованиям:

- содержать не менее пятнадцати символов;
- не являться словом, которое используется в словарях (русских или иностранных);
- содержать сочетания букв верхнего и нижнего регистров, цифры и спецсимволы:
  - буквы верхнего регистра (А-Я, A-Z);
  - буквы нижнего регистра (а-я, a-z);
  - цифры (0-9);
  - специальные символы (!, », №, %, *, / и др.);
- не содержать персонифицированную информацию (имя, адрес, дата рождения, телефон);
- храниться в зашифрованном виде в базе данных, доступ к которой ограничен;
- быть уникальными для каждого устройства.
- срок действия паролей технологических учетных записей не должен превышать одного года. При этом в целях повышения уровня доступности информационных систем Университета не рекомендуется устанавливать технические/программные ограничения срока действия паролей технологических учетных записей.



3.3. Пользовательские пароли должны соответствовать следующим требованиям:

- изменяться не реже, чем 1 раз в 90 дней;
- содержать не менее двенадцати символов;
- не являться словом, которое содержится в словарях (русских или иностранных);
- содержать сочетания букв верхнего и нижнего регистров, цифры и спецсимволы:
  - буквы верхнего регистра (А-Я, A-Z);
  - буквы нижнего регистра (а-я, a-z);
  - цифры (0-9);
  - специальные символы (!, », №, %, *, / и др.);
- не содержать персонифицированную информацию (имя, адрес, дата рождения, телефон);

3.4. Запрещена передача паролей пользователям по телефону, при помощи незащищенных почтовых сообщений либо иным другим открытым способом через Интернет.

3.5. Новый пароль учетной записи не должен совпадать ни с одним из пяти последних применявшихся паролей.

3.6. Если пользователь считает, что его пароль стал известен кому-либо, он должен сменить пароль и сообщить о компрометации руководителю структурного подразделения, администратору информационной системы и на адрес электронной почты: infosec@sevsu.ru.

3.7. Запрещено сообщать свой пароль кому-либо. Если кто-либо требует от пользователя сообщить его пароль, то пользователю необходимо отказать в предоставлении сведений о пароле и сослаться на настоящую Политику или направить требующего в ОЗИ. Исключение составляет запрос/опрос, осуществляемый работниками ОЗИ в соответствии с пунктом 2.1.10 настоящий Политики.

3.8. Работники ОЗИ обязаны не реже 1 раза в квартал проводить выборочные проверки паролей пользователей на стойкость к подбору или взлому для (не менее) трех учетных записей пользователей, подключенных к домену sevsu.lan. Если во время таких мероприятий пароль будет подобран или взломан, учетная запись будет заблокирована. Для разблокировки и смены пароля пользователю необходимо обратиться в Дирекцию информатизации и связи.

4. Ответственность

4.1. Контроль за соблюдением требований настоящей Политики возлагается на директора дирекции информатизации и связи.

4.2. Пользователь (владелец учетной записи) Университета несет персональную ответственность за сохранность своего пароля и его конфиденциальность.

4.3. Пользователи, участвующие в процессах управления паролями, несут ответственность за соблюдение требований настоящей Политики в части возлагаемых на них функциональных обязанностей.

5. Заключительные положения

5.1. Настоящая Политика вступает в силу с момента ее утверждения приказом ректора Университета.

5.2. Настоящая Политика подлежит пересмотру и актуализации не реже одного раза в три года, а также при возникновении инцидентов информационной безопасности или изменении законодательства Российской Федерации.

5.3. Внесение изменений или дополнений в настоящую Политику осуществляется путем подготовки изменений (дополнений) в настоящую Политику либо принятием Политики в новой редакции.

5.4. Изменения или дополнения в настоящую Политику утверждаются приказом ректора Университета.

5.5. Настоящая Политика подлежит регистрации и хранению в составе документов организационного характера номенклатуры дел отдела делопроизводства и архивного обеспечения до замены ее Политикой в новой редакции. Заверенная копия Политики подлежит хранению в Дирекции информатизации и связи.

Дирекция правового обеспечения
...утреннего контроля
А.В. Аброськин