УТВЕРЖДЕНА
приказом ФГАОУ ВО «СПбПУ»
от 28.12.2022 № 3042

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«САНКТ-ПЕТЕРБУРГСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ПЕТРА ВЕЛИКОГО»

ПОЛИТЕХ
Санкт-Петербургский
политехнический университет
Петра Великого

ПАРОЛЬНАЯ ПОЛИТИКА ФГАОУ ВО «СПбПУ»

Санкт-Петербург
2022 г.

Термины и определения

АРМ – автоматизированное рабочее место пользователя (персональный компьютер с прикладным программным обеспечением) для выполнения определенной производственной задачи.

ИР – это совокупность информационных объектов (информации и ее носителей), которые находятся в распоряжении ФГАОУ ВО «СПбПУ» и могут быть использованы для осуществления деятельности ФГАОУ ВО «СПбПУ».

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

Несанкционированный доступ – доступ к информации, нарушающий установленные правила разграничения доступа.

Парольная аутентификация – это процедура проверки подлинности пользователя путём сравнения введённого им пароля (для указанного логина) с паролем, сохранённым в базе данных пользовательских логинов.

Пользователь – физическое лицо, зарегистрированное в информационной системе ФГАОУ ВО «СПбПУ».

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 (support@spbstu.ru, +7 (812) 535-81-08, https://it.spbstu.ru).

Учетная запись пользователя – хранимая в информационной системе совокупность данных о пользователе, необходимая для его аутентификации и предоставления доступа к данным и настройкам. Учетная запись создается администратором при регистрации пользователя в операционной системе компьютера, в системе управления базами данных, в сетевых доменах, приложениях и т.п.

1. Общие положения

1.1. Парольная Политика ФГАОУ ВО «СПбПУ» (далее – Политика) разработана в соответствии с Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и приказом ФСТЭК 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».

1.2. Требования настоящей Политики распространяются на всех работников федерального государственного автономного образовательного учреждения высшего образования «Санкт-Петербургский политехнический университет Петра Великого» (далее – ФГАОУ ВО «СПбПУ»).

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

1.4. Настоящая Политика определяет требования к порядку создания, хранения, использования, смены и другим вопросам, связанным с применением механизмов парольной аутентификации в ИС ФГАОУ ВО «СПбПУ».

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

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

1.7. Политика подлежит регулярному пересмотру с периодичностью один раз в год для приведения парольной защиты в соответствие реальным условиям. Также может

проводиться внеплановый пересмотр при изменении перечня решаемых задач, конфигурации технических и программных средств.

1.8. Контроль за исполнением требований настоящей Политики возлагается на начальника Управления информационной безопасности.

2. Правила создания паролей

2.1. Временный пароль для доступа к ИС ФГАОУ ВО «СПбПУ» предоставляется службой поддержки пользователей при регистрации работника в качестве пользователя ИС ФГАОУ ВО «СПбПУ».

2.2. В течение недели с момента предоставления временного пароля пользователь должен самостоятельно создать новый пароль доменной учетной записи. Для этого необходимо на сайте https://staff.spbstu.ru/ ввести текущий логин и пароль, перейти в раздел «Персональные данные» -> «Учетная запись» и нажать кнопку «Сменить пароль». В случае возникновения вопросов обратитесь в службу поддержки пользователей.

2.3. Длина пароля системных учетных записей (администратора домена, администратора приложений и сетевого оборудования, локального администратора и т.д.) должна составлять не менее двенадцати символов.

2.4. Длина пароля пользовательских учетных записей (работников подразделений, преподавателей, студентов и т.д.) должна составлять не менее восьми символов.

2.5. Пароль должен содержать:

- буквы нижнего регистра (a-z);
- минимум одну букву верхнего регистра (A-Z);
- минимум одну цифру (0-9);
- минимум один специальный символ (!@#$%^&*()_;%:? и др.).

2.6. Пароль не должен содержать:

- имя учетной записи пользователя или какую-либо его часть;
- персональную информацию (имена членов семьи, адреса, телефоны, даты рождения и т.д.);
- последовательности из более чем двух символов, расположенных рядом на клавиатуре (например, 123, qwe и другие);
- одного и того же повторяющегося символа либо повторяющейся комбинации из нескольких символов (например, Ps.9999000);
- словарных последовательностей (например, root, admin, professor, university и т.д.).

2.7. Примеры надежных паролей:

- DAyZr@j^Y3Gw;
- R6&uPpLwMqES;
- Sn0Wy^CiTy^.

2.8. Для некоторых АРМ, сетевого оборудования и ИР могут предъявляться специальные требования по длине и содержанию паролей. Эти требования устанавливаются в иных локальных нормативных актах ФГАОУ ВО «СПбПУ».

2.9. Для автоматического создания паролей могут применяться специальные программные средства. При этом сгенерированные пароли должны удовлетворять всем требованиям, указанным в настоящей Политике.

2.10. Запрещается использование стандартных паролей фирм-производителей, предназначенных для доступа к системным ресурсам, серверам, АРМ и активному сетевому оборудованию.

2.11. Запрещается создавать общие пароли совместно с другими пользователями.

3. Правила хранения паролей

3.1. Администратор должен обеспечить хранение паролей в базе данных в зашифрованном виде, доступ к которой ограничен.

3.2. Пользователь должен принимать все меры для того, чтобы исключить возможность компрометации принадлежащего ему пароля.

3.3. Запрещается хранить пароли в файлах, электронных записных книжках, облачных заметках, сохраненных сообщениях в мессенджерах.

3.4. Запрещается хранить пароли на бумажных и других материальных носителях информации, доступ к которым есть у других лиц.

4. Правила использования паролей

4.1 Администратор должен обеспечить автоматическую блокировку доменных учетных записей после пяти неудачных попыток ввода пароля. Последующая разблокировка доменной учетной записи должна производиться автоматически не менее чем через 15 минут.

4.2. Запрещается использовать пароль доменной учетной записи на сторонних ресурсах.

4.3. При вводе пароля необходимо исключить возможность его просмотра посторонними лицами или техническими средствами (фото-, видеокамеры, веб-камеры, презентации экрана и другие средства).

4.4. Запрещается сообщать пароль от учетной записи кому-либо, включая родственников, коллег, руководителей по телефону, по электронной почте или с использованием иных средств передачи информации.

4.5. Запрещается допускать кого-либо к работе под своей учетной записью.

4.6. Администратор должен производить проверку надежности паролей доменных учетных записей не реже чем один раз в год.

5. Правила смены паролей

5.1. Пользователи ФГАОУ ВО «СПбПУ» должны иметь возможность изменения паролей.

5.2. Стандартные пароли фирм-производителей, предназначенных для доступа к системным ресурсам, серверам, АРМ и активному сетевому оборудованию должны быть изменены.

5.3. Пароли системных учетных записей (администратора домена, администратора приложений и сетевого оборудования, локального администратора и т.д.) должны меняться не реже чем один раз в шесть месяцев.

5.4. Пароли пользовательских учетных записей (работников подразделений, преподавателей, студентов и т.д.) должны меняться не реже чем один раз в год.

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

5.6. При смене пароля новое значение должно отличаться от предыдущего не менее чем на пять символов.

5.7. В случае компрометации или утери пароля незамедлительно должно проводиться его внеплановое изменение. При этом пользователь должен обратиться в службу поддержки пользователей и сообщить о факте компрометации или утери пароля.

5.8. В случае обнаружения утечки доменных учетных данных служба технической поддержки выполняет изменение пароля и информирует пользователя об изменениях.

6. Правила прекращения действия паролей

6.1. Прекращение действия пароля возможно при истечении срока его действия, внеплановой смене, компрометации, утере либо удалении учетной записи.

6.2. В случае прекращения полномочий пользователя, в том числе увольнения, перехода на другую работу, в обязательном порядке производится удаление его учетной записи и пароля немедленно после окончания последнего сеанса работы данного пользователя с системой.

6.3. При прекращении полномочий пользователей не допускается сохранение или передача другим пользователям их учетных записей и паролей.

6.4. Запрещается разглашение паролей после прекращения их действия.

7. Ответственность

7.1. Начальник Управления информационной безопасности ФГАОУ ВО «СПбПУ» несет ответственность за:

- разработку положений, инструкций, форм служебных записок (заявок) по процессам организации парольной защиты;
- планирование мероприятий по парольной защите;
- анализ состояния парольной защиты;
- контроль соблюдения требований к организации парольной защиты;
- проведение служебных проверок по фактам утечки и компрометации учетных данных пользователей;
- проведение разъяснительных и консультационных работ с пользователями ИС в части создания, изменения, использования и хранения паролей;
- разработку предложений о совершенствовании парольной защиты.

7.2. Ответственные за информационную инфраструктуру в подразделениях и институтах ФГАОУ ВО «СПбПУ» несут ответственность за исполнение требований, установленных настоящей Политикой, в зоне своей ответственности.

7.3. Работники ФГАОУ ВО «СПбПУ» несут персональную ответственность за исполнение требований, установленных настоящей Политикой.