TOMSK POLYTECHNIC UNIVERSITY
ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

Министерство науки и высшего образования Российской Федерации
федеральное государственное автономное
образовательное учреждение высшего образования
«Национальный исследовательский Томский политехнический университет» (ТПУ)

ПРИКАЗ

29.03.2024 № 89-1/од

Об утверждении Политики обеспечения безопасности информации при управлении парольной информацией

Во исполнение Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»:

1. Утвердить «Политику обеспечения безопасности информации при управлении парольной информацией» в соответствии с приложением и ввести в действие с даты регистрации приказа.
2. Начальнику отдела делопроизводства Ильиных Е.В. довести настоящий приказ до сведения руководителей структурных подразделений
3. Контроль за исполнением настоящего приказа оставляю за собой.

Проректор по цифровизации К. Г. Квасников

Е.А. Недоспасова
вн. 2118

3449788

Приложение к приказу ТПУ
от 29.03.2024 № Б9-1/од

Дата введения «29.03» 2024 2024

ПОЛИТИКА
ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ПРИ УПРАВЛЕНИИ ПАРОЛЬНОЙ ИНФОРМАЦИЕЙ

Владелец документа:	Отдел информационной безопасности
Регламентируемый вид деятельности/процесс:	Цифровизация

Томск – 2024

1. Общие положения

1.1. Политика обеспечения безопасности информации при управлении парольной информацией федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский Томский политехнический университет» (далее соответственно – Политика, ФГАОУ ВО НИ ТПУ, Университет) представляет собой корпоративную политику информационной безопасности ФГАОУ ВО НИ ТПУ, определяющую нормы по защите парольной информации (далее - пароли) при работе с информационными ресурсами и (или) в информационных системах (далее - ИТ-инфраструктура) Университета, действующие во всех структурных подразделениях Университета.

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

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

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

- определение видов паролей, используемых в Университете;
- определения правил формирования и использования паролей для обеспечения их стойкости;
- определения правил обращения с паролями для соблюдения их безопасности (конфиденциальности).

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

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

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

2. Нормативные ссылки

Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

3. Термины, определения и сокращения

3.1. Термины и определения

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

Аутентификация – процедура проверки подлинности лица путём сравнения введённого им пароля с паролем, сохранённым в базе данных учетных записей ИТ-инфраструктуры Университета.

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

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

Компрометация пароля – 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 хранится 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 Университета к информационным ресурсам и лежат в основе механизмов аутентификации, используемых при предоставлении доступа в ИТ-инфраструктуре Университета.

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

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. Сокращения

ГИУ – главный информационный узел Университета.

ОИБ – отдел информационной безопасности Университета.

НСД – несанкционированный доступ.

ФГАОУ ВО НИ ТПУ - федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский Томский политехнический университет».

4. Область действия

4.1. Политика обязательна к применению всеми лицами, являющимися сотрудниками или обучающимися ФГАОУ ВО НИ ТПУ и для которых в Университете

создана учетная запись в ИТ-инфраструктуре.

4.2. В случае создания учетной записи Университета для лиц, не являющимися сотрудниками или обучающимися ФГАОУ ВО НИ ТПУ, Политика предоставляется для ознакомления при выдаче пароля сотрудниками ГИУ.

5. Правила обеспечения безопасности информации при управлении парольной информацией

5.1. Все лица, создающие, передающие, получающие и использующие пароли, должны выполнять установленные Политикой требования.

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

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

5.4. В Университете используются следующие виды паролей:

Пользовательские (условно-постоянные) – создаются уполномоченными сотрудниками ГИУ, передаются пользователям (владельцам учетной записи) способом, исключающим их компрометацию, и действуют в течение установленного срока действия пароля в соответствии с правилами создания и использования паролей.

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

5.5. В Университете действуют следующие общие правила использования паролей:

- пользовательский (условно-постоянный) пароль может быть самостоятельно изменен пользователем досрочно (до истечения установленного срока действия);
- пароль администратора может быть изменен пользователем досрочно (до истечения установленного срока действия), для смены пароля администратора необходимо обратиться в ГИУ.

5.6. После окончания срока действия пользовательского (условно-постоянного) пароля или пароля администратора учетная запись пользователя автоматически блокируется и для восстановления доступа к информационной системе или сервису пользователю необходимо обратиться в ГИУ.

5.7. В Университете организуется контроль выполнения установленных Политикой требований. Контроль проводится ОИБ на периодической основе либо по распоряжению проректора по цифровизации Университета.

6. Правила создания и использования паролей

6.1. 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.

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

Таблица 1

Установленное требование	Описание требования	Правила	
		Пользовательский пароль	Пароль администратора
к минимальной длине пароля	минимальное количество символов, требуемое системой при создании пароля	не менее 13	не менее 13
к максимальной длине пароля	максимальное количество символов, ограниченное системой при создании пароля	не более 64	не более 64
к сложности пароля	обязанность использования определенных символов при создании пароля	заглавные и строчные буквы латинского алфавита, цифры и специальные символы	заглавные и строчные буквы латинского алфавита, цифры и специальные символы
к сроку действия пароля	максимальный срок действия пароля (при истечении требуется замена пароля)	не более 365 дней[1]	Не более 365 дней[2]

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

---

[1] Заложено в пароль при генерации.

[2] Для отдельных информационных систем в инструкциях или локальных нормативных актах может устанавливаться иной срок действия пароля (90 или 120 дней) в зависимости от требований по обеспечению безопасности персональных данных.

6.3.1. Необходимо использовать сочетание букв верхнего и нижнего регистров латинского алфавита (например, aZ, Az);

6.3.2. При использовании цифр необходимо использовать цифры из диапазона от 0 до 9;

6.3.3. При использовании специальных символов возможно использовать символы из следующего набора: Blank space @ # $ % ^ & * _ ! + = { } | : , . ? ` ~ ( ) ; < > .

6.3.4. Пароль не должен являться словом на любом языке, диалекте, сленге, жаргоне, которое, в том числе:

- может содержаться в словарях (русских или иностранных);
- основано на персональной информации пользователя (например, фамилии, дате рождения, номерах СНИЛС или ИНН, адреса или номера телефонов);
- содержит фамилию или имена друзей, сотрудников, вымышленных персонажей, кличку животного и т. д.;
- содержит компьютерные термины или названия, команды, названия сайтов, компаний, оборудования, программного обеспечения;
- содержит возможные названия ФГАОУ ВО НИ ТПУ или географические наименования, например, "Tomsk", "Moscow" или их производные;
- слово или число по шаблону типа «aaabbb», «QwertY», «zyxwvuts», «12345» и т.п.

7. Правила обращения с паролями

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

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

7.3. Пользователям запрещается:

7.3.1. Сообщать (передавать) личный пароль другим лицам, включая работников Университета;

7.3.2. Озвучивать личный пароль голосом, в том числе находясь рядом с другими лицами;

7.3.3. Сообщать кому-либо информацию о своих правилах формирования пользовательского (условно-постоянного) пароля;

7.3.4. Указывать личный пароль в анкетах или различных «опросниках»;

7.3.5. 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;

7.3.6. Хранить пароль в файле в облачном сервисе, на компьютере, включая переносной, без использования шифрования.

7.4. При подозрении на компрометацию пароля пользователь должен прекратить использовать этот пароль и сменить его самостоятельно или при помощи службы технической поддержки Университета.

7.5. Если пользователь в силу исполнения должностных обязанностей выполняет работы по администрированию информационных систем, то он должен:

7.5.1. Использовать для этого пароли, отличающиеся от его обычных пользовательских паролей;

7.5.2. При создании пароли должны передаваться (сообщаться) только пользователю, для которого этот пароль создан. Запрещается передавать (сообщать) пароли через других работников Университета или каких-либо других третьих лиц.

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

8. Документы, регламентирующие деятельность по управлению парольной информацией

8.1. Для организационной поддержки положений Политики в Университете разрабатываются и вводятся в действие регламенты деятельности по обеспечению безопасности информации при управлении парольной информацией для определения границ зон ответственности участников процессов.

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

9. Ответственность

9.1. 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 ФГАОУ ВО НИ ТПУ.

10. Исключения

10.1. Отдельные особенности применения Политики, при наличии уважительной причины к отклонению от ее условий, должны быть согласованы с ОИБ Университета посредством направления служебной записки на имя проректора по цифровизации ФГАОУ ВО НИ ТПУ в системе электронного документооборота либо установлены в отдельном локальном нормативном акте.

Лист согласования документа 'Локальный нормативный акт 3449787 (27.03.2024)'

Краткое содержание : Политика обеспечения безопасности информации при управлении парольной информацией. Цифровизация. Политика. Действует с даты регистрации. Вводится впервые.

Ведущий эксперт (ОО УЦ)	согласен	27.03.2024 09:36	Недоспасова Е.А.

Исполнитель: Недоспасова Е.А. (вн. тел. 2118)

3449787

Лист согласования документа 'Приказ 3449788 (27.03.2024)'

Краткое содержание : Политика обеспечения безопасности информации при управлении парольной информацией. Цифровизация. Политика. Действует с даты регистрации. Вводится впервые.

Проректор по цифровизации (УЦ)	согласен	29.03.2024 11:24	Квасников К.Г.
и.о. Начальника отдела (ЮО)	согласен	29.03.2024 09:39	Сон Д.В.
Ведущий юрисконсульт (ЮО)	согласен	28.03.2024 10:55	Крупская И.А.
Ведущий юрисконсульт (ЮО)	делегировано (с замечаниями)	Замечания : Делегировано Крупская И.А. 28.03.2024 09:49	Воробьева Е.И.
Проректор по режиму и безопасности (РиБ)	согласен	27.03.2024 17:41	Карташов А.А. (Боровков И.Л.)
Начальник отдела (ОИБ)	согласен	27.03.2024 16:15	Корнилкин С.В.
Начальник отдела (ОД)	согласен	27.03.2024 15:15	Ильиных Е.В. (Реутова Н.Ю.)
Ведущий эксперт (ЦК)	согласен	27.03.2024 13:58	Яблокова С.А.
Директор (ЦК)	делегировано (с замечаниями)	Замечания : Делегировано Яблокова С.А. 27.03.2024 09:40	Каргина Е.Б.

Исполнитель: Недоспасова Е.А. (вн. тел. 2118)

3449788