Приложение № 3
к приказу ООО «Техно-Телеком»

от 02.10.2024 № 33

ПОЛОЖЕНИЕ
по организации парольной защиты в ООО «Техно-Телеком»

1. Общие положения

1.1. Настоящее Положение разработано в соответствии с требованиями:

- Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных»;

- постановления Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- приказа ФСТЭК России от 18.02.2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке и информационных системах персональных данных».

1.2. С целью ограничения доступа к информационным ресурсам и системам ООО «Техно-Телеком» (далее – Общество) устанавливается единая система установки паролей.

Настоящее Положение регламентирует организационно-техническое обеспечение процессов создания, изменения, блокирования, удаления учетных записей, процессов генерации, использования, изменения и прекращения действия паролей в Обществе, меры обеспечения безопасности при использовании учетных записей и паролей, а также ответственность работников Общества (далее – пользователи).

1.3 Требования настоящего Положения распространяются на всех пользователей, использующих в работе средства вычислительной техники и должны применяться для всех средств вычислительной техники, эксплуатируемых в Обществе.

1.4. В настоящем Положении используются следующие термины и определения:

Локально-вычислительная сеть (ЛВС) – комплекс оборудования и программного обеспечения, обеспечивающий передачу, хранение и обработку информации.

Автоматизированное рабочее место (АРМ) – комплекс средств вычислительной техники и программного обеспечения, предназначенный для выполнения определенных задач, приобретено на средства Общества и состоящий на бухгалтерском учете.

Автоматизированная система (АС) – система, состоящая из персонала, комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Информационная безопасность (ИБ) – состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз.

Несанкционированный доступ – доступ субъекта к информации в нарушение установленных в системе правил разграничения доступа.

Учетная запись – информация о пользователе: имя пользователя, его пароль, права доступа к ресурсам и привилегии при работе в системе. Учетная запись может содержать дополнительную информацию (адрес электронной почты, контактный телефон и т.п.).

Принцип минимальных привилегий – принцип, согласно которому «каждому субъекту системы предоставляется минимальный набор полномочий (или минимальный допуск), необходимый для выполнения возложенных задач. Применение этого принципа ограничивает ущерб, наносимый субъектом в случае случайного, ошибочного или несанкционированного использования.

Компрометация – факт доступа постороннего лица к защищаемой информации, а также подозрение на него.

Ключевой носитель – электронный носитель (token, флэш-накопитель, компакт-диск и т.п.), на котором находится ключевая информация (сертификаты, ключи, пароли и т.п.).

Учетные записи с ограниченными правами – любые учетные записи, не принадлежащие к группе администраторов и не обладающие повышенными привилегиями, используются работниками подразделений.

Временные учетные записи – учетные записи с ограниченными правами и ограниченные по времени действия, используются работниками подразделений, которым необходимо получить временный доступ к ресурсам ЛВС, либо лицами, не являющимися работниками Общества.

Привилегированные учетные записи – любые учетные записи обладающие полномочиями администратора, используются для управления работой АРМ и (или) ЛВС Общества.

Служебные учетные записи – учетные записи, которые не соответствуют реальному человеку, используются службами или приложениями для доступа к ресурсам, необходимым для выполнения их функций.

2. Правила формирования учетных записей и паролей

2.1. Организационно-техническое обеспечение процессов создания, изменения, блокирования, удаления учетных записей и процессов генерации, использования, изменения и прекращения действия паролей в ЛВС возлагается на отдел безопасности и режима.

2.2. Создание, изменение, блокирование, удаление учетных записей Общества производится отделом безопасности и режима на основании кадровых документов (приказ о приеме на работу, увольнении, переводе, отпуске).

2.3. Каждый пользователь получает свое имя учетной записи, которое составляется работниками отдела безопасности и режима (далее – администратор ЛВС) и доводится пользователю.

По умолчанию пользователям создаются учетные записи с ограниченными правами, с доступом к АРМ и ЛВС Общества, корпоративной электронной почте, общим сетевым ресурсам Общества, общим сетевым ресурсам подразделения, личной сетевой папке пользователя.

Изменение привилегий учетных записей производится отделом безопасности и режима в соответствии с Положением о порядке предоставления доступа к информационным ресурсам.

2.4. Пароли для учетных записей с ограниченными правами первоначально формируются администратором ЛВС, а в дальнейшем выбираются пользователями самостоятельно, с учетом требований настоящего Положения.

2.5. Пароли для учетных записей, используемых для удаленного подключения, служебных и привилегированных учетных записей формируются работниками отдела безопасности и режима с учетом требований настоящего Положения и установкой параметра «Запретить смену пароля пользователем».

2.6. Имя пользователя и индивидуальный пароль являются идентификатором пользователя в ЛВС.

2.7. Для авторизации в ЛВС пользователь обязан ввести свое имя пользователя и набрать индивидуальный пароль, после чего он получает доступ к предоставленным ему ресурсам.

2.8. С целью контроля над реализацией прав доступа пользователей к информационным ресурсам Общества должно быть организовано ведение аудита ЛВС с использованием встроенных механизмов операционной системы и средств защиты информации.

2.9. Действия пользователей, допущенных к информационным ресурсам Общества могут протоколироваться. Ответственность за уничтожение, изменение информации несет пользователь, под чьим именем операция была зарегистрирована, если в результате расследования не определено конкретное виновное лицо.

2.10. Нарушение пользователями целостности установленного программного обеспечения, а также самовольная установка программ, не предназначенных для выполнения должностных обязанностей, категорически запрещается.

2.11. Пароли учетных записей с ограниченными правами должны выбираться пользователями самостоятельно с учетом следующих требований:

- длина пароля должна быть не менее 8 символов;

- в числе символов пароля обязательно должны присутствовать буквы верхнего и нижнего регистра и цифры, желательно использование специальных символов (@, #, $, &, *, % и т.п.);

- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования рабочих станций, известные названия, жаргонные слова и т.д.), общепринятые сокращения (qwerty, pa$$w0rd, и т.п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетаний букв и знаков, которые можно угадать, основываясь на информации о пользователе;

- пароль не должен быть словом русского либо английского языка, в котором заменены некоторые символы (o->0,s->$, a->@ и т.п.);

- при смене пароля новый пароль должен отличаться от старого не менее, чем двумя символами, расположенными не подряд.

2.12. Пароли учетных записей используемых для удаленного подключения, служебных и привилегированных учетных записей должны выбираться с учетом следующих требований:

- длина пароля должна быть не менее 12 символов;

- в числе символов пароля обязательно должны присутствовать буквы верхнего и нижнего регистра, цифры и специальные символы (@, #, $, &, *, % и т.п.). Исключение составляют АС Общества, в которых использование подобных спецсимволов недопустимо;

- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования рабочих станций, известные названия, жаргонные слова и т.д.), общепринятые сокращения (qwerty, pa$$w0rd, и т.п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетаний букв и знаков, которые можно угадать, основываясь на информации о пользователе;

- пароль не должен быть словом русского либо английского языка, в котором заменены некоторые символы (o->0,s->$, a->@ и т.п.);

- при смене пароля новый пароль должен отличаться от старого не менее, чем четырьмя символами, расположенными не подряд.

3. Правила работы с паролями

3.1. Запрещается записывать пароли на бумаге, в файле, электронной записной книжке, мобильном телефоне и любых других предметах и носителях информации.

3.2. При вводе пароля работник должен исключить произнесение его вслух, возможность его просмотра посторонними лицами и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерами и т.п.).

3.3. Запрещается сообщать свой пароль полностью или частично другим пользователям, запрещается спрашивать или подсматривать пароль других пользователей.

3.4. Запрещается предоставлять доступ в АС Общества под своей учетной записью.

3.5. Запрещается авторизация в АС Общества под учетной записью другого пользователя.

3.6. В случае производственной необходимости (командировка, отпуск и т.п.), при проведении проверочных мероприятий, выполняемых начальником отдела безопасности и режима и требующих знания пароля пользователя, допускается раскрытие значений своего пароля начальнику и работникам отдела безопасности и режима. По окончании указанных мероприятий пользователи самостоятельно производят немедленную смену значений «раскрытых» паролей.

3.7. В случае возникновения нештатных ситуаций, форс-мажорных обстоятельств, а также производственной необходимости использования учетных записей работников (в их отсутствие) допускается изменение их паролей работниками отдела безопасности и режима. В подобных случаях, работники, чьи пароли были изменены, обязаны сразу же после выяснения факта смены своих паролей, установить их новые значения.

3.8. К управлению учетными записями пользователей необходимо подходить исходя из принципа «минимальных привилегий», т.е. пользователь не должен иметь прав доступа, как к локальной системе, так и к ЛВС Общества больше, чем это необходимо ему для выполнения своих должностных обязанностей.

3.9. Плановая смена паролей пользователей проводится регулярно, не реже одного раза в 6 месяцев.

3.10. Внеплановая смена любого пароля пользователя производится:

- по просьбе самого пользователя;

- по требованию работников отдела безопасности и режима.

3.11. В случае прекращения полномочий пользователя (увольнение и т.п.) работниками отдела безопасности и режима производится изменение личного пароля, блокирование или удаление учетной записи пользователя по представлению менеджером по кадрам кадровых документов, после окончания последнего сеанса работы данного пользователя.

3.12. В случае планового отсутствия работника более одного месяца (командировка, отпуск и т.п.) его учетная запись блокируется работниками отдела безопасности и режима по представлению менеджером по кадрам кадровых документов.

3.13. Доменные учетные записи, которые не использовалась более 60 дней, блокируются работниками отдела безопасности и режима.

3.14. Изменение забытого пользовательского пароля производится работниками отдела безопасности и режима на основании обращения пользователя, для учетных записей с ограниченными правами устанавливается параметр «Требовать смену пароля при следующем входе в систему».

3.15. Для предотвращения угадывания паролей, при пятикратном неправильном вводе пароля доменная учетная запись пользователя должна автоматически блокироваться на 20 минут.

3.16. При временном оставлении рабочего места в течение рабочего дня, работник обязан заблокировать АРМ нажатием комбинации клавиш «Win + L», либо «Ctrl + Alt + Delete» и выбрать действие «Заблокировать».

3.17. При возникновении вопросов связанных с использованием учетных записей и паролей, пользователь обязан обратиться к работникам отдела безопасности и режима.

4. Временные учетные записи

4.1. Для предоставления временного доступа к ресурсам ЛВС Организации (для лиц, не являющихся работниками Общества, для работников, которым необходимо получить временный доступ к ресурсам ЛВС, и т.п.) необходимо использовать временные учетные записи.

4.2. Порядок получения временных учетных записей:

- работник Общества через руководителя своего подразделения либо лицо, не являющее работником Общества через доверенное лицо, оформляет заявку «На предоставление доступа к информационным, ресурсам», указав в заявке, что требуемая учетная запись временная и определив временные рамки ее использования;

- заявка направляется начальнику отдела безопасности и режима для рассмотрения;

- временная учетная запись создается работниками отдела безопасности и режима;

- пользователь, получивший временную учетную запись, информируется об ограничениях, связанных с её использованием.

5. Локальные учетные записи

5.1. Локальные учетные записи АРМ Общества (Administrator, Администратор, Guest, Гость) предназначены для служебного использования работниками отдела безопасности и режима при настройке систем и не предназначены для повседневной работы.

5.2. Работникам запрещается создание и использование локальных учетных записей на АРМ Общества и входящих в состав домена, либо в состав какого-либо из его поддоменов.

5.3. Встроенная учетная запись Guest (Гость) должна быть заблокирована на всех АРМ Общества при первоначальном конфигурировании операционной системы.

5.4. Встроенная учетная запись Administrator (Администратор) должна быть заблокирована на всех АРМ Общества при первоначальном конфигурировании операционной системы, либо защищена паролем согласно требованиям настоящего Положения.

5.5. BIOS АРМ Общества должен быть защищен паролем согласно требованиям настоящего Положения.

6. Служебные и привилегированные учетные записи

6.1. При использовании привилегированных учетных записей необходимо руководствоваться принципом «минимальных привилегий», т.е. привилегии администратора должны использоваться только уполномоченным персоналом и только если выполняемая задача требует наличия таких привилегий.

6.2. Запрещается использовать привилегированные учетные записи в повседневной работе, не связанной с необходимостью их использования (установка, конфигурирование, восстановление и т.п. операционной системы и сервисов). В случае необходимости запуска программы с правами администратора, необходимо использовать команду «Run As..», либо «вторичный вход в систему». В случае «вторичного входа в систему», при необходимости оставления АРМ, владелец привилегированной учетной записи должен заблокировать АРМ, либо выполнить выход из системы.

6.3. Учетные записи с привилегиями администратора домена, администратора схемы, администратора предприятия должны использоваться исключительно при установке, конфигурировании, восстановлении входящих в домен серверов и иных действиях, для выполнения которых использование других учетных записей невозможно.

6.4. При развёртывании служб, сервисов и приложений необходимо использовать служебные учетные записи с наименьшими привилегиями необходимыми для их работы. Ниже приведена иерархия наименьших привилегий, в которой приведены используемые службами учетные записи, начиная с наиболее предпочтительных:

- локальная служба;
- сетевая служба;
- уникальная учетная запись локального пользователя;
- уникальная учетная запись пользователя домена;
- локальная система;
- учетная запись локального администратора;
- учетная запись администратора домена.

6.5. Учетные записи с привилегиями администратора домена для служб допускается использовать в исключительных случаях и только на серверах

входящих в группу серверов высокой степени безопасности, на остальных серверах и компьютерах домена должна быть применена групповая политика, ограничивающая использование учетных записей с привилегиями администратора домена для служб.

6.6. В случае прекращения полномочий (увольнение, переход на работу в другое подразделение внутри Общества и другие обстоятельства) работника отдела безопасности и режима, которому по роду работы были предоставлены полномочия по управлению парольной защитой Общества, необходимо внеплановое изменение паролей всех зависящих от него учетных записей.

7. Действия при компрометации пароля

7.1. В случае компрометации личного пароля, пользователь немедленно принимает меры по внеплановому изменению личного пароля и докладывает о факте компрометации администратору ЛВС, непосредственному руководителю и начальнику отдела безопасности и режима (письменно).

7.2. В случае компрометации пароля учетной записи производится смена паролей в объеме, зависящем от полномочий данной учетной записи.

7.3. По всем фактам компрометации паролей проводится служебное разбирательство.

8. Аппаратные средства аутентификации

8.1. Для повышения защиты АРМ Общества от несанкционированного доступа может использоваться двухфакторная аутентификация (по паролю и предмету - далее ключевой носитель информации).

8.2. Каждому пользователю АРМ Общества, для которого предусмотрена двухфакторная аутентификация, выдается персональный ключевой носитель информации, который учитывается в отделе безопасности и режима (однозначное сопоставление ключевого носителя его владельцу).

8.3. Ключевые носители информации маркируются в отделе безопасности и режима (уникальный номер ключевого носителя).

8.4. В случае прекращения необходимости использования персонального ключевого носителя (увольнение работника, прекращение функционирования объекта, на котором носитель использовался для аутентификации и т.п.) информация с данного носителя стирается, либо в случае невозможности его очистки носитель уничтожается.

8.5. Пользователям АРМ Общества категорически запрещается оставлять без личного присмотра, а также передавать другим лицам

персональные ключевые носители, сообщать коды от персонального ключевого носителя, если таковые имеются.

8.6. В случае утраты персонального ключевого носителя пользователь обязан немедленно сообщить об инциденте руководителю своего подразделения и начальнику отдела безопасности и режима. При возникновении подобного инцидента необходимо незамедлительно принять меры для недопущения несанкционированного использования утраченного персонального ключевого носителя.

9. Ответственность

9.1. Работники Общества, нарушившие требования настоящего Положения могут быть привлечены к ответственности в соответствии с действующим законодательством и локальными нормативными актами Общества.

9.2. Форма и степень ответственности определяется исходя из вида и размера ущерба, нанесенного Обществу действиями либо бездействием соответствующего работника.

9.3. Работники Общества несут персональную ответственность за все действия совершенные от имени их учетной записи, если с их стороны не были выполнены требования для предотвращения компрометации учетной записи в соответствии с настоящим положением.

9.4. Отдел безопасности и режима контролируют исполнение работниками Общества требований настоящего Положения.

9.5. О выявленных нарушениях настоящего Положения начальник отдела безопасности и режима докладывает Заместителю генерального директора Общества по безопасности.

9.6. Все пользователи, должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, за разглашение парольной информации и сохранность информации на отведенных ему разделах сервера. Ознакомление осуществляется под роспись в журнале ознакомления.

Начальник отдела безопасности и режима ООО «Техно-Телеком» Б.Б. Бобурченко

СОГЛАСОВАНО
Заместитель генерального директора ООО «Техно-Телеком» Р.Р. Ромашков