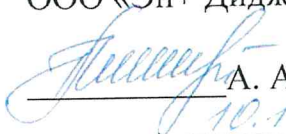


Стандарт предприятия

Управление паролями

Введен впервые

УТВЕРЖДАЮ
Генеральный директор
ООО «Эн+ Диджитал»

 А. А. Герасименко
10.10.2018
(дата)

Введен в действие приказом
ООО «Эн+ Диджитал»
от 08.10.18г. № 23

ООО «Эн+ Диджитал»

Содержание

Содержание	2
Введение	Ошибка! Закладка не определена.
1. Область применения	3
2. Нормативные ссылки	3
3. Сокращения и определения	3
4. Общие положения	3
5. Основные требования	4
6. Обеспечение конфиденциальности паролей	5
7. Контроль	6
8. Ответственность	6
Лист регистрации изменений	8

1. Область применения

1.1. Настоящий стандарт предприятия устанавливает парольную политику ООО «Эн+ Диджитал» (далее Компании).

1.2. Настоящий стандарт предприятия распространяется на всех пользователей информационных систем Компании.

1.3. Настоящий стандарт предприятия входит в состав нормативных документов системы управления Компании.

2. Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие документы:

- СТП 003-2018 «Управление доступом к информационным ресурсам ИС».

3. Сокращения и определения

3.1. В настоящем стандарте используются следующие сокращения:

ИБ - информационная безопасность;

ИТ – информационные технологии;

ИС – информационная система.

3.2. В настоящем стандарте используются следующие определения:

Компания ООО «Эн+ Диджитал», а также партнеры, являющиеся пользователями или администраторами информационных систем ООО «Эн+ Диджитал», подписавшие соответствующие соглашения.

Подразделения ИБ – подразделение (работник), ответственное за контроль обеспечения ИБ Компании, либо организация, осуществляющая такие функции по договору возмездного оказания услуг.

ИТ служба – подразделение (работник) Компании, осуществляющее функции ИТ обеспечения Компании, либо организация, осуществляющая такие функции по договору возмездного оказания услуг.

Пользователи информационной системы – все работники Компании (штатные, временные, работающие по контракту и т.п.), а также все прочие лица (подрядчики, аудиторы и т.п.), зарегистрированные в ИС Компании в порядке, устанавливаемом настоящим стандартом, и получившие права на доступ к информационным ресурсам/системам в соответствии с функциональными обязанностями.

Административный пароль – пароль для административной учетной записи с расширенными привилегиями доступа в информационной системе.

4. Общие положения

4.1. Пароли, предоставляемые работникам для осуществления доступа к информационным ресурсам/системам, лежат в основе всех программно-технических механизмов обеспечения информационной безопасности Компании. Несоблюдение правил выбора, хранения и использования паролей может привести к нарушению конфиденциальности, целостности либо доступности информационных ресурсов и повлечь причинение ущерба Компании.

4.2. Настоящий стандарт устанавливает требования к порядку выбора, хранения, использования, периодичности смены паролей и другим вопросам, связанным с применением механизмов парольной аутентификации в информационных системах Компании.

4.3. Требования настоящего стандарта распространяются на всех пользователей

Компании, зарегистрированных в ИС в установленном порядке и получивших право на доступ к ресурсам корпоративной сети в соответствии с функциональными обязанностями.

4.4. Для отдельных категорий пользователей корпоративной сети могут существовать особые требования по выбору, хранению и использованию паролей. Реализация данных требований осуществляется при наличии технической возможности и согласованию с Подразделением ИБ.

5. Основные требования

5.1. Для регистрации нового работника Компании или подрядной организации необходимо подать в ИТ службу запрос в соответствии с СТП 003-2018 «Управление доступом к информационным ресурсам ИС».

5.2. Пароли для доступа к информационным ресурсам/системам предоставляются пользователям Компании работниками ИТ службы при регистрации этих работников в качестве пользователей корпоративной сети. При получении пароля пользователь обязан произвести замену этого пароля на новый. В дальнейшем пользователь должен осуществлять смену своих паролей самостоятельно в соответствии с требованиями настоящего стандарта.

5.3. Пользователи информационных систем должны производить смену своих паролей не реже, чем раз в квартал. Пользователи системных и административных записей должны согласовать частоту замены паролей с Подразделением ИБ.

5.4. С целью предотвращения несанкционированного доступа к рабочим местам пользователей, а также к ресурсам корпоративной сети с использованием чужих учетных записей (имен пользователей), пользователи обязаны блокировать экраны своих компьютеров в случае оставления ими своего рабочего места нажатием на компьютерной клавиатуре набора клавиш Ctrl+Alt+Del и далее - кнопки «Блокировать компьютер».

5.5. Все выбираемые пользователями пароли должны отвечать приведенным ниже требованиям:

- Содержать три группы символов из четырех: прописные буквы (a-z, а-я), заглавные буквы (A-Z, А-Я), цифры, специальные символы (!@#\$%^&*()_+|~-=\`{}[]:;'\<?.,./)
- Содержать не менее 8 символов, административный пароль не менее 13 символов.
- Имя учетной записи никаким образом полностью или частично не должно входить в состав пароля.
- Пароль не должен являться комбинацией повторяющихся одинаковых символов (zzXXYyYY, XxXx11122).
- Пароль не должен являться группой символов, последовательность расположения которых на клавиатуре легко вычисляется (например, 1234, qWerty, zXc123 и т.п.).
- Не являться персональной информацией (имена членов семьи, адреса, телефоны, даты рождения и т.п.).

5.6. Пользователи могут выбрать легко запоминающиеся пароли, которые в то же время являются трудно угадываемыми для других лиц, т.е. являются сложными, если будет выполнено хотя бы одно из следующих условий:

- Несколько слов написаны слитно (такие пароли известны под названием «passphrases»);
- При наборе слова на клавиатуре использованы клавиши, смещенные относительно нужных на один ряд вверх, вниз, вправо или влево;
- Слово набрано со смещением на определенное количество букв вверх или вниз по алфавиту;
- Комбинация цифр и обычного слова;

- Намеренно неправильное написание слова (но не обычная в данном слове орфографическая ошибка);
- Строчка стиха.

5.7. Запрещается использование пустых паролей и паролей «по умолчанию», назначаемых производителями либо разработчиками ПО и оборудования. Данные пароли должны меняться администраторами в процессе настройки на соответствующие требованиям настоящего стандарта.

5.8. Работники ИТ службы там, где это возможно, должны настраивать в операционных системах и приложениях следующие параметры парольной политики:

- Минимальная длина пароля – 8 символов;
- Пароль должен отвечать требованиям сложности п.п.5.5-5.6;
- Максимальный срок действия пароля – 90 дней;
- Минимальный срок действия пароля – 20 дней;
- Неповторяемость паролей (хранить 20 предыдущих);
- Использование шифрования при хранении паролей;
- Автоматическая блокировка пользовательских учетных записей после 100 неудачных попыток введения пароля. Автоматическая разблокировка пользовательского пароля – 10 мин.

5.9. Работники ИТ службы также осуществляют настройку на рабочих местах пользователей блокирования экранов (при помощи запароленного «хранителя экрана») через 10 минут неактивности пользователя. По согласованию с Подразделением ИБ создают исключения для пользователей, к которым данная блокировка не может быть применена или изменено время блокировки.

6. Выдача паролей

6.1. При регистрации работников в качестве пользователей работниками ИТ службы создаются соответствующие учётные записи и назначаются для них временные пароли. Временные пароли должны отвечать требованиям сложности, определённым в разделе 5 настоящей Политики.

6.2. Временные пароли должны передаваться пользователям безопасным способом, исключающим возможность их (паролей) компрометации. Запрещается передача паролей посредством электронной почты (если только не используется шифрование передаваемых электронных писем) и иных открытых каналов передачи данных, за исключением телефонной связи.

6.3. При передаче временных паролей работники ИТ службы должны уведомлять пользователей о необходимости произвести смену пароля. Если механизмы ИС поддерживают опцию обязательной смены пароля при первом входе в систему, то данная опция должна быть включена.

7. Обеспечение конфиденциальности паролей

7.1. Пользователям запрещается предпринимать какие-либо действия по получению (раскрытию) паролей других пользователей.

7.2. Пользователи обязаны соблюдать необходимые меры предосторожности для обеспечения конфиденциальности своих паролей.

7.2.1 Запрещается:

- Сообщать свой пароль кому-либо, включая коллег, руководителей и специалистов службы технической поддержки, по телефону, по электронной почте или какими-либо иными способами.

– Хранить пароли в доступной для чтения форме в командных файлах, сценариях автоматической регистрации, программных макросах, функциональных клавишах терминала, на компьютерах с неконтролируемым доступом, а также в иных местах, где неуполномоченные лица могут получить к ним доступ. Например, ни в каких приложениях пользователи не должны выбирать такую опцию конфигурации, как автоматическое сохранение пароля.

– Записывать пароли и оставлять эти записи в местах, где к ним могут получить доступ неуполномоченные лица.

– Произносить свой пароль вслух.

– Использовать общие пароли совместно с другими пользователями.

Примечания:

1. Если кто-либо требует от Вас раскрытия пароля, сошлитесь на настоящий стандарт или предложите обратиться за разъяснениями в ИТ службу либо к Менеджеру ИБ.

2. Пароль должен быть немедленно изменен в соответствии с разделом 5, если имеются основания полагать, что данный пароль стал известен кому-либо еще, кроме самого пользователя. Необходимо сообщить Менеджеру ИБ о факте компрометации пароля.

3. Работникам ИТ службы для выполнения ими своих служебных обязанностей, ни при каких обстоятельствах, не требуется знание паролей пользователей. Для этого у них есть все необходимые полномочия. В случае необходимости они произведут смену пароля пользователя и сообщат ему об этом, после чего пользователь обязан произвести его замену в соответствии с разделом 5.

8. Контроль

8.1. Общий контроль выполнения требований настоящего стандарта осуществляется Менеджером ИБ. С целью проверки надежности используемых паролей ими периодически могут осуществляться тестовые «взломы» паролей пользователей. По указанию Менеджера ИБ пользователи должны производить смену паролей, не удовлетворяющих критериям надежности, устанавливаемым настоящим стандартом.

8.2. В случаях, когда выполнение требований п.5.8. невозможно полностью, владелец информационной системы согласует с Менеджером ИБ и ИТ службой реализуемые в ней параметры парольной политики.

9. Ответственность

9.1. Ответственность за осуществление общего контроля выполнения правил настоящего стандарта, а также за поддержание данного документа в актуальном состоянии несут Менеджер ИБ.

9.2. Ответственность за реализацию работниками ИТ службы требований настоящего стандарта, возлагается на руководителя ИТ службы.

9.3. Руководители структурных подразделений Компании несут ответственность за ознакомление под роспись подчиненных сотрудников с настоящим стандартом, а также за выполнение положений настоящего стандарта в подконтрольных им подразделениях.

9.4. Работники несут персональную ответственность за нарушение требований и положений данного стандарта и могут быть привлечены к дисциплинарной ответственности, в соответствии с положениями действующего законодательства Российской Федерации.

Лист согласования**СОГЛАСОВАНО:**

Структурное подразделение, должность	Подпись	Фамилия И.О.	Дата

РАЗРАБОТЧИК:

Должность	Подпись	Фамилия И.О.	Дата
Исполнительный директор		Шевченко Д.А.	

Лист регистрации изменений

[illegible]

¹ Ссылка на документ, разрешающий внесение изменений и содержащий тест изменений.