УТВЕРЖДАЮ

Генеральный директор
ООО «Сатурн»

Соколов А.А.

«___» _____ 2018 г.

СИСТЕМА МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РЕГЛАМЕНТ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

УПРАВЛЕНИЕ ПАРОЛЬНОЙ ЗАЩИТОЙ

[ИБ-202]

(версия 1.1)

2018 г.

Оглавление

1. Введение **3**
2. Область применения **3**
3. Термины, определения и сокращения **3**
4. Требования к паролям **5**
4.1. Общие требования 5
4.2. Требования к политике домена 6
5. Смена паролей **8**
6. Контроль и ответственность **8**

1. Введение

Применение паролей для аутентификации субъектов доступа является одним из базовых механизмов защиты информации в информационных системах.

Под субъектами доступа понимаются как пользователи информационных систем, так и служебные учетные записи, необходимые для функционирования информационных систем. Таким образом, применяются пользовательские и служебные пароли.

Пароль относится к сведениям конфиденциального характера и должен сохраняться в секрете.

2. Область применения

Настоящий регламент определяет организационно–техническое обеспечение процессов генерации, смены и прекращения действия паролей в информационных системах и системах обработки информации в Компании, а также контроль за действиями пользователей и обслуживающего персонала при работе с паролями.

Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах автоматизированных систем, контроль за действиями исполнителей и обслуживающего персонала систем при работе с паролями возлагается на пользователей и администраторов соответствующих информационных систем.

Настоящий регламент предназначен для применения сотрудниками Компании во всех предприятиях и структурных подразделениях, использующих средства информатизации и информационные системы. Все работники Компании должны быть ознакомлены с настоящим регламентом.

3. Термины, определения и сокращения

Администратор ИС	Непосредственно обеспечивает настройку и администрирование ИС на прикладном и/или системном уровне. Взаимодействует с администраторами Департамента по ИТ Компании осуществляющими администрирование ИС на системном уровне.
АРМ	Автоматизированное рабочее место пользователя (персональный компьютер с прикладным ПО) для выполнения определенной производственной задачи
Владелец ИС	Лицо, выполняющее роль заказчика конкретной ИС со стороны руководства Компании. Владелец ИС отвечает за эксплуатацию ИС перед руководством Компании, утверждает регламент использования ИС, уполномочен размещать запросы на ввод в эксплуатацию ИС, разработку, доработку, внедрение подсистем и сервисов, необходимых для решения задач бизнес-процессов

	компании.
ИБ	Информационная безопасность – комплекс организационных и технических мероприятий, обеспечивающих конфиденциальность, целостность и доступность информации
ИС	Информационная система – система, обеспечивающая хранение, обработку, преобразование и передачу информации с использованием вычислительной техники
ИСПДН	Информационная система персональных данных – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств
ИТ	Информационные технологии – совокупность методов и процессов, обеспечивающих хранение, обработку, преобразование и передачу информации с использованием средств вычислительной техники
Ответственный за эксплуатацию ИС	Обеспечивает функционирование ИС и отвечает за ее эксплуатацию перед Владельцем ИС. Организует работу Администратора ИС, взаимодействие с Департаментом ИТ Компании, пользователями ИС и другими заинтересованными сторонами.
Пароль	Идентификатор субъекта доступа, который является его (субъекта) секретом
ПДн	Персональные данные
ПК	Персональный компьютер
ПО	Программное обеспечение
Пользователь	Работник Компании, использующий ресурсы информационной системы для выполнения своих должностных обязанностей
Право на доступ	Совокупность правил, регламентирующих порядок и условия доступа пользователя ИС к ее ресурсам
Привилегия на доступ	Исключительное право на доступ к ресурсам ИС
Реестр	Документ «Реестр разрешенного к использованию ПО». Содержит перечень коммерческого ПО, разрешенного к

	использованию в Компании
Ресурс	Все, что имеет ценность для Компании
СВТ	Средства вычислительной техники
СМИБ	Система менеджмента информационной безопасности
Субъект доступа	Лицо или процесс, действия которого регламентируются правилами разграничения доступа
Третья сторона	Лицо или организация, считающаяся независимой по отношению к Компании
Учетная запись	Информация о пользователе ИС: имя пользователя, его пароль, права доступа к ресурсам и привилегии при работе в системе. Учетная запись может содержать дополнительную информацию (адрес электронной почты, телефон и т.п.)

4. Требования к паролям

4.1. Общие требования

Личные пароли доступа к информационным системам, ресурсам организации и ресурсам АРМ сотрудников Компании должны формироваться и распределяться с учетом следующих требований:

- идентификаторы пользователей и их пароли должны быть уникальными для каждого пользователя;
- пароли должны состоять как минимум из 6 символов (не должны быть именами или известными фразами);
- длина паролей для администраторов серверов, баз данных, сетевого оборудования, а также средств защиты информации должна составлять не менее 8 буквенно-цифровых символа;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры. Рекомендуется использовать в парольной фразе специальные символы (@, #, $, &, *, % и т.п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, АС, USER и т.п.);
- пароли должны генерироваться автоматически и после ввода администратором учетной записи передаваться пользователям;
- пароли должны держаться в тайне, то есть не должны сообщаться другим людям, не должны вставляться в тексты программ, и не должны записываться на бумагу;

- чтобы предотвратить использование того же самого или угадываемого пароля, пароли должны меняться не реже, чем каждые 90 дней;
- пароли учетных записей администраторов серверов, баз данных, сетевого оборудования, а также средств защиты информации должны меняться не реже чем раз в месяц;
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 3 позициях;
- учетные данные пользователей должны быть заблокированы после 5 (пяти) неудачных попыток входа в систему. Все случаи неверно введенных паролей должны быть записаны в системный журнал, в целях определения и расследования инцидента информационной безопасности;
- сеансы работы пользователей с АРМ и сетевых соединений с сервером должны блокироваться после пятнадцатиминутной неактивности (или другого согласованного периода). Для возобновления сеанса должен снова требоваться ввод пароля.

Работники Компании, использующие в работе информационные системы, системы обработки информации и ресурсы АРМ, должны быть ознакомлены с перечисленными выше требованиями и ответственности за разглашение парольной информации, а также за использование паролей, не соответствующих данным требованиям.

Для генерации «стойких» паролей могут применяться специальные программные средства. Система централизованной генерации и распределения паролей должна исключать возможность ознакомления посторонних лиц с паролями сотрудников подразделений.

В случае возникновении нештатных ситуаций, форс-мажорных обстоятельств и т.п., а также при наличии технологической необходимости использования имен и паролей некоторых сотрудников (исполнителей) в их отсутствие, такие сотрудники обязаны сразу же после смены своих паролей их новые значения (вместе с именами соответствующих учетных записей) в запечатанном конверте или опечатанном пенале передавать на хранение администратору информационной безопасности АС (руководителю подразделения). Опечатанные конверты с паролями исполнителей должны храниться в недоступном для остальных сотрудников месте. Для опечатывания конвертов должны применяться личные печати владельцев паролей (при их наличии у исполнителей), либо печать администратора информационной безопасности.

4.2. Требования к политике домена

В рамках домена Компании должны использоваться централизованные политики, реализуемые средствами контроллера домена Microsoft Active Directory с применением групповых политик.

Требования, предъявляемые для паролей доменных пользователей, являются обязательными для применения всеми сотрудниками Компании и включают в себя:

- идентификаторы пользователей и их пароли должны быть уникальными для каждого пользователя;
- пароли должны состоять как минимум из 8 символов (не должны быть именами или известными фразами);
- длина паролей для администраторов домена должна составлять не менее 12 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры. Рекомендуется использовать в парольной фразе специальные символы (@, #, $, &, *, % и т.п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, АС, USER и т.п.);
- чтобы предотвратить использование того же самого или угадываемого пароля, пароли должны меняться не реже, чем каждые 90 дней;
- пароли учетных записей администраторов серверов, баз данных, сетевого оборудования, а также средств защиты информации должны меняться не реже чем раз в месяц;
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 3 позициях;
- учетные данные пользователей должны быть заблокированы после 5 (пяти) неудачных попыток входа в систему. Все случаи неверно введенных паролей должны быть записаны в системный журнал, в целях определения и расследования инцидента информационной безопасности;
- сеансы работы пользователей с АРМ и сетевых соединений с сервером должны блокироваться после пятнадцатиминутной неактивности (или другого согласованного периода). Для возобновления сеанса должен снова требоваться ввод пароля.

Пример результирующей политики, применяемой на рабочих компьютерах пользователей, представлен на Рисунке 1.

Политика	Параметр безопасности
Вести журнал паролей	3 сохраненных паролей
Максимальный срок действия пароля	90 дн.
Минимальная длина пароля	8 зн.
Минимальный срок действия пароля	0 дн.
Пароль должен отвечать требованиям сложности	Включен
Хранить пароли, используя обратимое шифрование	Отключен
Время до сброса счетчика блокировки	30 мин.
Пороговое значение блокировки	5 ошибок входа в систе...
Продолжительность блокировки учетной записи	0

Рисунок 1. Результирующая политика.

5. Смена паролей

Плановая смена паролей пользователей должна проводится регулярно, не реже одного раза в квартал. Внеплановая смена личного пароля, блокировка или удаление учетной записи работника Компании в случае прекращения его полномочий (увольнение, переход в другое подразделение и т.д.) должна производиться уполномоченными сотрудниками – администраторами ОИТ немедленно после окончания последнего сеанса работы данного работника с информационными системами.

Полная внеплановая смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри организации и другие обстоятельства) сотрудников отдела кадров или ОИТ, ответственных за генерацию паролей, администраторов средств защиты, системных администраторов и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой подсистем АС.

В случае компрометации личного пароля пользователя должны быть немедленно предприняты меры по внеплановой смене паролей в зависимости от полномочий владельца скомпрометированного пароля.

Хранение сотрудником (исполнителем) значений своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у администратора информационной безопасности или руководителя подразделения в опечатанном личной печатью конверте (возможно вместе с персональными ключевыми носителями).

6. Контроль и ответственность

Контроль за соблюдением правил хранения и использования пароля возлагается на пользователя ИС и администратора информационной системы.

Выполнение сотрудниками Компании требований настоящего регламента контролируется службой ИБ Компании, в том числе с применением технических средств.

Работники Компании несут ответственность за нарушения требований настоящего регламента. Нарушения, повлекшие утечку защищаемой информации, несанкционированный доступ, несанкционированное копирование, модификацию и блокирование или уничтожение информации, в рамках действующего трудового, административного, законодательства Российской Федерации.