НКЦКИ
НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru
E-mail: threats@cert.gov.ru

Об угрозах безопасности информации, вызванных некорректными парольными политиками

ALRT-20210514.1 | 14 мая 2021 г.

Уровень угрозы: ВЫСОКИЙ

TLP: WHITE

Подвержены уязвимости	Служебные почтовые адреса сотрудников организации
Актуальность угрозы	Актуально по настоящее время
Описание	По каналам НКЦКИ получены сведения об участившихся случаях компрометации информационных ресурсов государственных и коммерческих организаций. Анализ инцидентов показывает, что распространенной причиной получения злоумышленником несанкционированного доступа является использование пользователями слабых паролей, а также одинаковых паролей для доступа к корпоративным и личным ресурсам. Исходя из указанного выше, рекомендуем разработать и внедрить в ваших организациях парольные политики при работе с корпоративными сервисами. А также обратить внимание пользователей на недопустимость использования одинаковых паролей к корпоративным и личным информационным ресурсам. До утверждения парольной политики рекомендуем реализовать набор следующих первоочередных мер.
Рекомендации по нейтрализации угрозы	• Организовать смену паролей не реже одного раза в 180 дней. • Блокировать пользователей после 10 неудачных попыток входа не менее чем на 5 минут. • Не использовать в качестве пароля имя учетной записи или часть полного имени пользователя длиной более двух рядом стоящих символов. • Длина пароля должна быть не менее 9 символов. • Пароль должен включать в себя символы из всех следующих наборов: – латинские заглавные буквы (от A до Z); – латинские строчные буквы (от a до z); – цифры (от 0 до 9); – специальные символы (например: !, $, #, %). • Не публиковать сведения, позволяющие идентифицировать связь корпоративных и личных информационные ресурсов. • Использовать уникальные пароли для каждой учетной записи. • По возможности использовать двухфакторную аутентификацию.