Исследование «В безопасности ли ваши пароли?»

Март 2022

rt-solar.ru
solar@rt-solar.ru

Ростелеком Солар

Содержание

Введение

Пароли — это способ аутентификации пользователей для доступа к ресурсам и информации, одна из первых линий защиты компании. Наличие в компании парольной политики позволяет предъявлять пользователям требования и предоставлять рекомендации по безопасности паролей, правила их администрирования, процедуры реагирования на нарушения и доводить до сведения всех работников роль управления паролями в обеспечении безопасности предприятия.

Для многих компаний управление паролями остается слабым местом — это заметно по информации о регулярных взломах с использованием учетных данных. Поэтому надежность паролей и эффективно работающая парольная политика имеют первостепенное значение в обеспечении целостной кибербезопасности всего предприятия.

Уровень детализации парольной политики зависит от условий работы конкретной компании и ее руководителей. Но мы, со своей стороны, помимо общепринятых рекомендаций по процедурам создания, использования и администрирования паролей, советуем учитывать также следующие важные моменты:

- Использовать соответствующее программное обеспечение для управления паролями (для создания, шифрования, хранения и обновления паролей)
- Рассмотреть возможность использования парольной политики как части общей программы управления доступом
- Рассмотреть возможность использования новых дополнительных технологий идентификации и аутентификации, например MFA, включая биометрию и одноразовые пароли, чтобы усилить безопасность
- Рассмотреть возможность использования технологии единого входа (SSO), чтобы сократить количество шагов, необходимых для доступа к различным системам и ресурсам
- Как и любую другую политику, периодически пересматривать и обновлять парольную политику, чтобы поддерживать ее актуальность и эффективность
- Обеспечить периодическую осведомленность сотрудников, т. е. проводить обучение и тренинги по безопасной работе с учетными данными, чтобы сотрудники понимали важность безопасности паролей и риски, связанные с использованием слабых паролей и компрометацией учетных данных

Ключевые цифры и факты

53%

пользователей меняют пароли от аккаунтов реже одного раза в год, только когда забывают старый, или вообще никогда этого не делают

50%

пользователей ненадежно хранят пароли: записывают на бумаге, пользуются автозапоминанием в браузере, хранят в файлах на устройстве, с которого осуществляется вход в аккаунты

59%

пользователей используют одинаковые пароли для разных аккаунтов — всегда или периодически

Ключевые цифры и факты

19%

сотрудников компаний иногда или часто передают свои логины-пароли коллегам

44%

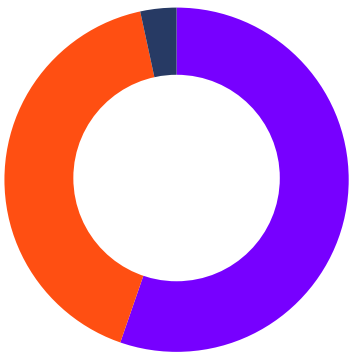
тех, кто передает свои учетные данные коллегам, в дальнейшем либо не всегда меняют пароли доступа в свои рабочие аккаунты, либо вообще никогда этого не делают

Результаты исследования

1. Надежность паролей и защищенность аккаунтов

В рамках данного исследования аналитики «Ростелеком-Солар» спросили российских интернет-пользователей, насколько используемые ими пароли от личных и рабочих аккаунтов соответствуют основным требованиям безопасности.
При этом аналитики напомнили респондентам, что основными требованиями к безопасности паролей являются: уникальность пароля (каждый пароль используется только для одной учетной записи и при этом он нигде ранее не применялся); минимальная длина в 8 знаков, а также сложность пароля (он должен включать цифры, буквы разного регистра, символы). В результате чуть более половины пользователей утверждают, что соблюдают все перечисленные требования безопасности при создании и использовании паролей от своих учетных записей. Еще 42% пользователей соблюдают два из трех правил безопасности паролей, поэтому считают, что в целом их аккаунты неплохо защищены. И лишь 3% участников исследования признают, что их пароли защищены слабо и порой не соответствуют ни одному из вышеперечисленных признаков безопасности.

Всем ли требованиям безопасности (уникальность, длина, сложность) соответствуют ваши пароли?



- **55%** — Да, мои пароли надежно защищены (соответствуют всем трем перечисленным признакам безопасности)
- **42%** — В целом скорее надежно защищены (2/3 требований соблюдены)
- **3%** — Мои пароли скорее слабо защищены (соответствуют 1 признаку или менее)

В то же время, если посмотреть на аналогичную статистику среди американских пользователей, выясняется, что 66% американцев используют один и тот же пароль в нескольких различных онлайн-аккаунтах, 24% американцев используют в качестве пароля слово «password», «Qwerty» или цифры «123456» и т. п.

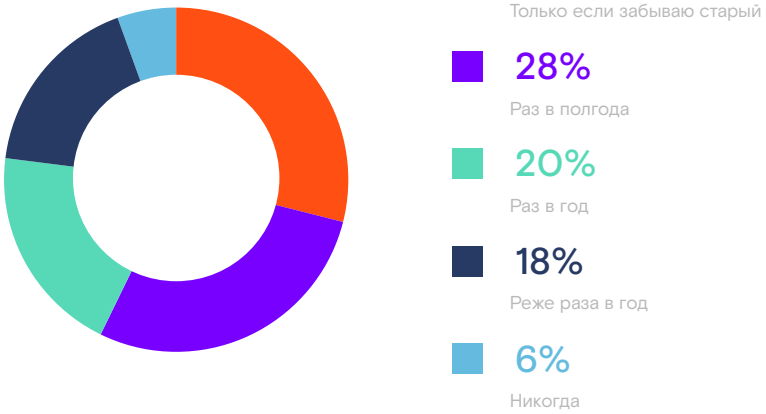
Основные выводы

Безусловно, массовый ликбез населения в вопросах киберграмотности, который ведут лидеры российской ИБ-отрасли, дает свои плоды. Однако в целом складывается впечатление, что российские пользователи переоценивают защищенность своих паролей.

С учетом того, что эксперты по информационной безопасности рекомендуют менять пароли не реже раза в квартал, а от особо критичных сервисов вроде онлайн-банкинга — ежемесячно, защищенность аккаунтов пользователей рунета вызывает опасения.

Также участникам исследования был задан вопрос, как часто они меняют пароли от своих аккаунтов для сохранения их защищенности. Здесь картина выглядит уже менее радужной: более половины респондентов отмечают, что меняют пароли от аккаунтов реже одного раза в год, только когда забывают старый, или вообще никогда этого не делают. При этом 48% опрошенных все же озабочиваются сменой паролей от аккаунтов ежегодно или даже раз в полгода.

Как часто вы меняете пароли для защиты своих аккаунтов?



Между тем российские пользователи все же хотели бы повысить защищенность своих аккаунтов, взяв на вооружение передовые методы защиты доступа. Так, более половины респондентов готовы использовать для этих целей механизмы двухфакторной аутентификации, например связку пароль или код доступа плюс отпечаток пальца или сканирование сетчатки глаза. 17% сочли полезным демонстрацию пароля при вводе для исключения ошибок при вводе сложных паролей; 16% — запрет на копипаст паролей и 15% — возможность создания длинных паролей до 64 символов (например, из фраз с разрешением включать в них любые символы, даже пробелы и смайлики).

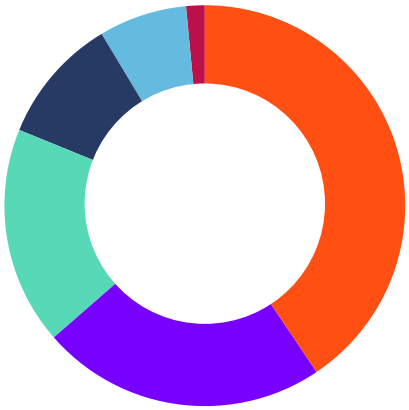
2. Хранение паролей

Чем больше вопросов эксперты задавали респондентам, тем нагляднее выявлялась слабая защищенность пользовательских паролей. Так, выяснилось, что половина опрошенных используют для хранения паролей в том числе от важных аккаунтов ненадежные методы: записывают пароли на бумаге, пользуются автозапоминанием паролей в браузере, а также хранят пароли в файликах на устройстве, с которого осуществляется вход в аккаунты. Еще 41% респондентов просто запоминают свои пароли, что явно свидетельствует о том, что такие пароли не соответствуют требованиям безопасности и являются либо довольно простыми, либо повторяющимися от аккаунта к аккаунту. Среднестатистический человек просто не в состоянии запомнить множество уникальных длинных, состоящих из различных символов паролей от десятков аккаунтов.

Лишь 7% опрошенных используют специализированные программы-менеджеры паролей для их защищенного хранения.

Таким образом, подавляющее большинство российских пользователей применяют слабые методы хранения паролей.

Где вы храните свои пароли?



- **41%** — В памяти
- **23%** — По старинке записываю на бумаге — не доверяю этим новомодным гаджетам
- **17%** — Пользуюсь автоматическим запоминанием в браузере, ведь это удобно: не надо ничего запоминанать, просто заходишьавтоматом и всё
- **10%** — В отдельных файлах на устройстве
- **7%** — Использую менеджер паролей для защищенного хранения паролей
- **2%** — Другое

Таким образом, можно заключить, что часть из тех 55%, кто заявляет, что их пароли надежно защищены, мягко говоря, лукавят.

3. Использование паролей

Давайте вспомним, сколько респондентов в ответе на вопрос, насколько надежно защищены их пароли, ответили, что их пароли хорошо защищены, поскольку отвечают всем трем требованиям безопасности. Так ответило 55% опрошенных. А теперь посмотрим на диаграмму ниже: из нее видно, что лишь 41% пользователей применяют разные пароли от разных сервисов. То есть почти 60% участников исследования, по сути, признаются, что не выполняют важнейшего требования безопасности паролей — их уникальности.

Используете ли вы одинаковые логины-пароли для разных сервисов?

41%
Использую разные пароли для разных сервисов

31%
50 на 50

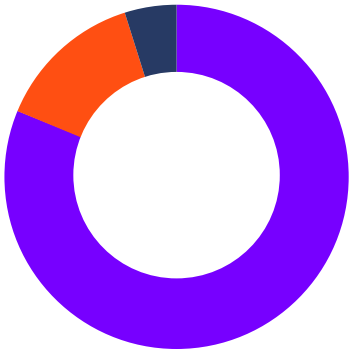
18%
Да, почти во всех сервисах использую одинаковые логины-пароли

10%
Логины использую разные, а пароли почти везде одинаковые

4. Передача паролей третьим лицам

Следует отметить, что, по крайней мере, на рабочем месте, судя по всему, пользователи более ответственно относятся к безопасности паролей от рабочих аккаунтов. Безусловно, этому способствует определенная зрелость самих российских организаций в вопросах информационной безопасности: применение современных технических средств защиты доступа, введение в компаниях строгих правил обращения с учетными записями сотрудников и т. п. Так, более 80% сотрудников компаний утверждают, что никогда не передают свои логины-пароли от рабочих аккаунтов третьим лицам, поскольку это запрещено правилами компании. И все же чуть менее 20% респондентов признались, что иногда или даже довольно часто нарушают это правило с целью оперативного выполнения некоторых рабочих задач.

Как часто вы передаете свои логины-пароли коллегам?



81%

Никогда не передаю — это небезопасно и запрещено правилами компании

14%

Иногда передаю (например, когда я не в офисе и нужно, чтобы коллега переслал мне информацию с рабочего компьютера или сделал за меня срочную задачу)

5%

Довольно часто — мы с коллегами нередко выручаем друг друга, когда «прилетает» что-то срочное от руководства

И все бы ничего, но при этом 44% из тех, кто передает свои учетные данные третьим лицам, затем либо не всегда меняют пароли доступа в свои рабочие аккаунты, либо вообще никогда этого не делают. И именно здесь возникают серьезные риски компрометации доступа, которые могут в дальнейшем обернуться большими проблемами для компании. Поскольку дальнейшая передача прав доступа к данному аккаунту, а через него и к внутренним ресурсам компании уже никак не контролируется самой организацией.

Основные выводы

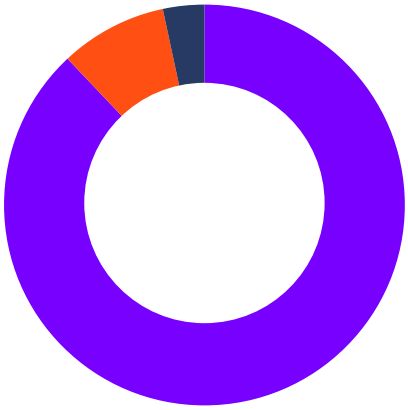
Это одна из распространенных схем передачи доступа за пределы компании, которым затем могут свободно воспользоваться внешние злоумышленники для совершения атаки на организацию.

С радостью можно признать, что массовый ликбез населения в вопросах киберграмотности, который в последние годы активно ведет российское ИБ-сообщество, дал свои плоды и оберегает граждан от грубейших ошибок в обращении с конфиденциальной информацией.

5. Пароли и социальная инженерия

Пожалуй, единственный вопрос, по которому опрошенные продемонстрировали редкое единодушие и высокий уровень киберграмотности, касался правил поведения в случае звонка от представителя банка, в котором респонденты хранят свои сбережения. Почти 90% опрошенных заявили, что не предоставят звонящему им работнику финансовой организации свои учетные данные от онлайн-банка, прервут звонок и сами перезвонят в банк по официальным контактам для проверки информации о подозрительных операциях на счетах.

Назовете ли вы свои логин-пароль от онлайн-банка звонящему вам представителю банка?



88%

Брошу трубку и перезвоню в банк сам по официальному номеру телефона, чтобы узнать, что на самом деле происходит

9%

Попрошу звонящего ответить на мои уточняющие вопросы, чтобы понять, что это действительно работник банка, и если его ответы не вызовут подозрений, то назову логин и пароль

3%

Назову работнику банка логин и пароль, чтобы предотвратить списание денег с моего счета

Методология и профиль респондентов

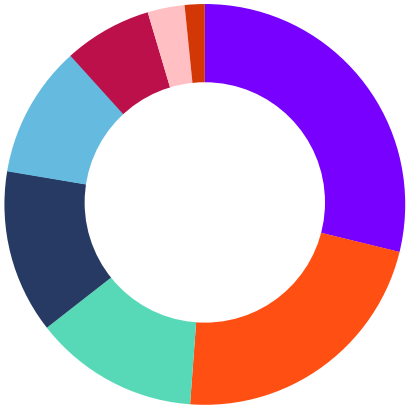
Опрос проводился в марте 2022 года.

В ходе опроса респондентам предлагалось выбрать один из предложенных вариантов ответа или указать свой вариант ответа в свободной форме.

В опросе приняли участие более 300 пользователей. 51% опрошенных составили женщины, 49% — мужчины. 34% респондентов — люди в возрасте от 30 до 40 лет, 27% — от 40 до 50 лет, 15% — от 25 до 30 лет, 11% — младше 25 лет, 9% — от 50 до 60 лет и 4% — старше 60 лет.

География респондентов представлена всеми 8 федеральными округами России.

Региональное распределение респондентов



- **29%** Центральный федеральный округ (включая Москву)
- **22%** Приволжский федеральный округ
- **13%** Сибирский федеральный округ
- **13%** Южный федеральный округ
- **11%** Северо-Западный федеральный округ (включая Санкт-Петербург)
- **3%** Дальневосточный федеральный округ
- **7%** Уральский федеральный округ
- **2%** Северо-Кавказский федеральный округ

Данное исследование проведено методом электронного опроса аудитории сервиса проведения опросов Яндекс.Взгляд, который позволяет провести опрос среди российской аудитории пользователей различных сервисов Яндекса.

Ростелеком
Солар

rt.ru
rt-solar.ru

solar@rt-solar.ru
+7 (499) 755-07-70