Способы защиты информации

**Парольная политика. Приложения аутентификации.
Генерация паролей. Менеджеры паролей.**

Идентификация – это процесс распознавания информационной системой пользователя, который указывает свое уникальное имя (логин, идентификатором) при входе в систему.

Аутентификация – это процедура проверки подлинности заявленного пользователя, процесса или устройства.

Авторизация – это предоставление определённому лицу или группе лиц прав на выполнение определённых действий; а также процесс проверки данных прав при попытке выполнения этих действий.


Регистрация
Исходные данные
Логин:
Мастер
Пароль:
Кот Шрёдингера
Система
Мастер
Вход в систему
Идентификация
Кто это?
Логин:
Мастер
Система
Мастер
Аутентификация
Как проверить?
Пароль:
Кот Шрёдингера
Система
Мастер
Авторизация
Что может делать?
Логин:
Мастер
Пароль:
Кот Шрёдингера
Система
Мастер
Действия
Результат
Выполнен вход в систему
Появится страница интерфейса
Личный кабинет
Мастер
Действия

Парольная политика – это некий комплекс правил, основная цель которого состоит в мотивации пользователей к использованию надежных паролей и правильному обращению с ними

Парольная политика позволяет настраивать:

- Количество неудачных попыток, после которых происходит блокировка.
- Время, в течение которого совершены эти попытки.
- Время, на которое блокируется пользователь после неудачного/неверного ввода данных для авторизации
- Время жизни паролей
- Мониторинг неудачных паролей
- Возможность вставки пароля из буфера
- Использование менеджеров паролей
- Блокировка неактивных учетных записей
- Блокировка сеансов без действий

Многофакторная аутентификация – это концепция защиты, требующая как минимум двух способов аутентификации (подтверждения) данных учетной записи, чтобы установить истинность личности и разрешить доступ в систему. Для проверки идентификационных данных многофакторная аутентификация объединяет несколько факторов, которые не связаны между собой напрямую. Например, такие, как знание, владение, свойство.

Цель многофакторной аутентификации

- путем формирования многоуровневой защиты осложнить злоумышленнику получение несанкционированного доступа в систему: сеть, устройства, базы данных. Когда один из факторов аутентификации оказывается скомпрометирован – вступает в действие второй, что повышает шансы блокировки доступа. Зачастую именно такая защита становится камнем преткновения для злонамеренных действий нарушителей.

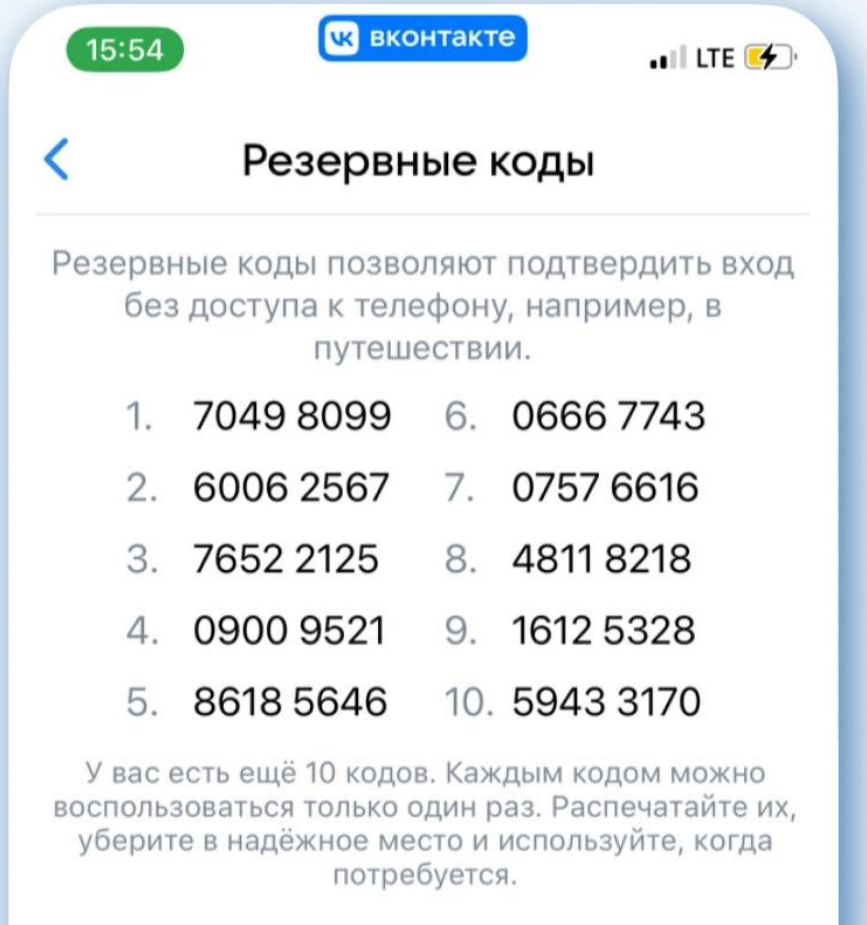
Приложения аутентификации – это безопасный и простой метод проверки личности, генерирующий номерные коды, которые пользователи вводят вместе с учетными данными для доступа к учетной записи.

Приложения аутентификации (работают и на андроидах, и на яблоках)

- Google Authenticator
- Microsoft Authenticator
- Яндекс.Ключ
- FreeOTP

Как работает одноразовый пароль на основе времени (TOTP)?

Резервный код используется, когда привязанное устройство недоступно. Резервные коды формируются сразу при подключении к сервису, но при необходимости можно сформировать новые в личном кабинете.



Резервные коды являются одноразовыми и для повторного применения нужно генерировать новые.

Генерация случайных чисел — процесс, который с помощью устройства генерирует последовательность чисел или символов, которая может быть предсказана разумным образом только на основании случайности.

Физические

Генерация происходит на основе физических явлений. Является случайным.

Алгоритмические

Генерация происходит на основе заданного алгоритма. Рано или поздно начинают зацикливаться, а значит, их результат можно предсказать. Однако в определенных пределах результаты работы таких генераторов можно считать случайными.

Менеджер паролей – программа, которая помогает пользователям создавать надежные пароли и хранить их в защищенной базе данных. Чтобы получить всю необходимую информацию при входе в учетную запись, надо ввести единый мастер-пароль. Он используется для шифрования содержимого хранилища.

Зачем нужен менеджер паролей?

- Хранение всех паролей в одном месте (не на листочке)
- Многофакторная аутентификация
- Генерация паролей (в том числе одноразовых)
- Возможность копипаста данных аккаунта без остатка в буфере обмена
- Иерархическая структура всех данных о сайтах
- Хранение ключей восстановления
- Защита в путешествиях
- Родительский контроль