Альберт Сысоев

ПАРОЛЬ

Альберт Сысоев
Пароль

http://www.litres.ru/pages/biblio_book/?art=40275765
ISBN 9785449617675

Аннотация

В этой книге понятным и простым языком описаны способы создания и хранения ваших паролей. Представлены случаи, когда надежность вашего пароля не играет никакой роли, так как сам по себе пароль не является панацеей в области IT-безопасности. А также представлены рекомендации по безопасной работе в сети Интернет, в частности обеспечение безопасности при работе в вашей онлайн-интернет-банковской системе. Вы узнаете, как надежно и безопасно хранить все ваши пароли на компьютере или смартфоне.

Содержание

Пароль

Альберт Сысоев

ISBN 978-5-4496-1767-5
Создано в интеллектуальной издательской системе Ridero

«За безопасность необходимо платить, за ее отсутствие расплачиваться» Уинстон Черчилль

Об этой книге

Книга, которая хорошо написана, всегда кажется мне слишком короткой.
Джейн Остин

Вы не найдете в этой книге подробных технических описаний организации IT безопасности. Но после применения элементарных навыков, которые вы с легкостью освоите с помощью книги, станет возможным во многом обезопасить свою жизнь и работу с электронными вычислительными устройствами – компьютерами и смартфонами.

Мы привыкли использовать в своих домах и квартирах надежные входные двери, сложно вскрываемые замки. Но при этом, многие люди, не боясь, отдают свою пластиковую банковскую карту в руки другого человека, для оплаты работ или услуг, что не может быть безопасно.

Задумайтесь, когда вы в последний раз, не по настоянию системы электронной почты, а по собственной инициативе меняли свой пароль на электронный почтовый ящик, который расположен на бесплатном сервисе? Многие, к сожалению, меняют пароли уже после факта взлома аккаунта и проведения через него незаконных действий.

Эта книга призвана дать определенный небольшой багаж знаний о том, как управлять вашими логинами и паролями,

которые, де-факто, являются вашими ключами к ЭВМ и ресурсам планетарной сети Интернет. Вы узнаете, как надежно и, главное, безопасно хранить ваши конфиденциальные данные, в том числе информацию для авторизации. Мы рассмотрим две очень распространенных программы. Первую программу вы сможете использовать на своем персональном компьютере под управлением Windows, а другая программа будет работать на вашем смартфоне под управлением операционной системы Android.

В завершение, вы сможете прочитать о несанкционированном проникновении на компьютер и его последствиях, а также узнаете, как злоумышленники попытались украсть у человека с карточки крупную сумму денег. Все истории основаны на реальных событиях, но в целях безопасности изменены должным образом.

Вы, как читатель, отдаете себе отчет и полностью соглашаетесь с тем, что данная книга является всего лишь справочным материалом, выражающим личное мнение автора, и не побуждает вас к каким-либо действиям. Все, что вы предпримите, исходя из написанного в этой книге, вы будете делать на ваш личный страх и риск. Автор не несет ответственность за любые последствия ваших действий. Все торговые марки, а также иные права на интеллектуальную и иную собственность сохраняются за их правообладателями.

Что такое пароль?

– Пароль?
– Пароль!
– Правильно, проходите.
© Народная мудрость в Интернет

Слово «пароль», как и его понятие, в нашем языке возникло из французского. При прямом переводе la parole (фр.) значит – слово или условное слово.

Первые упоминания об использовании секретных или условных слов появились еще в 201 году до нашей эры. Например, в Древнем Риме пароли использовались для безопасного прохождения людей ночью. Один из воинов, выбранный командиром, направлялся к командующему легионом, у которого получал специальную деревянную табличку с паролем. При прохождении в ночное время постов человек называл условное слово, и стража пропускала его.

Как видите, даже спустя тысячелетие, человечество все еще использует пароли. Как в военных целях, так и в гражданских. ПИН-код вашей банковской карты не что иное, как древнеримское секретное слово, пароль, а саму пластиковую карту можно сравнить с древнеримской деревянной табличкой, на которой это слово записано для того, чтобы пропустить вас.

На компьютерах пароли использовались уже с 1961 года, когда в Массачусетском технологическом институте появилась первая открытая система CTSS[1]. На этом вычислителе была предусмотрена команда LOGIN для того, чтобы можно было войти в систему, введя пароль.

В книге Марка Бернетта «Perfect Passwords» утверждается, что среди англоязычных пользователей самым распространенным паролем является «123456», а возможные комбинации «1234» и «12345678» занимают третье и четвертое места по распространенности. Разумеется, не стоит использовать что-то подобное в вашей повседневной жизни – это очень небезопасно.

Так же хочу вас предупредить об использовании ваших памятных дат в качестве пароля. Каким бы образом вы не крутили дату своего рождения, будь то «18031986» или «18marta1986goda», данное сочетание не составит проблем подобрать и получить несанкционированный доступ к ресурсам под вашим именем.

Кстати, не только пароли являются частью безопасности доступа. Помните, как в шпионских фильмах существова-

---

[1] CTSS (Compatible Time-Sharing System) – операционная система, разработанная командой Фернандо Корбато из Массачусетского Вычислительного Центра. Это была первая ОС с технологией разделения машинного времени. Эта технология позволяла работать сразу нескольким людям на одном компьютере, тем самым экономя машинное время. С появлением «Compatible Time-Sharing System» не нужно было ждать своей очереди, да и программистам стало удобнее работать вместе над одним проектом.

ли не просто парольные фразы, но и ответы на них, чтобы можно было однозначно определить личность агента. В настоящее время для определения принадлежности учетной записи, за которой, в идеале, должна аутентифицироваться определенная личность, используют такое понятие, как «имя пользователя». Но об этом в следующей главе.

Что такое имя пользователя?

В одном из банков России, где-то в районе обеденного времени 90-х годов XX века:

– Валь! Какой пароль на программу?

– Ку-ку!

– Валь! А ку-ку через черточку или нет?

Вы знаете, или слышали такие термины как: «логин», «юзер», «пользователь», «имя пользователя». Все это, под разными названиями, призвано однозначно определить личность того, кто производит вход или подсоединение куда-либо. Многие интернет сайты для процесса аутентификации пользователей используют адрес электронной почты, что принципиально выполняет основную функцию однозначного определения личности пользователя.

Вообще, в современной информационно-технологической отрасли проверку подлинности или авторизацию принято разделять на два уровня:

1. ***Идентификация*** – это ввод личных данных пользователя, которые предположительно должны совпадать с теми данными, которые хранятся в базе данных идентификаторов пользователей.

2. Аутентификация – сама проверка введенной пользователем информации и принятие на основе полученных результатов решения о допуске либо отказе в авторизации

пользователя.

То есть, в любом случае, система доступа подразумевает некоего человека, который хочет получить разрешение на доступ к работе с какими-либо ресурсами, будь то компьютерная сеть, операционная система или сейф, в котором хранятся какие-либо предметы или документы.

И когда вы ввели свое имя пользователя для получения ресурсов, система контроля будет знать, когда вы входили, и к каким ресурсам у вас был доступ. При любом возникшем расследовании эти данные могут быть использованы как в вашу пользу, так и против вас. Так как будет считаться, что вы однозначно авторизованы.

Авторизация, то есть процесс определения личности пользователя, может быть осуществлена многими способами. Возьмем для рассмотрения самые основные:

1. ***Парольная защита*** – только пользователю известен некий набор символов, который он передает системе для получения доступа.

2. ***Использование предметов*** – метод авторизации с использованием, например, обычного ключа для замка, электронного бесконтактного пропуска, либо специализированного USB ключа.

3. ***Биометрическая*** – одна из самых ненадежных систем, основанная на проверке тембра голоса, отпечатка пальца или ладони. А ненадежная она потому, что палец или ладонь можно ампутировать без желания на то пользователя. Обыч-

ные ключи можно спрятать, а так придется прятаться самому.

4. ***Скрытая информация*** – система проверки, основанная на сличении местоположения авторизуемого пользователя с его предыдущей геолокацией, или, например, на проверке определенного программного кода, который должен присутствовать в обязательном порядке на компьютере или ином вашем оборудовании. Например, если вы постоянно работаете с веб-сайтом, находясь в России, а однажды подключились с острова Гаити, это, как правило, означает кражу вашего пароля.

Информация для авторизации пользователя в наше время содержит не только сведения о пароле, но и о том, кто именно получает доступ. Вся эта информация хранится в определенном виде в специальных базах данных, конкретнее об этом пойдет речь в следующей главе.

Как в компьютере хранятся и передаются пароли?

Из телефонного разговора системного администратора с коммерческим директором предприятия:

– Выдвини верхний ящик.

– Он заперт.

– Там в серванте, за бутылкой виски, в стакане, ключ от стола, а в ящике футляр для очков, в нем бумажка с паролем.

Конец ознакомительного фрагмента.