Вальтер Граукригер

Статьи по вопросам личной безопасности. Сборник №1

12+

Вальтер Граукригер

Статьи по вопросам личной безопасности. Сборник №1

http://www.litres.ru/pages/biblio_book/?art=58529088
SelfPub; 2020

Аннотация

Настоящий сборник содержит статьи: "Главный секрет выживания", "Уровни секретности личной информации", "Грамотная работа с паролями", "Мифы о киллерах".

Сборник подготовлен по материалам сайта graukrieger.com

Главный секрет выживания

В подобного рода статьях обычно описывают, как наловить к обеду птичек и рыбок, как без спичек развести костер, как пойманную мелочь на нем приготовить без кастрюли, и тому подобные милые сердцу выживальщика лайфхаки. Но сейчас мы ставим перед собой задачу иного рода. Ниже речь пойдет не о робинзовнских глупостях, а о реальном подходе, которому обучают диверсантов, офицеров тактической разведки, партизан, и всех тех, кто вынужден долго выживать в самых негостеприимных условиях. Подходе, известном всем специалистам, но обсуждать который не принято, потому что выглядит он, мягко говоря, некрасиво. Сразу оговоримся: мы не пропагандируем подобные методы, а всего лишь беспристрастно описываем то, как вопросы выживания решаются на профессиональном уровне.

Давайте начнем с того, что поставим несколько животрепещущих практических вопросов. Вопрос первый: что кушают диверсанты, находящиеся месяц и более на вражеской территории? Конечно, можно сходить в магазин. Но там, где действуют диверсанты, как правило, магазинов нет. Даже если и есть, то в маленьком городке, где все на виду, посторонний мужчина, закупающий консервы в большом количестве, будет выглядеть подозрительно. Да и первая же встреча с полицией поставит под угрозу всю операцию. Взятый с

собой сухой паек и убитая в лесах дичь – тоже неправильные ответы. Никакой парашют не выдержит здоровенного мужика вместе с месячным запасом продуктов для него. А диверсант, занятый отловом сусликов и отстрелом медведей, не сможет качественно делать свою работу. Отлавливать и отстреливать придется каждый день, потому что холодильник и оборудование для консервации в снаряжение не входят.

Вопрос второй: на чем ездят диверсанты, когда нужно преодолеть расстояние в десятки километров? Ходят пешком – не всегда правильный ответ. Конечно, любой уважающий себя офицер глубинной разведки сможет пройти и сто, и двести километров. Только во что он после такой прогулки превратится? И не закончится ли война раньше, чем он дойдет до места назначения? Да и оторваться от преследователей с собаками и вертолетами пешком вряд ли получится. А личный транспорт диверсанту на работе не полагается.

Вопрос третий: где взять диверсанту лекарство, которого нет в распоряжении, флягу взамен утраченной, одежду или обувь взамен порванной? На все эти вопросы существует единственно правильный ответ – украсть или отобрать. Лучше, конечно, украсть, чтобы не засветиться. Но можно сработать под бандита и банально кого-нибудь ограбить, благо по внешнему виду диверсанты не слишком отличаются от бандитов. Голодный или разгуливающий в порванных ботинках разведчик никогда не станет думать о таких мелочах, как уголовный кодекс. И точно не будет церемонится с вла-

дельцами транспортного средства, когда ему срочно надо куда-нибудь съездить. Это, кстати, одна из причин, почему военную разведку редко и неохотно используют внутри страны. Полиция и даже государственная служба безопасности приучены действовать куда более деликатно.

Разумеется, в современной диверсионной войне все не так просто и прямолинейно. И партизаны, и разведчики часто прибегают к услугам группы обеспечения, которая снабжает продуктами, оказывает медицинскую помощь и добывает актуальную для диверсионной группы информацию в районе проведения операции. Если маршрут предстоит длинный, то с группой могут забросить девушку с полным комплектом документов и аптечных рецептов на все случаи жизни. Когда возникает надобность, она и самый щуплый разведчик переодеваются, например, в хиппи и ходят по магазинам и аптекам. Влюбленная парочка бродяг, закупающихся провизией, выглядит не так подозрительно. А в больших городах бывает, что диверсанты и вовсе живут на съемных квартирах с полным комфортом, ни от кого не скрываясь. Но это все-же редкость. Правильно обученный разведчик должен уметь действовать в любых условиях, полагаясь только на себя. И в большинстве случаев ему приходится бороться за свою жизнь самыми что ни есть первобытными способами.

Главный секрет выживания в том, что эффективнее всего выживать за счет других людей. Да, разведчик может под-

стрелить косулю или наловить рыбы, но он ни в коем случае не станет этим заниматься, если можно обнести чью-нибудь кладовую. Он не будет пытаться купить мотоцикл, даже если у него есть деньги, он его угонит. Это неэтично, зато оптимально с практической точки зрения. Тут приходится выбирать – идти к цели кратчайшим путем или соотносить свои действия с правами человека, законом кармы, и черт его знает еще с чем.

Подход к решению важных жизненных задач всегда можно подсмотреть у природы. Растения получают и синтезируют нужные им вещества напрямую из почвы, воздуха и солнечного света. Но растение практически полностью представляет собой фабрику по производству этих веществ. Травоядные животные продвинулись дальше, они насыщаются быстрее и эффективнее, пожирая растения. Хотя их желудочно-кишечный тракт и огромен, но все же в процентном отношении существенно меньше его растительного аналога. Еще эффективнее хищники. Пожирая других животных, они сразу получают легко усвояемые белки и жиры. Тигр никогда не смог бы совершать свои грациозные прыжки, занимай у него кишечник столько же места, сколько у быка.

Диверсант или разведчик, как и любой другой человек, столкнувшийся с жесткой необходимостью выживания, обязательно становится хищником, иногда в прямом смысле этого слова. И как бы ужасно это не звучало, людоедство входит в программу подготовки соответствующих специали-

стов. Не то, чтобы по выходным им давали на завтрак человечину, но уметь убить и съесть человека разведчик обязан. Как и уметь украсть или отобрать. И практикуется такое не только у диверсантов. В побег из отдаленных мест отбывания наказания иногда берут "кабанчика" – заключенного, которого съедят в дороге. Пышным цветом людоедство всегда процветало и в голодные времена.

Мы не знаем, правильно это, или нет. Мы не судим разведчиков и голодающих. Мы просто констатируем факт: в экстремальных условиях выживание эффективно лишь за счет других людей, их имущества, ресурсов, а иногда и плоти. Выжить, наплевав на мораль, или умереть благородным человеком – каждый решает для себя сам. Главное не витать в облаках и не фантазировать, а видеть вещи такими, каковы они есть. И называть их своими именами.

Уровни секретности личной информации

Ниже мы рассмотрим уровни секретности личной информации. Необходимо учитывать, что различные источники трактуют понятие личной информации по-разному. В частности, отождествляют его с понятием персональных данных. Такое сужение может быть оправдано с юридической точки зрения, но не эффективно с точки зрения личной безопасности. Поэтому под личной информацией мы будем подразумевать совокупность сведений, касающихся конкретного лица. Это могут быть любые сведения, начиная от адреса и телефона, и заканчивая вкусами и предпочтениями. Их стро-

гое разграничение по категориям является одним из базовых требований личной безопасности и залогом сохранности личной тайны.

Третий уровень – публичная информация

Самые скрытные люди охотно и много рассказывают о себе. И все их рассказы чаще всего чистая правда. И лишь изредка – ложь, но такая, в которую искренне верит рассказчик, и которую невозможно проверить. Вы никогда не найдете у них секретов, потому что никогда не узнаете, где надо искать. Изобилие неотличимой от правды информации решительно обо всем является прекрасным средством сокрытия тайны. Искусство лжи, о котором мы подробно писали, предполагает отсутствие белых пятен в биографии, связях, предпочтениях и делах.

Чтобы упростить себе задачу сохранения тайны, нужно выделить и прекратить скрывать все, что можно узнать о вас, не прилагая особых усилий. Дата рождения, адрес прописки, места учебы и работы, увлечения и приятельские контакты… Поступая таким образом, вы, во-первых, избавите себя от тяжелого и бессмысленного труда утаивания шила в мешке, а во-вторых, создадите репутацию правдивого и открытого человека. Отдельно позаботьтесь о заполнении пустот. Если вы, к примеру, равнодушны к музыке, дайте себе труд прослушать дюжину наиболее популярных песен или композиций, чтобы без запинки ответить на вопрос о музыкальных предпочтениях. Рассказы из студенческой жизни, про-

фессиональные байки и пространные отчеты о проведенном с приятелями времени всегда должны быть наготове.

Все это и есть информация третьего уровня, то есть открытые сведения. На первый взгляд определение ее в отдельный уровень может показаться не оправданным, однако это не так. Смысл в проведении для себя предельно ясной черты между тем, что можно не скрывать, а что нужно скрыть обязательно.

Второй уровень – конфиденциальная информация

Сюда относится все, огласка чего может причинить вам ущерб, и что технически возможно скрыть. Прежде всего это сведения о профессиональной деятельности – клиенты, контракты, расчеты. Также это информация о дружеских связях, которые следует отличать от приятельских. Связь с другом более тесная и значимая, следовательно, от друга можно получить больше информации о вас, а также есть возможность прибегнуть к шантажу угрозами причинения вреда другу. Истинные вкусы и предпочтения тоже иногда приходится скрывать, чтобы не давать пищу для размышления чересчур любознательным аналитикам.

Важно понимать, что ко второму уровню относится лишь та конфиденциальная информация, которая при определенных обстоятельствах все же может быть раскрыта, и к раскрытию которой вы, в принципе, готовы. На втором уровне мы обычно имеем дело с информацией, разделенной между несколькими участниками какого-либо процесса. Хотя она

и является конфиденциальной, на ее надежное сохранение в тайне все же надеяться не нужно. Поэтому всегда необходимо иметь план действий на случай ее утечки. И, конечно же, надо быть готовым предоставить доступ к ней по требованию правоохранительных органов. Следовательно, сведения, способные вас серьезно скомпрометировать, относятся к более высокому уровню секретности.

Обязательно найдите время, внимательно и неспеша определите информацию о себе, своей деятельности и своем окружении, которая является конфиденциальной, и не подлежит огласке. Раз и навсегда проведите внутри четкую грань между конфиденциальной и публичной информацией, и вы получите гарантию, что однажды не проболтаетесь и не оставите бумажку с записанным паролем на видном месте.

Первый уровень – личная тайна

Личная тайна представляет собой информацию, которая никогда и ни при каких обстоятельствах не может быть сообщена третьим лицам. Прежде всего это сведения о совершенных вами поступках, за которые вас могут наказать. Далее это сведения о криптовалютных кошельках и депозитах в банках, обеспечивающих высокий уровень приватности, а также о тайниках с деньгами, документами, носителями информации, оружием и спецтехникой. И, конечно же, сведения о ваших наклонностях, связях и делах, которые могут вызвать неодобрение в обществе.

В некоторых случаях информацией первого уровня о вас

могут естественным образом владеть другие люди. Например, если вы коллективно занимались некой деятельностью, за которую может последовать наказание. В этом случае надо поступать следующим образом:

1. Уничтожить все компрометирующие документы и принять профилактические меры в отношении посвященных в тайну людей.

2. Достичь так называемого равновесия страха. Оно возникает в случае, когда разгласивший информацию о вас пострадает не меньше вашего. В определенных ситуациях равновесие страха может быть достигнуто и с теми, от кого зависят последствия для вас от разглашения тайны.

3. Если произойдет утечка, твердо, последовательно и до конца отрицать все, настаивая на версиях ошибки, клеветы и фабрикации улик.

Существует еще одно исключение, при котором вы сами можете открыть доступ к информации первого уровня. Речь идет об оказании вам помощи, когда вы открываете доступ к тайнику, паролю или счету своему доверенному лицу. Чтобы свести риск к минимуму, необходимо заранее смоделировать соответствующую ситуацию, и сделать, говоря компьютерным языком, "песочницу". То есть создать счет или тайник, существование которого вы можете рассекретить в случае крайней необходимости. Количество средств и качество предметов должно быть достаточным для оказания вам помощи, но недостаточным для причинения существенного

вреда.

Критически важным условием сохранения личной тайны является сокрытие самого факта ее существования. Информация первого уровня секретности не может храниться на персональном компьютере в зашифрованном виде, так как существует масса методов заставить человека сообщить пароль. Стратегический запас средств не может храниться на счету в банке страны, гражданином которой вы являетесь, так как существует масса поводов заморозить счет до туманного "выяснения обстоятельств", которое может длиться годами и обернуться неприемлемыми требованиями.

Особые требования предъявляются к тайникам. Предметы, составляющие личную тайну, не могут храниться в тайниках, расположенных на вашей территории, так как связь тайника с вами не должна прослеживаться даже после его детального исследования. По этой же причине в тайнике не должно быть ваших отпечатков пальцев, волос и прочего биологического материала. Все файлы на физических носителях информации должны быть зашифрованы и носить имена в виде случайного набора символов. Документы на бумажных носителях должны храниться в контейнерах, оборудованных системой самоуничтожения в случае несанкционированного доступа.

Также учтите, что инстинкт велит людям делиться своими тайнами. Эта особенность является частью механизма взаимного обмена информацией, помогающего выжить всем

стайным животным. И, разумеется, этот механизм широко эксплуатируется в качестве средства доступа к личным тайнам. Наиболее распространены следующие каналы утечки информации первого уровня:

1. Исповедь. Тайна исповеди на практике защищена далеко не так хорошо, как в теории. Даже честный священник это всего лишь человек, со всеми присущими ему уязвимыми местами. И заставить его совершить нужное действие ничуть не сложнее, чем любого другого человека.

2. Откровения с личным психологом. Частники, как правило, ведут анонимный прием и заботятся о собственной репутации, что дает хоть какое-то подобие гарантии тайны. Рассказать же что-то психологу или психиатру на ставке все равно, что совершить донос на самого себя.

3. Тщеславие. Скрытность предполагает образ жизни, максимально приближенный к посредственности. Умение хранить тайны очень плохо сочетается с желанием блистать, иметь популярность и находиться в центре внимания. При определенных обстоятельствах людям определенного склада идея произвести впечатление может показаться более привлекательной, чем идея сохранить свои действия в тайне.

4. "Пьяная исповедь". Иногда алкоголь обостряет чувство вины, снижает бдительность и одновременно растормаживает речевые центры. В результате возникает непреодолимое желание "облегчить душу". Результаты такого "облегчения" очень плачевны, поэтому тем, кто подвержен подобным эф-

фектам, рекомендуется пить в одиночестве, а еще лучше не пить вовсе.

5. "Постельные откровения". Влюбленность вообще и секс в частности вызывают мощнейший выброс в кровь веществ, сходных по действию с наркотиками. В результате исчезает осторожность и происходит смещение акцентов значимости. Мир начинает казаться прекрасным, объект любви самым важным, а тайна чем-то малосущественным. Особенно сильно это выражено у женщин, поэтому их привлекают к работе спецслужб крайне неохотно.

Чтобы исключить возможность утечки информации первого уровня под действием психологических факторов, необходимо четко маркировать ее в памяти. То есть раз и навсегда, для любых переживаний и обстоятельств поставить перед ней внутренний знак моментальной остановки.

Грамотная работа с паролями

Умение работать с паролями не ограничивается способностью придумать пароль, отличный от 123456 или года рождения. При всем изобилии программ-хранителей, серьезный подход диктует необходимость некоторые пароли держать в голове. Заучить раз и навсегда дюжину последовательностей символов для нормального человека не представляет особенного труда, но дело в том, что их надо регулярно менять, и это становится реальным испытанием для памяти. В этой статье мы расскажем, в каких случаях необходимо, и как правильно придумывать и держать в памяти качественные,

регулярно изменяемые пароли, как записывать их на бумаге таким образом, чтобы никто не понял, что это, и какими программами лучше пользоваться для их безопасного хранения. А также поделимся несколькими лайфхаками, делающими жизнь более скрытной, а следовательно безопасной.

Какие пароли можно держать только в памяти

Как мы уже писали, любая информация должна быть отнесена к одной из трех категорий: та, которую можно сообщать всем, та, которую можно сообщать доверенным лицам, и та, которую нельзя сообщать никому и не при каких обстоятельствах. Так вот доступ к информации первого уровня необходимо осуществлять исключительно по памяти. Поясним на простом примере. Допустим, у нас есть файлы, содержимое которых как раз и представляет собой информацию первого уровня. Тогда анонимно соединяемся с удаленным хранилищем файлов, и заливаем туда запароленный архив с ничего не говорящим именем. После чего стираем без возможности восстановления файл на компьютере, и вуаля! Теперь не только нельзя просмотреть файлы, но и невозможно связать их с нашей персоной, поскольку при правильном анонимном соединении с хранилищем наша с ним связь вообще никак не видна. Только чтобы не было ни единой зацепки, логин и пароль удаленного хранилища, а также пароль к архиву надо держать исключительно в памяти, и нигде более.

Привыкший к комфорту читатель может спросить, а за-

чем такие сложности? Не проще ли зашифровать файлы, и дело с концом? Разумеется, так проще, но есть нюансы. Например в Великобритании за отказ предоставить доступ полиции к зашифрованным файлам можно угодить в тюрьму. И это отнюдь не абстрактная страшилка, реальные приговоры уже выносились. В странах, где такого закона пока нет, отказ предоставить правоохранительным органам доступ к закрытой информации будет квалифицирован как препятствование расследованию с тем же результатом. Если же доступ захотят получить менее озабоченные соблюдением законности граждане, может получиться совсем уж некрасиво. Так что проще еще не значит лучше. Мы не устаем повторять простую, но важную истину: безопасность и удобство сочетаются плохо. Обычно ради одного приходится частично жертвовать другим.

Конечно, в качестве компромиссного варианта можно воспользоваться тем же трукриптом, позволяющим создать криптоконтейнер, а потом засунуть этот контейнер в гущу системных файлов или вообще замаскировать под продукты жизнедеятельности вируса. Но наличие программы типа truecrypt заставит интересующихся искать контейнеры, а это не такая и сложная задача для профессионала. Не так часто встречаются абсолютно непонятные файлы, сплошь заполненные хаотическим набором нулей и единиц. Кроме того, возникнет проблема с резервным копированием. Если присутствие непонятного файла на компьютере еще можно по-

считать случайным, то наличие его копии на флешке или в вашем аккаунте облачного хранилища объяснить случайностью не получится. Но в любом случае главный пароль доступа ко всей этой цепочке все равно придется держать в памяти.

Немного мнемоники

Допустим, нам надо придумать годный к запоминанию изменяющийся пароль к сервисам гугла. Для начала придумаем слово, которое у нас будет намертво ассоциироваться с гуглом. Например – булка. Так и запомним себе: гугл – булка. Первая часть пароля готова: bulka. Далее ставим счетчик изменений пароля. Поскольку пароль у нас первый, так и пишем: 01. Вторая часть пароля готова, и все вместе будет: bulka01. А дальше самое интересное.

Для третьей части пароля нужно придумать любое число. Оно будет стартовым, и его надо просто запомнить, как номер телефона. Поскольку первая часть пароля у нас для разных сервисов будет разной, третью часть можно сделать одинаковой, что на порядок упростит задачу. А еще надо придумать алгоритм, по которому стартовое число изменяется с каждым изменением пароля. Это не так сложно, как кажется. Рассмотрим на примере.

Допустим мы выбрали стартовым числом 8571. Тогда самый первый пароль будет: bulka018571. А в качестве алгоритма возьмем сложение третьей части пароля со счетчиком, умножение этой суммы на 13, и отбрасывание цифр слева та-

ким образом, чтобы осталось всего четыре цифры. Посмотрим, что получится при изменениях нашего пароля.

Первый пароль: bulka018571. Булка указывает на гугл, 01 это порядковый номер пароля в череде изменений, а 8571 это стартовое число, которое надо запомнить раз и навсегда. Его можно безбоязненно написать на самом видном месте, и все будут думать, что это пин код от какой-то безвестной банковской карты или телефона.

По прошествии времени надо будет поменять пароль в целях безопасности. При следующем изменении пароля bulka остается неизменной, как и при всех последующих изменениях для гугла. 01 превращается в 02 – к счетчику изменений пароля всякий раз прибавляется единичка. С числом 8571 производим действия согласно алгоритму. Счетчик в пароле был 01, поэтому к 8571 прибавляем единичку и получаем 8572. Полученное 8572 умножаем на 13 и получаем 111436. Далее от этого числа отбрасываем столько циферок слева, сколько нужно, чтобы осталось четырехзначное число. В итоге от 111436 остается 1436. Это и будет третьей частью измененного пароля. Полностью измененный пароль теперь выглядит так: bulka021436.

Предлагаем читателям самостоятельно потренироваться в дальнейших изменениях пароля. Не забывайте, что дальше счетчик надо прибавлять к уже изменившейся третьей части пароля, а потом умножать это на 13. То есть каждый следующий пароль будет выводиться из предыдущего. Стартовое

число нам может понадобиться, если придется восстанавливать всю цепочку. Первые пять паролей выглядят так:

bulka018571
bulka021436
bulka038694
bulka043061
bulka059845

Для яндекса, мейл ру и прочих сервисов цифровая часть пароля остается в точности такой же, меняется только слово. Таким образом мы получаем единый алгоритм изменения паролей для всех сервисов, и все это вполне реально удержать в памяти! Только чтобы не запутаться, пароли придется одновременно менять для всех сервисов, тогда номер счетчика и вся цифровая часть пароля будут одинаковы для всех сервисов. Запомнить придется слово для каждого сервиса, одинаковое для всех стартовое число, и порядковый номер изменения. Если пароли менять не часто, то и первая, и вторая, и третья части пароля удерживаются в памяти.

Алгоритм выше приведен для примера. Мы не позиционируем его как самый простой, надежный и остроумный. В случае анализа длинного фрагмента цепочки изменений хороший математик выявит закономерность. Но, с другой стороны, где он такую цепочку возьмет? Разумеется, алгоритм можно и нужно придумать другой, свой. Вместо цифр брать буквы, и выводить новые буквы, сдвигаясь вперед по алфавиту на определенное плавающее число, это увеличит на-

дежность. Простор для фантазии широкий. Только учтите, что плохо подобранный алгоритм может дать повторяющиеся символы, чего необходимо избежать.

И напоследок самое главное: никакие алгоритмы, упрощающие запоминание, не помогут, если пароли вводить из хранилища, и никогда не делать этого по памяти. Поэтому вначале каждый день нужно проверять сохранность всех паролей в памяти. И лишь спустя время можно будет устраивать такие проверки реже, но не менее одного раза в неделю.

Хороший пароль – хешированный пароль

Развивая идею об изменении паролей в соответствии с алгоритмом, мы неизбежно придем к мысли о возможности написания программы для легкой генерации списка хоть на сто лет вперед. Вообще-то, идея генерировать пароль программными средствами не слишком хороша, так как всегда придется иметь в распоряжении соответствующую утилиту. И если ее утратить, это может стать проблемой. С другой стороны, помня алгоритм, и умея написать рабочую версию Hello World хоть на каком-нибудь языке программирования, восстановить все можно будет за пятнадцать минут.

Мы хотим предложить компромиссный вариант: программу, которую можно не только быстро написать, но и скачать из разных источников в интернете, и заказать у любого программиста, не вызывая подозрений. Разумеется, речь идет о хешировании. Эта, в общем-то, алгоритмически довольно сложная процедура распространена настолько широко,

что получить к ней доступ можно всегда. Призываем неискушенного читателя не бояться непонятного слова. Считайте, что над придуманным вами паролем надо будет совершить еще одно преобразование, которое хорошо известно всем программистам. В его тонкости вникать нет необходимости, все уже продумано до вас. Надо только скачать программу с приглянувшегося ресурса в сети, и нажать на кнопку Старт. Приведем пример использования хеша для вывода пароля.

Требование наличия кодового слова, ассоциированного с сервисом, остается. То есть, продолжая пример, первая часть пароля для гугла остается прежней: bulka. Счетчик изменений тоже остается: 01. Зато больше запоминать ничего не надо. Если к паролю bulka01 применить операцию хеширования, и отделить первые двенадцать символов вычисленного хеша, мы получим очень качественный двенадцатисимвольный пароль: MTEyMGRiM2Fj. Небольшая тонкость в том, что разновидностей процедур хеширования достаточно много, и нужно еще помнить, какая именно используется. Но тут многообразие обманчиво, и выбирать особенно не из чего. Функция SHA256 на сегодняшний день является стандартом, и на ней смело можно остановиться.

У хеш-функции есть две приятные особенности. Во-первых, она необратима. Это значит, что по хешу определить исходную фразу настолько тяжело, что с этим не справятся современные компьютеры за обозримое время. А по

первым двенадцати символам хеша восстановить ключевую фразу невозможно даже теоретически. Во-вторых, изменение даже одного символа в исходной фразе повлечет за собой кардинальное изменение всего хеша. Например, следующий в череде изменений пароль bulka02 после хеширования алгоритмом SHA256 и отделения первых двенадцати символов будет иметь вид: ZDE5YTQ3Njgx. Сравните с MTEyMGRiM2Fj (хешем от bulka01) – ничего общего. Таким образом, случайная компрометация хешированного пароля не даст злоумышленнику ключа к системе, по которой меняются пароли.

Применение хеширования избавляет от необходимости подгадывать определенное количество символов, чтобы пароль не получился слишком длинным (о длине пароля мы еще поговорим). Более того, чем длиннее пароль перед хешированием, тем он надежнее. Мы предлагаем пользоваться не отдельными словами, а целыми фразами. Например, возьмем в качестве пароля фразу: to be, or not to be, that is the question. Удалим из нее знаки препинания, пробелы, и добавим четырехзначный счетчик: tobeornottobethatisthequestion0001. Затем применим функцию SHA256, отделим первые двенадцать символов, и получим: ZmM2Zjg0N2Mx. Точно так же можно брать и фразы на русском, написанные транслитом или в английской раскладке клавиатуры.

Теперь несколько практических рекомендаций. В сети

есть очень много предложений вычислить хеш прямо онлайн, ничего не скачивая. Так делать нельзя, потому что ваш пароль утечет в интернет. Надо найти программу, скачать ее, и установить у себя на компьютере. Запускать ее лучше в песочнице, на случай вирусов. Также будет полезно не разрешить ей соединяться с интернетом. Программе, рассчитывающей хеш, интернет не нужен, и если она пытается туда выйти, значит дело не чисто. И последнее. Установив программу, проследите, чтобы она считала хеш так же, как и все те программы, что делают это онлайн на разных сайтах. Учтите, что один и тот же хеш можно выводить разными символами. Ищите результат, похожий на приведенные выше примеры. Если увидите, что в результатах нет букв k,l,m,n и далее, значит это не то, что надо. Кроме того, программирование с ошибками никто не отменял. В качестве проверки программы можете ввести bulka01 и прочесть первые двенадцать символов. Это должно быть MTEyMGRiM2Fj.

Сколько и каких символов должен содержать пароль

Сразу надо разделить все пароли на две большие категории. Первая это пароли, вводимые для получения доступа к онлайн сервисам. Ко второй относятся пароли, защищающие архивы и зашифрованные файлы. Требования к ним разные. Мы не рекомендуем использовать пароли к онлайн сервисам длиннее двенадцати символов. На сегодняшний день этого вполне достаточно, так как прямой перебор путем отправки запроса на сервер и получения ответа идет слишком мед-

ленно даже для взлома существенно более коротких паролей. Кроме того, ни один уважающий себя ресурс не позволит вводить пароли как из пулемета, на определенной попытке ip адрес просто заблокируют. С другой стороны слишком длинные пароли могут на сервере молча обрезаться или, что еще хуже, некорректно обрабатываться. Так что длина в двенадцать символов является оптимальной в современных реалиях. Для шифрования файлов, напротив, необходимо использовать как можно большее количество символов в предлагаемых алгоритмом рамках. Здесь оптимальным будет пароль в тридцать два символа. Минимально допустимым может считаться двадцатисимвольный пароль.

И те и другие пароли должны содержать только заглавные и строчные латинские буквы и цифры. Некоторые сервисы пропагандируют и даже требуют включения в пароль экзотических символов. Что ж, если вы столкнулись с подобным требованием, подчинитесь ему. Но делать такие вещи по собственной инициативе мы не рекомендуем. Существует стандартный набор символов, которые по идее должны обрабатываться так же, как и буквы, и их, опять же по идее, можно безопасно включать в пароль. Но это в теории. На практике же иногда попадаются программисты с совершенно удивительной способностью разместить грабли там, где их, казалось бы, разместить невозможно в принципе. Поэтому лучше не рисковать.

Напоследок расскажем об одной исключительной ситуа-

ции, которую надо уметь обрабатывать. Некоторые сервисы могут потребовать пароль, в обязательном порядке содержащий хотя бы одну цифру, одну строчную букву и одну заглавную букву. А значит если хеш вашего пароля не содержит одного из обязательных символов, сервис его не примет. Существует два способа решения этой проблемы.

Сложный способ требует модификации алгоритма получения конечного пароля. Здесь самым удобным будет вариант брать не 1-12 символы из хеша, а 2-13. Если и с этим паролем что-то не так, то 3-14, и так далее. Вероятность того, что любые идущие подряд 12 символов длинной последовательности полного хеша будут забракованы, стремится к нулю. Но теоретически такое возможно. Тогда придется проскочить один порядковый номер в очереди при смене пароля. Например, если будут забракованы все возможные 12-символьные пароли, получающиеся из bulka59 не подойдут, то надо пропустить этот пароль, и сразу ставить bulka60.

Существует и более легкий путь. Все будет прекрасно работать, если к любому паролю в обязательном порядке добавлять, например, Aa1. Тогда, вне зависимости от хеша, конечный пароль будет обязательно содержать все необходимые символы. Но серьезный человек так не поступит. Потому что последовательность Aa1 позволит идентифицировать личность (пусть и анонимную), как одного и того же пользователя. Конечно, все сервисы хором поют сладкую песню, что все хранятся у них на сервере только в хешированном

виде, и даже их собственные сотрудники не знают ваш любимый пароль. Но давайте оставим эти сказки детям, верящим в Деда Мороза и Карлсона.

Логин тоже важен

Во всех инструкциях к регистрации на сайтах очень любят поговорить о паролях и попроверять их на надежность. О логине либо не говорят вообще ничего, либо укажут символы, которые он может содержать. А вы никогда не думали о том, что плохой логин или никнейм может привести к расконспирации?

Худший из всех возможных логинов тот, который содержит ваши персональные данные. Sokolov1994 – очень плохой логин, если ваша фамилия Соколов, и вы родились в 1994 году. Vasya_10_12, ChertanovoYuzhnoe, Pythonprogrammer – тоже отвратительные логины. Но это как бы лежит на поверхности. Юзер, который кажется себе тонким конспиратором, может взять ник Vasya, в то время, как его зовут Петя, и радоваться, что всех перехитрил. А по факту он во всеуслышание заявил о своей принадлежности к русскоговорящему сообществу. Выдать могут не только буквы, но и цифры. Наличие трех шестерок в нике сообщит о христианском культурном пространстве, а специфический порядок написания числа и месяца выдаст американца.

Хороший ник это обычное английское слово и несколько одинаковых или идущих подряд цифр (кроме 666). Простое английское слово может знать и китаец, и индус, и француз.

А постучать пальцем по какой-нибудь цифре это первое, что придет в голову человеку любой национальности, когда ник с его любимым словом занят. Хорошие ники это cucumber111 и tomato1234.

Пара слов о софте

Точнее даже не пара, а одно, так как мы намерены порекомендовать всего один программный продукт: KeePass. Этот хранитель паролей имеет целый ряд преимуществ, которые делают его на голову выше конкурентов.

1. Открытый исходный код.
2. Бесплатность.
3. Использование стойкого алгоритма AES (256-бит).
4. Портативная версия для Windows.
5. Порт под линукс: KeePassX.
6. Удобная организация каталогов.
7. Настройка автозаполнения.
8. Возможность хранить текстовую информацию.
9. Возможность присоединять файлы и хранить их в зашифрованной базе.
10. Встроенный генератор паролей.

Если вы все же решите подобрать себе что-нибудь другое, выбирайте только продукт с открытым кодом, и которым, по возможности, пользуется еще кто-то, кроме автора. Также сразу отметите все программы, хранящие пароли в облаке – добром такое не кончается. И позаботьтесь о регулярном создании резервных копий зашифрованной базы паролей.

Мифы о киллерах

Пришло время развенчать некоторые распространенные мифы о наемных убийцах. Разумеется, любое правило немыслимо без исключений. Специалист, близко знакомый с предметом, вероятно сможет вспомнить необычных персонажей и необычные ситуации, не укладывающиеся в рамки статистического большинства. Но наша цель состоит как раз в обратном – рассказать о том, чего не бывает в подавляющем большинстве случаев.

Миф №1: Профессия киллера высоко оплачивается

Время от времени приходится слышать о каких-то чудовищных суммах, выплаченных за убийство вполне себе обычных граждан, в лучшем случае охраняемых коллективом бывших вояк или уголовников разной степени дилетантства. Такая "охрана" может помешать киллеру даже средней квалификации разве что случайно. Поэтому суммы в десятки тысяч долларов за такую работу не имеют ни малейшей связи с реальностью, если, конечно, цель не занимает одну из ключевых должностей в государстве и не охраняется профессионалами высокого уровня. Ценник за подобные услуги стартует от нескольких сотен долларов у наркоманов и гастарбайтеров, и заканчивается в районе нескольких тысяч долларов у более-менее сносных специалистов. Но это если платить напрямую киллеру, чего в жизни практически никогда не бывает. В профессионально исполненном заказном убийстве обязательно присутствует цепочка посредни-

ков, которые за свои услуги возьмут никак не менее половины гонорара, поэтому цена для конечного потребителя вырастает в разы. Но собственно киллер этого никак не почувствует и все равно получит ровно столько, сколько стоит именно его работа.

Миф №2: Киллеры – люди свободные и независимые

В жизни все обстоит с точностью до наоборот. Дело в том, что в такую специфическую профессию просто так не приходят, как можно прийти в профессию, например, автослесаря или программиста. Не может начинающий киллер дать рекламу своих услуг, ему нужен своего рода импрессарио, который возьмет на себя организационные вопросы. Но такой импрессарио тоже не может давать рекламу, и получается замкнутый круг. На практике киллер всегда обслуживает определенную криминальную структуру, у которой, в силу специфики деятельности, периодически появляются заказы. А чтобы не было сюрпризов, наемного убийцу держат на коротком поводке компроматом, располагая исчерпывающей информацией по проведенным им ликвидациям. Со свободными художниками, которых мы видим в кино, связываться серьезные люди не станут. Только прочно сидящий на крючке киллер будет послушно выполнять любую работу, да и платить ему можно существенно меньше.

Миф №3: Киллеры – крутые ребята

В кино обычно так: наемный убийца накачан, владеет приемами карате, стреляет из любого оружия точно в цель,

лазает по отвесным стенам как таракан, и вдобавок без проблем гоняет на всех транспортных средствах, от самоката до самолета. При этом желательно, чтобы он был чертовски обаятелен и сексуален, и обязательно в костюме с галстуком и черных очках. В жизни все совсем по-другому. В уголовной иерархии убийцы стоят практически в самом низу, в противоположность элите – ворам, мошенникам, фальшивомонетчикам и даже профессиональным картежникам. Всем перечисленным профессиям надо долго и старательно учиться, а чтобы достичь высот, нужен еще и немалый талант. А вот грабителем, рэкетиром и убийцей может стать каждый дебил, и часто именно из этой категории граждан убийц и готовят. Ни о каком обаянии, ни о какой утонченности или крутизне речь здесь не идет. Типичный убийца это амбал с психическими отклонениями, освоивший один-два способа отправлять людей на тот свет.

Конечно, в каждой профессии есть место творчеству, как и люди, достигшие высокого мастерства. Но они тоже не похожи на крутых парней. Стрелки берегут руки как скрипачи и подолгу тренируются в тире. В результате никакого карате, часто остеохондроз и пивной живот. Талантливые подрывники и отравители получаются из гиков, над которыми издевались в школе. В зрелом возрасте к очкам и затравленному виду у них добавляется лысина и мятый костюм, который купила мама, но гладить его от старости уже не может. Бывают в виде исключения профессиональными убийцами и

женщины, но там такая проблема с головой, что затравленным очкарикам и не снилось. Так что, увы, образ крутого и обаятельного киллера остается жить исключительно на киноэкранах.

Миф №4: У наемных убийц существует кодекс поведения

Когда речь заходит о кодексах в преступном мире, у разумного человека появляется вопрос: какой кодекс вообще может быть у тех, кто сознательно и регулярно нарушает все законы, от библейских до государственных? Правда, воры еще пытаются для виду налепить некое подобие благородства. Например "правильный" домушник, забравшись в квартиру, обязательно оставит хозяину самое необходимое – один комплект одежды, тарелку, ложку… Известны случаи, когда вор, увидев крайнюю степень нищеты и детскую коляску, не только не крал вещи, но и оставлял на видном месте деньги. Такие выходки действительно иногда практиковались раньше. Помимо бравады они преследовали еще одну цель – заручиться поддержкой бедных слоев населения, к которым при случае можно было обратиться за помощью. Именно с этой целью устраивал пиры и раздачи денег нищим Мишка Япончик.

Киллеры возможности подобного маневра лишены начисто, так как ни передумать убивать, ни убить частично они не могут. И не любит их никто, включая их собственных боссов и заказчиков. Дело в том, что запрет на убийство себе подобных является древнейшим и строжайшим табу во всех че-

ловеческих сообществах. И тот, кто нашел в себе силы превозмочь этот запрет, бессознательно считается окружающими уже как бы не совсем человеком. Ну подумайте сами, захотелось бы вам дружить с тем, кому в принципе ничего не мешает вас безнаказанно убить? В такой ситуации придумывать какие-то кодексы совершенно бессмысленно, и никто, кроме писателей и сценаристов, этим не занимается.

Миф №5: Наемный убийца – универсальный солдат

Такое заблуждение тоже встречается, хотя и не так часто, как остальные. Здравый человек все-таки понимает, что быть профессиональным хирургом, акробатом и оперным певцом одновременно невозможно. Но под действием обильно производимых киностудиями боевиков у обывателя создается подспудное впечатление, что один и тот же киллер может и подстрелить, и взорвать, и отравить, и устроить несчастный случай. Конечно же, это не так. Хороший стрелок мог за всю жизнь ни разу не подержать взрывчатку в руках, не говоря уже о том, чтобы ее квалифицированно применить. Да и зачем ему? В таком деле риск слишком велик, чтобы экспериментировать. Научился попадать в голову со ста метров, и хорошо, и пользуйся. Киллеры высокого класса, наоборот, стараются как можно глубже разобраться в многочисленных тонкостях своей узкой специализации, чтобы пожить подольше. Уж они-то как никто иной знают, что может произойти вследствие недобросовестного отношения к поставленной задаче.