УДК 343.98:004.056

ПРИМЕНЕНИЕ БИОГРАФИЧЕСКИХ ФАКТОВ ПРИ ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ОБУЧАЮЩИХСЯ НА ЮРИДИЧЕСКИХ ФАКУЛЬТЕТАХ

Юань Владимир Лишиньевич

Западно-Сибирский филиал Российского государственного университета правосудия,
г. Томск
e-mail: it-rigon@mail.ru

A METHOD FOR ENCRYPTING PASSWORDS BASED ON BIOGRAPHICAL FACTS TO IMPROVE THE SECURITY OF ELECTRONIC ACCOUNTS IN FORENSIC CLASSES DURING STAFF TRAINING IN LAW FACULTIES

Yuan Vladimir L.

West Siberian branch of the Russian State University of Justice, Tomsk

Аннотация. В последнее время возросло количество случаев взлома учетных записей пользователей. Среди сервисов и приложений, доступ к которым утрачен, встречаются не только развлекательные сервисы и приложения, но и, связанные с образованием и работой. Часть сервисов хранит большое количество персональных данных пользователей, что приводит к тому, что злоумышленники получают доступ к этим данным для последующего их использования в криминальной деятельности, например, нередки случаи оформления кредитов и займов на пользователей. В рамках преподавания курса «криминалистика» специально для студентов был разработан и использован алгоритм шифрования паролей, основанный на биографических фактах из жизни самих студентов, который предоставляется студентам в рамках темы «Криминалистические методы изучения личности преступника». По окончании занятия, связка с этими паролями остается на руках у самих студентов и никому не демонстрируется, однако, основанные на этой связке записки с паролями могут быть у всех на виду, без опасений взлома, поскольку запись в них была произведена с использованием шифра, в основе которого лежат биографические факты из жизни самих студентов. Преимуществами такого метода являются создание уникального пароля, отсутствие необходимости в

Abstract. Recently, the number of cases of hacking of user accounts has increased. Among the services and applications to which access has been lost are not only entertainment services and applications, but also those related to education and work. Some services store a large amount of personal data of users, which leads to attackers gaining access to this data for their subsequent use in criminal activities, for example, there are frequent cases of issuing loans fraudulent schemes. As part of teaching the “Forensics” course, a password encryption algorithm was developed and used specifically for students, based on biographical facts from the lives of the students themselves, which is provided to students within the framework of the topic “Forensic methods for studying of a criminal personality.” At the end of the lesson, the bundle with these passwords remains in the hands of the students themselves and is not shown to anyone, however, notes with passwords based on this bundle can be in plain sight for everyone, without fear of hacking, since they were recorded using a code in which is based on biographical facts from the lives of the students themselves. The advantages of this method are creating a unique password, the absence of the need to use special programs, applications and services, universality of use in most services and applications, high reliability and protection against hacking by methods associated with brute force password guessing ("brute force") and high protection against decryption.

использовании специальных программ, приложений и сервисов, универсальность использования в большинстве сервисов и приложениях, высокая надежность и защита от взлома методами, связанными с перебором пароля («брутфорс»), и высокая защита от дешифровки.

Недостатками такого метода являются прямая зависимость от фактического знания собственной биографии, дословного знания букв и цифр из этих фактов, значительное время на набор таких паролей для доступа в учетную запись, уязвимость к клавиатурному шпиону («кейлоггеру»), при этом лица, хорошо знающие биографию пользователя, могут осуществить успешный взлом с помощью программы «Hydra». Кроме того, к некоторым сервисам, сайтам, приложениям и программам, на которых установлены ограничения количества знаков в пароле, данный метод не сработает, хотя максимально возможный объем такой пароль займет.

Ключевые слова: Биографический факт, биография, пароли, доступ к учетной записи, информационная безопасность, защита информации, методика обучения, шифрование, учётная запись.

The disadvantages of this method are the direct dependence on actual knowledge of one’s own biography, verbatim knowledge of letters and numbers from these facts, significant time spent typing such passwords to access accounts, vulnerability to a keylogger (“keylogger”), while persons who know the user’s biography well, can carry out successful hacking using the Hydra program. In addition, this method will not work for some services, sites, applications and programs that have restrictions on the number of characters in the password, although such a password will take up the maximum possible space.

Keywords: biographical fact, biography, passwords, account access, information security, information protection, teaching methods, encryption, account.

Для цитирования: Юань В.Л. Применение биографических фактов в вопросах информационной безопасности на занятиях по криминалистике при подготовке кадров на юридических факультетах // Проблемы правовой и технической защиты информации. 2023. №11. С. 61-70.

For citation: Yuan V.L. A method for encrypting passwords based on biographical facts to improve the security of electronic accounts in forensic classes during staff training in law faculties // Legal and Technical Problems Information Protection. 2023. No. 11. P. 61-70.

Введение. С широким внедрением информационных технологий в повседневную жизнь, цифровизацией различных аспектов жизнедеятельности, вопрос оперативного доступа к учетным записям различных электронных сервисом вышел на первый план. Большинство пользователей стараются сохранять вход в различные электронные сервисы: к примеру, в приложениях для обмена сообщениями (мессенджерах), электронной почте, социальных сетях вход выполнен уже очень давно и теперь нет необходимости каждый день заново вводить пароли и проходить проверку личности для получения доступа к учетным записям. Вместе с тем, размещение персональных данных в база данных различных организаций, органов и ведомств, помимо упрощения обмена данными и ускорения документооборота, одновременно создало угрозу кражи злоумышленниками этих данных для последующего использования в криминальной деятельности и взрывной рост числа взломанных учетных записей пользователей был вполне закономерным явлением вместе с ростом количества этих учетных записей, приведшим к поиску

путей их защиты от неправомерного доступа.

В рамках подготовки студентов-юристов на занятиях по криминалистике, очень важно сделать упор на изучение вопросов информационной безопасности, т.к. обучающиеся студенты сами нередко становятся жертвами злоумышленников, которые взламывают их учетные записи, нередко тем самым, нарушая учебный процесс, особенно если речь идет о доступе к сервисам и приложениями, вовлеченным в обучение. На сегодняшний день существует немало способов защиты учетной записи от взлома, большинство из которых сводятся к дополнительным проверкам личности пользователя и создание барьеров для злоумышленников: звонок на мобильный телефон, СМС-сообщение на мобильное устройство пользователя, сообщение на его электронную почту для подтверждения входа в рамках двухступенчатой проверки личности пользователя (т.н. двухфакторная аутентификация), ответ на специальные вопросы, одноразовые пароли и другие методы, хотя универсального способа с надежной защитой учетной записи от взлома пока еще не существует и перечисленные методы имеют свои уязвимости.

С другой стороны, немаловажным является установка надежного и устойчивого ко взлому пароля. Анализ научных исследований, посвященных информационной безопасности и вопросам создания устойчивых ко взлому паролей для учетной записи показал, что в основном рекомендации исследователей сводятся к трем основным принципам создания надежного пароля: пароль должен быть уникальным, длинным и сложным [1, с. 903; 2. с. 119; 3. с. 81-82; 4. с. 24; 5. с. 86; 6. с. 9-10]. Ряд авторов также указывает на необходимость регулярной смены паролей, разумность использования менеджеров паролей и генераторов случайных паролей [1. с. 905; 3. с. 82; 7. с. 229], однако при анализе прикладной ценности этих рекомендаций обнаруживается ряд существенных недостатков:

1. Регулярная смена пароля требует времени, а также запоминания или фиксации факта смены паролей, учитывая тот факт, что многие пользователи имеют множество учетных записей, на практике люди не меняют пароли на своих учетных записях годами.

2. Использование менеджера паролей, как и использование любого другого сервиса сопряжено с обращением к дополнительным инструментам, которыми тоже необходимо учиться пользоваться и подавляющее большинство пользователей предпочитают простые и быстрые решения, исключающие вариант, когда им приходится обращаться к очередному, новому, еще одному инструменту (особенно, электронному).

3. Генераторы случайных паролей создают пароли, которые необходимо потом где-то фиксировать и спрятать и такие пароля среднестатистический пользователь не выучит и даже не будет пытаться.

Встречаются рекомендации создавать пароли путем замены букв на символы [8. с. 159; 2. с. 119], такой метод известен как "mangling", однако, как отмечают авторы, «хотя этот алгоритм является на практике наиболее распространенным, фактически, его недостатки можно сформулировать так: пароли, созданные способом mangling’a трудно запомнить человеку, но легко отгадать машине» [3. с. 80], а «пароли, в которых происходят слишком частые замены символов и в которых используется большое количество букв разных регистров, являются трудными для запоминания» [9. с. 16]. Таким образом, помимо того, что пароль должен быть уникальным, длинным и сложным, он также должны быть доступен для запоминания [10. с. 413] и, по возможности, где-нибудь зафиксирован. По поводу записи, фиксации и хранения паролей на случай его забывания, существует опасность доступа к ним посторонних лиц [11. с. 189], в связи с чем пароль должен быть не только где-нибудь зафиксирован и сохранен, но он должен быть зафиксирован и сохранен в месте, форме и виде, минимизирующему риск получения к нему посторонними лицами

доступа. Все вышесказанное делает задачу создания надежного и устойчивого ко взлому пароля непростой, решение которой, однако, может быть найдено в использовании индивидуальности личности пользователя как ключевого свойства для создания уникального, сложного и длинного пароля, который будет близок, понятен и доступен для запоминания (а чаще всего, запоминать такие вещи людям даже не нужно – они и так это всегда помнят). Само понятие «личность» достаточно обширно изучено в криминалистической науке и ее индивидуальность ярко прослеживается, в первую очередь, в ее биографии [12. с. 198; 13. с. 17; 14 с. 112]. В основе биографии каждого человека лежат биографические факты, особенно важные из которых человек помнит всегда, что может прослеживаться во всем, что он говорит [15. с. 159] или делает, при этом, при создании надежного пароля исследователи не рекомендуют включать свое имя, возраст, год рождения, номер телефона, название города и т.д. [7. с. 229]. Часть таких биографических фактов может быть положена в основу сформированной связки, из которой потом будут создаваться пароля для большого числа учетных записей.

Методика. Методика заключается в том, что биографические факты обучающихся сами по себе становятся основой для универсальной, но в то же время, индивидуальной связки паролей в зашифрованном виде, позволяющем создавать сложные и длинные пароли (от 50 знаков и выше) и при этом, никогда их не забывать. Стоит заметить, что во многом она похожа на предлагаемую в научной литературе методику составления паролей [3. с. 81-82], однако в ее основе лежат не 4 случайных слова, которые необходимо запоминать, а биографические факты из собственной жизни.

На первоначальном этапе, обучающиеся записывают в своих заметках на смартфонах или на листке бумаги связку из 3-5 биографических фактов с использованием английских букв, поскольку многие сервисы, приложения и программы устанавливают требования к языку раскладки, на котором вводится пароль. Это будет Лист №1.

Обычно, предлагается универсальная схема, при этом, сама по себе она будет отличаться у всех студентов, поскольку в ее основе лежат сведения из биографии самих студентов, о которых, как правило, мало кто осведомлен, причем, для шифрования используются именно такие биографические факты, которые содержат в себе еще и цифру: к примеру, если это факт проживания по указанному адресу, то это номер дома и квартиры, если это любимый фильм – то это еще и год премьеры, если это имя, то еще и год рождения и т.д.

Как правило, стандартная методика включает в себя базовую связку из комбинации четырех биографических фактов:

1. Адрес места жительства, с которым связаны самые яркие и теплые воспоминания, включая название улицы, номер дома и номер квартиры (при наличии).
2. Самый любимый фильм или сериал, включая год его премьеры.
3. Фамилия, имя, отчество (при наличии) и дата рождения кумира или любимого музыкального исполнителя, а также актера или актрисы с детства или юности.
4. Кличка, порода и год рождения питомца, который был или который есть до сих пор.

К примеру, это может выглядеть следующим образом:

1. Klueva_49_102
2. Ready_Player_One_2018
3. Drake_Bell_27.06.1986
4. Bimka_German_Shepherd_1995

Первый уровень шифрования включает в себя обозначение каждого биографического факта из сформированной четверки определенным знаком, например:

1. H (Home)=Klueva_49_102
2. F (Film)=Ready_Player_One_2018
3. I (Idol)=Drake_Bell_27.06.1986
4. LP (Lovely Pet) = Bimka_German_Shepherd_1995

На этом уровне достаточно записывать пароли в виде комбинаций из этих

обозначений, при этом, если пароль требуется только в виде цифр (доступ в мобильной приложение Сбербанка или доступ на мессенджер WhatsApp), например:

1. Пароль на Госуслуги: HILPF
2. Пароль в VK.com: IFF
3. Пароль для входа в электронную образовательную платформу, типа Moodle: LPIHI

Исходя из того, что скрывается за этими обозначениями, такие пароли буквально будут выглядеть следующим образом:

1. Пароль на Госуслуги: Klueva_49_102Drake_Bell_27.06.1986Bimka_German_Shepherd_1995Ready_Player_One_2018 – всего 81 знак.
2. Пароль в VK.com: Drake_Bell_27.06.1986Ready_Player_One_2018Ready_Player_One_2018 – всего 63 знака.
3. Пароль для входа в электронную образовательную платформу, типа Moodle: Bimka_German_Shepherd_1995Drake_Bell_27.06.1986Klueva_49_102Drake_Bell_27.06.1986 – всего 81 знак.

Второй уровень шифрования включает в себя обозначение каждой комбинированной связки биографического факта из сформированной четверки определенным знаком, например:

1. Комбинация HI будет впредь обозначаться как 0.
2. Комбинация IF будет впредь обозначаться как A.
3. Комбинация LPIII будет впредь обозначаться как M.
4. Комбинация FIFI будет впредь обозначаться как 29.

На этом уровне необходимо записывать пароли в виде указанных обозначений, например:

1. Пароль на Госуслуги: AM0
2. Пароль в VK.com: M29
3. Пароль для входа в электронную образовательную платформу, типа Moodle: 290

Запись с обозначением комбинаций на втором уровне должна быть произведена на другом листке бумаги – Лист№2.

Исходя из того, что скрывается за этими обозначениями, такие пароли в формате первого уровня буквально будут выглядеть следующим образом:

1. Пароль на Госуслуги: IFLPIIIHI
2. Пароль в VK.com: LPIIIFIFI
3. Пароль для входа в электронную образовательную платформу, типа Moodle: FIFIHI

Эти же пароли в развернутом, буквальном формате будут выглядеть следующим образом:

1. Пароль на Госуслуги: Drake_Bell_27.06.1986Ready_Player_One_2018Bimka_German_Shepherd_1995Drake_Bell_27.06.1986Drake_Bell_27.06.1986Drake_Bell_27.06.1986Klueva_49_102Drake_Bell_27.06.1986 – всего 165 знаков.
2. Пароль в VK.com: Bimka_German_Shepherd_1995Drake_Bell_27.06.1986Drake_Bell_27.06.1986Drake_Bell_27.06.1986Ready_Player_One_2018Drake_Bell_27.06.1986Ready_Player_One_2018Drake_Bell_27.06.1986 – всего 173 знака.
3. Пароль для входа в электронную образовательную платформу, типа Moodle: Ready_Player_One_2018Drake_Bell_27.06.1986Ready_Player_One_2018Drake_Bell_27.06.1986Klueva_49_102Drake_Bell_27.06.1986 – всего 118 знаков.

Дальнейшие уровни шифрования не имеют практического смысла, в связи с чем, для дополнительной защиты от взлома студентам также были предложены два варианта: использование записи комбинаций первого и второго уровней, а также использование спецсимволов, которые обозначают определенную особенность в записи паролей.

К примеру, если взять один пароль из стандартной связки I - Drake_Bell_27.06.1986, то спецсимволы будут изменять его запись, по причине чего, даже если кому-то удастся получить доступ к знанию о том, что скрывается за обозначениями в базовой связке, он все равно будет совершать ошибки в попытке получить доступ к учетной записи, если в него будут заложено использование спецсимвола, значение которого он не знает. Условные обозначения также должны

быть записаны на отдельной бумаге – Лист №3.

1. «Оборотный» – пароль записывается задом наперед [2. с. 19].

Обозначение: <

Итог: 6891.60.72_lleB_ekarD

2. «Языковой» – пароль записывается на русском языке при включенной английской раскладке.

Обозначение: z

Итог: Lhtqr_<tkk_27.06.1986

3. «Полный» – пароль записывается с дополнительными, уточняющими сведениями.

Обозначение: +

Итог: Drake_Bell_27.06.1986_Nickelodeon

4. «Алфавитный» – пароль записывается исключительно с использованием букв, без цифр.

Обозначение: a

Итог: Drake_Bell_Nickelodeon

5. «Цифровой» – пароль записывается исключительно с использованием цифр, без букв.

Обозначение: n

Итог: 27.06.1986

6. «Усеченный» – определенные сегменты пароля исключены. Какие именно сегменты – указываются в виде чисел, соответствующие порядковому номеру знака в пароле.

Обозначение: -3.7.9.11.17

Итог: Drke_el27.061986

7. «Согласные» – пароль записывается исключительно с использованием согласных букв в пароле.

Обозначение: c

Итог: Drk_Bll_27.06.1986

8. «Гласные» – пароль записывается исключительно с использованием гласных букв в пароле.

Обозначение: v

Итог: ae_e_27.06.1986

9. «Инвазивный» – в пароль вводятся посторонние символы и числа. Вначале указывается знак, через тире – указывается порядковый номер знака, после которого этот посторонний знак вводится [2. с. 19].

Обозначение: *-5.#-2.&-10

Итог: Dr#ake*_Bell&_27.06.1986

10. «Интервальный» – в пароль через каждый определенный знак вводится посторонний символ. После знака равенства указывается знак, а после знака "слеш", т.е. символа в виде косой черты, указывается интервал знаков, после которых посторонний символ вписывается.

Обозначение: 8=@/5.%/9

Итог: Drake@_Bel%l@_27.0@6.1%98@6

Как вариант, возможно использование не только спецсимвола, но и порядкового номера в указанном списке, к примеру, вместо спецсимвола «v», можно использовать цифру 8, а вместо спецсимвола «+», цифру 3, что дополнительно запутает потенциального злоумышленника, который не знает, что у спецсимволов могут быть аналоги в виде цифр.

Студентам рекомендуется хранить все записи с их биографическими фактами, которые использованы в базовой связке отдельно от записей комбинаций и обозначений спецсимволов, чтобы при получении доступа к одному, защита учетной записи не была полностью утрачена. Сам листок (Лист №4) с указанием учетных записей на сайтах, сервисах и приложениях с паролями к ним в зашифрованном виде может быть открыт для всех и лежать на столе около компьютера и других устройств без опасения, что им кто-нибудь воспользуется, поскольку без доступа к знанию о том, что обозначают те или иные символы и их комбинации, такие «подсказки» не будут представлять ценности для потенциального злоумышленника. Информация о том, что пароль у студента к госуслугам выглядит как «AM0» ничего не даст.

Результаты. Оценка степени надежности и устойчивости ко взлому паролей, созданных на основе биографических фактов по описанной выше методике, производилась с использованием двух сервисов: Kasperskiy password checker и сервиса на сайте ru.top50vpn.com.

В качестве образца был использован пароль для госуслуг: «Drake_Bell_27.06.1986Ready_Player_One_2

018Bimka_German_Shepherd_1995Drake_Bell_27.06.1986Drake_Bell_27.06.1986Drake_Bell_27.06.1986Drake_Bell_27.06.1986Klueva_49_102Drake_Bell_27.06.1986» без кавычек, длинною в 165 знаков.

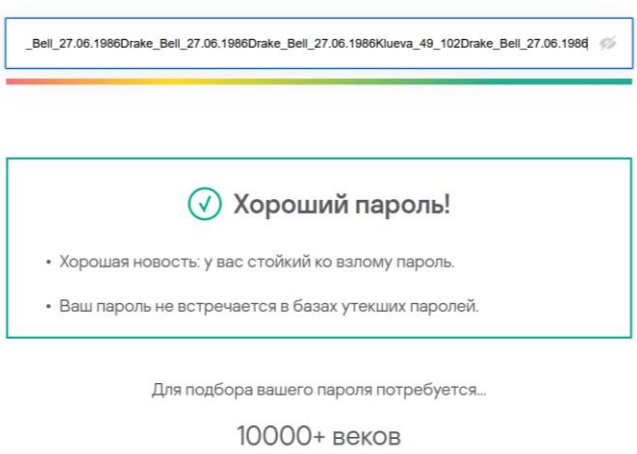

Рисунок 1. Результат проверки надежности пароля AM0 на сайте password.kaspersky.com

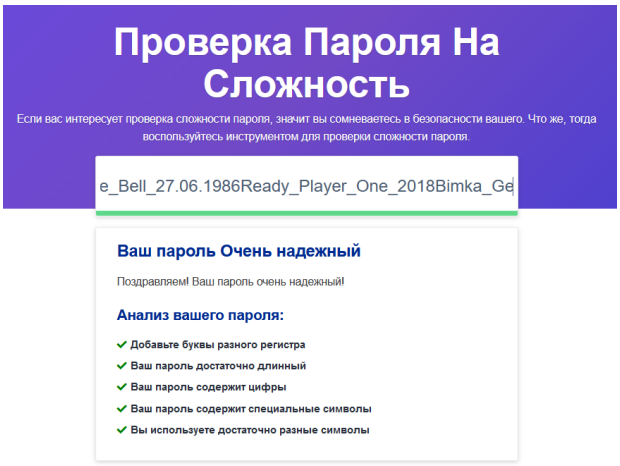

Рисунок 2. Результат проверки надежности пароля AM0 на сайте ru.top50vpn.com

Кроме того, в качестве эксперимента был также проведен анализ степени устойчивости и надежности более короткого пароля типа HF/12: Klueva_49_102Ready_Player_One_2018 длинною 34 знака.

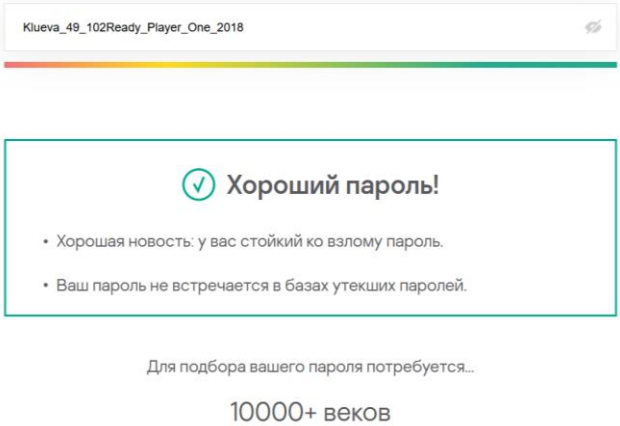

Рисунок 3. Результат проверки надежности пароля HF/12 на сайте password.kaspersky.com

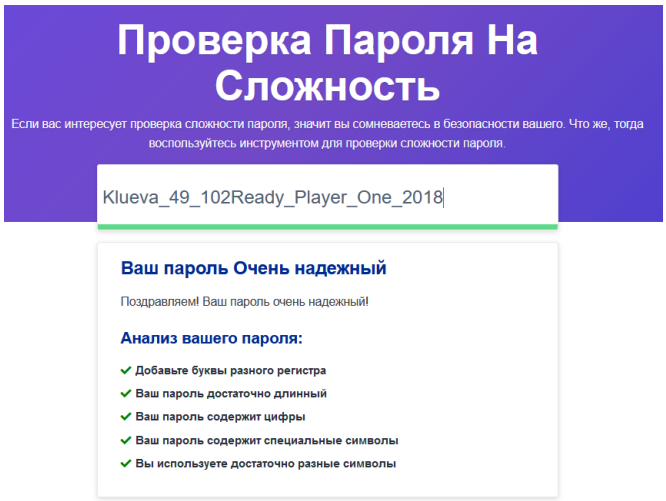

Рисунок 4. Результат проверки надежности пароля HF/12 на сайте ru.top50vpn.com

Вывод по итогам проведенных оценок степени надежности паролей, созданных на основе биографических фактов из жизни пользователя заключается в том, что даже короткие пароли (пароли типа HF/12 длинной в 34 знака), в который заложено всего 2 биографических факта: адрес дома, с которым связаны самые яркие и теплые воспоминания, включая название улицы, номер дома и номер квартиры (при наличии) и название самого любимого фильма или сериала, включая год его премьеры, демонстрирует высокую устойчивость ко взлому. На занятиях по криминалистике студентам следует объяснить, что даже если Лист №4 будет лежать на столе возле устройства, на котором будет написано буквально следующее: vk.com=HF/12, то только сам автор будет знать, что скрывается за этим странным, на первый взгляд, обозначением, ведь именно он самостоятельно создал собственную индивидуальную шифровку.

Следует упомянуть, что от некоторых студентов периодически поступает вопрос: с ростом числа выпускников, прошедших обучение и подготовку, включая знакомство с данной методикой, растет вероятность, что часть из них также могут попытаться получить неправомерный доступ к учетным записям лиц, использующих такую же методике, на что получают ответ, что даже знание о том, что обозначают HF/12 и другие знаки (хотя не факт, что пользователь использовал «стандартные» обозначения, которые выдаются всем студентам на занятиях по криминалистике) не обеспечивает успешный взлом без знания биографических фактов, скрывающихся за этими знаками, вместе с этим, студентам по окончанию занятий все же рекомендуется использовать собственные обозначения, знаки и иные биографические факты из своей жизни.

Преимуществами описанной методики составления паролей на основе собственных биографических фактов являются:

1. уникальность пароля;
2. отсутствие необходимости в использовании специальных программ, приложений и сервисов;
3. универсальность использования в большинстве сервисов и приложениях;
4. высокая надежность и защита от взлома методами, связанными с перебором пароля («брутфорс»);
5. высокая защита от дешифровки.

Недостатками описанной методики составления паролей на основе собственных биографических фактов являются:

1. прямая зависимость от фактического знания собственной биографии, дословного знания букв и цифр из этих фактов;
2. значительное время на набор таких паролей для доступа в учетную запись;
3. уязвимость к клавиатурному шпиону («кейлоггеру»);
4. лица, хорошо знающие биографию пользователя, могут осуществить успешный взлом с помощью программы «Hydra»;

5. не применимо к сервисам, сайтам, приложениям и программам, на которых установлены ограничения количества знаков в пароле.

Прикладная ценность предлагаемой методики составления паролей на основе собственных биографических фактов заключается в следующем:

1. студенты обучаются навыку созданиях сложных и длинных паролей с минимальным риском их забыть или потерять;

2. студенты знакомятся с культурой хранения своих персональных данных и соблюдению конфиденциальности значимых фактов из своей биографии;

3. студенты знакомятся с основами биографического метода в криминалистическом изучении личности.

Готовая связка паролей устранит распространенную проблему выдумывания нового пароля как при необходимости смены прежнего пароля, так и при регистрации новых учетных записей для доступа в новые сервисы и приложения, число которых ежегодно растет. Еще одна практическая ценность данной методики находится за пределами образовательных отношений: так, при расследовании преступлений возникнет необходимость получения доступа к учетным записям пользователя, результаты биографического анализа его личности могут помочь при осуществлении взлома его паролей (к примеру, при помощи программы «Hydra»).

Библиографический список

1. *Кочанова А.Г. Надежные пароли: как их создать и чем они полезны // Международный научный журнал «ВЕСТНИК НАУКИ». 2023. № 6 (63). Т.1. С. 902-908.*

2. *Черкасова Н.В., Нестеренко Е.И. Методы создания надежных паролей и необходимость их применения // Новая наука: Стратегии и векторы развития: Международное научное периодическое издание по итогам Международной научно-практической конференции (19 января 2016 г., г. Ижевск). / в 3 ч. Ч.2. Стерлитамак: РИЦ АМИ, 2016. 204 с. С. 117-119.*

3. *Кубасов И.А. Арясина М.А. Некоторые практические аспекты создания криптостойких и легкозапоминаемых паролей // Вестник Всероссийского института повышения квалификации сотрудников МВД России. 2014. № 3 (31). С. 79-82.*

4. *Лим В.Б. Создание надежных паролей // Проблемы науки. 2021. № 3 (62). С. 23-24.*

5. *Степкин Б.А., Малахов С.В. Как требования к паролю влияют на его безопасность // Скиф. Вопросы студенческой науки. 2021. № 4 (56). С. 83-86.*

6. *Назаров Д.М., Калашников В.Г. Методика проверки надежности пароля с использованием облачных сервисов // Умная цифровая экономика. 2022. Т. 2. № 1. С. 6-11.*

7. *Щукарев И.А. Генератор пароля на основе MATLAB // Проблемы и перспективы экономических отношений предприятий авиационного кластера. Сборник научных трудов VII Всероссийской научной конференции. Ульяновск, 2023. С. 228-234.*

8. *Назаров Д.М. Методика создания надежного пароля для обеспечения экономической безопасности в условиях цифровизации // Известия Санкт-Петербургского государственного экономического университета. 2022. № 1 (133). С. 155-160.*

9. *Глотов А.И., Котилевец И.Д., Иванова И.А. Разработка усовершенствованных генераторов паролей // Ученые записки УлГУ. Сер. Математика и информационные технологии. УлГУ. Электрон. журн. 2021, № 1, С. 13-21.*

10. *Щукарев И.А., Маркова Е.В. Разработка генератора паролей с использованием GUI MATLAB // Программные продукты и системы. 2022. № 3. С. 413-419.*

11. *Цыбикова Т.С. Менеджеры паролей // Инновационные технологии в науке и образовании. Материалы V Всероссийской научно-практической конференции с международным участием. Отв. ред. Е.Р. Урмакшинова, С.Л. Буянтуев. 2017. С. 188-192.*

12. *Ведерников Н.Т. Биографический метод исследования личности: криминалистический и уголовно-процессуальный аспект // Вестник Томского государственного университета. 2019. № 449. С. 197–200.*

13. Ахмедшин Р.Л. Лекции по правовой психологии : учебное пособие. Томск : Издательский Дом Томского государственного университета, 2019. 454 с.

14. Юань В.Л. Биографический метод как базовый метод изучения личности допрашиваемого перед допросом // Проблемы использования криминалистических знаний в правоприменительной деятельности : материалы Всероссийской научной конференции, посвященной 30-летию кафедры криминалистики ЮИ ТГУ, 30 января - 1 февраля 2014. г. Томск, 2014. С. 112-114.

15. Алексеева Т.А. Криминалистическая характеристика содержательности как структурного элемента устной речи // Вестник Томского государственного университета. 2014. № 378. С. 159–161.