Шаханова М. В., Сидоров М.М, Шаханова Д.С. Проектирование системы защиты персональных данных организации // Международный журнал информационных технологий и энергоэффективности. – 2022. – Т. 7 № 3(25) часть 3 с. 43–50

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056.53

ПРОЕКТИРОВАНИЕ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ОРГАНИЗАЦИИ

Шаханова М. В., Сидоров М.М., Шаханова Д.С.
Морской государственный университет имени Г.И. Невельского, Владивосток, Россия (690003, г. Владивосток, ул. Верхнепортовая, д.50а), e-mail: marinavl2007@yandex.ru

В современном мире сложно найти человека совершеннолетнего возраста, персональные данные которого не хранились бы на каком-нибудь сервере на необъятных просторах всемирной паутины. Это и социальные сети, и данные заемщиков / вкладчиков в банки, и порталы государственных услуг. Персональные данные человека мошенники используют в своих корыстных неблаговидных целях. За последние годы в разы увеличились случаи компрометации баз данных с персональными данными клиентов банков, социальных учреждений и т.д. Основной способ компрометации персональных данных пользователей состоит во взломе баз данных аккаунтов или компрометации паролей пользователей. В настоящей статье изложены основные концептуальные решения проекта системы защиты аккаунтов пользователей от компрометации персональных данных.

Ключевые слова. Защита данных, персональные данные, информационная система, авторизация, пароль, управление данными, хеширование, модель, UML.

DESIGNING THE ORGANIZATION'S PERSONAL DATA PROTECTION SYSTEM

Shakhanova M. V., Sidorov M.M., Shakhanova D.S.
G.I. Nevelsky Maritime State University, Vladivostok, Russia (690003, Vladivostok, st. Verkhneportovaya, 50a), e-mail: marinavl2007@yandex.ru

In the modern world, it is difficult to find a person of legal age whose personal data would not be stored on some server on the vast expanses of the World Wide Web. These are social networks, data of borrowers /depositors to banks, and portals of public services. Fraudsters use a person's personal data for their own selfish, unseemly purposes. In recent years, the cases of compromising databases with personal data of customers of banks, social institutions, etc. have increased significantly. The main way to compromise users' personal data is to hack account databases or compromise user passwords. This article outlines the main conceptual solutions for the project of a system for protecting user accounts from compromising personal data.

Keywords: Data protection, personal data, information system, authorization, password, data management, hashing, model, UML.

Введение.

Персональные данные являются неотъемлемой частью современных информационных систем практически любой сферы (банковские, образовательные, социальные, здравоохранения, сервисы распространения и оказания услуг и торговли и т.д.). Все персональные данные охраняются Федеральным законом РФ от 27 июля 2006 года № 152-ФЗ «О персональных данных». Данный закон регулирует отношения, связанные с обработкой персональных данных, осуществляемой, в частности, поликлиникой [3]. Целью Федерального

закона № 152-ФЗ является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

В соответствии с ФЗ персональными данными является любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). В соответствии со ст. 5 № 152-ФЗ хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

В соответствии со ст. 6 № 152-ФЗ обработка персональных данных субъекта возможна только с его письменного согласия. При этом операторы, обрабатывающие персональные данные, обязаны не раскрывать их третьим лицам в любых случаях, не предусмотренных законом.

Анализ полного состава документа № 152-ФЗ «О персональных данных» показывает, что персональные данные пациентов поликлиники должно храниться в защищенном хранилище, недоступном третьим лицам. Хранилище должно предусматривать прямую защиту от компрометации техническими и социальными методами. Пользователи, имеющие доступ к персональным данным в хранилище, должны быть строго разграничены в доступе к тем данным, которыми они будут оперировать при выполнении своих прямых обязанностей.

Таким образом, над хранилищем персональных данных требуется служба верхнего уровня, отвечающая за делегирование полномочий доступа пользователей к персональным данным. Такой службой может быть административная оболочка базы данных в СУБД, либо клиентское приложение, которое будет организовывать работу с персональными данными. Таким образом, защита информации от угроз реализуется процедурой авторизации пользователей и ограничений их прав доступа к функциям и данным и определяется следующими правилами, которые являются частью политики информационной безопасности:

- операторские компьютеры, работающие с персональными данными, рекомендуется заблокировать паролем, известный только компетентным лицам;
- применение на операторских компьютерах антивирусного программного обеспечения;
- блокировка свободных портов коммутаторов и свитчей, входящих в состав сетевой инфраструктуры поликлиники;
- защита СУБД;
- проверка введенных пользователем данных на корректность;
- резервное создание дампа БД.

Проектирование системы защиты персональных данных организации.

Основа защиты персональных данных состоит в использовании надежной и эффективной системе хранения паролей пользователей информационных систем.

Первый аспект создания надежных паролей состоит в создании и введение в действие системы администрирования паролей пользователей. По-другому, пользователей необходимо обязать создавать наиболее защищенные пароли, которые будут в наименьшей степени поддаваться простому угадыванию и подбору. Очевидно, что пароль «123456» подобрать в разы легче, чем, например, «_0Rtk+!93=q». Для построения эффективной системы администрирования паролей должны быть предусмотрены следующие правила их формирования:

- ограничение пароля по минимальной длине;
- требование к паролю содержания символов из различных групп (буквы, заглавные и строчные, цифры, спецсимволы);
- установка максимального срока действия пароля, по истечении которого пароль необходимо заменить;
- ведение журнала истории паролей и слежение за несовпадением нового пароля с ранее использованными;
- автоматическая генерация пароля в соответствии с вышеперечисленными правилами.

Подсистема авторизации в информационной системе, также должна предусматривать средства для защиты от компрометации, попыток подбора пароля. Например:

- использование задержки (5-10 секунд) при вводе неправильного пароля;
- использование «капчи»;
- ограничение количества попыток на ввод пароля;
- блокировка пользователя после, например, трех попыток неправильного ввода пароля (распространено в банкоматах).

В соответствии с текущими задачами информационных систем, их спецификой, может быть предложена подсистема администратора (ответственного за информационную безопасность), в которой тот будет иметь инструмент гибкой настройки правил установки и использования паролей пользователей. Пример макета интерфейса такой подсистемы приведен на рисунке 1 (рисунок выполнен в редакторе визуальных форм среды разработки Microsoft Visual Studio 2015).

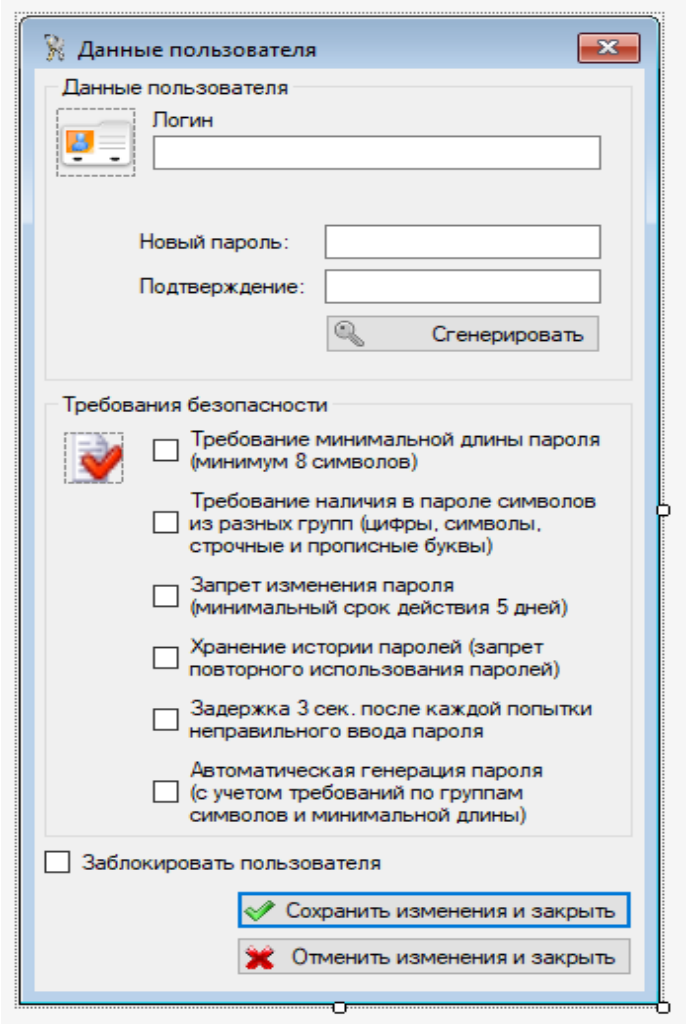

Рисунок 1 – Пример макета интерфейса подсистемы гибкой настройки правил установки и использования паролей пользователей

Атаки злоумышленников не всегда направлены на попытке подбора пароля. Нередки случаи, когда злоумышленник получает доступ к базе данных аккаунтов пользователей. В этом случае все пароли становятся доступными ему. Поэтому в современных системах давно уже не принято хранить пароли пользователей в открытом виде. Наиболее распространенный способ защиты пароля – хеширование.

Одним из ключевых требований для криптографических хеш-функций является условие, при котором при атомарном (то есть самом малом) изменении аргумента функции ее выходное значение менялось кардинально. Такое условие при его соблюдение обеспечит невозможность утечки информации по значению хеш-функции при незначительном изменении аргумента. Среди множества существующих хэш-функций принято выделять криптографически стойкие, применяемые в криптографии. Как правило, криптографическая стойкость хэш-функции обеспечивается следующими свойствами [1]:

- стойкость к коллизиям первого рода (необратимость): для заданного сообщения M должно быть практически невозможно подобрать другое сообщение M` имеющее такой же хэш. Это свойство также называется необратимостью хэш-функции;
- стойкость к коллизиям второго рода: должно быть практически невозможно подобрать пару сообщений (M, M`) с одинаковым хэшем.

Для увеличения устойчивости хешированных паролей к взлому перед хешированием к исходному паролю добавляется случайная последовательность символов, которая на сленге криптографии получила название «соль». Соль (модификатор входа хэш-функции) — строка данных, которая передаётся хеш-функции вместе со входной строкой (прообразом) для вычисления хэша (образа) [4]. Цель использования «соли» – усложнение определения прообраза хэш-функции методом перебора по словарю возможных входных значений (прообразов), включая атаки с использованием «радужных» таблиц.

При использовании одинаковых паролей «соль» сгенерирует различные хеши, что должно добавить дополнительную сложность для злоумышленников. На практике лучше применять статическую и динамическую «соль». Статическая «соль» – постоянная случайная строка, которая добавляется ко всем паролям. Динамическая «соль» генерируется индивидуально по заданному алгоритму для каждого пароля [2]. Использование динамической составляющей «соли» имеет дополнительное преимущество в случае, когда пользователь использует одинаковый пароль на нескольких ресурсах сразу, а злоумышленнику стал известен из его хешей. В этом случае использование динамической соли позволяет избежать компрометации аккаунтов пользователя на нескольких веб-сервисах сразу [5]. Для построения эффективной защиты пароля предлагается:

- использование алгоритма хеширования, например, SHA256;
- для повышения устойчивости пароля к взлому перед хешированием добавлять «соль» из трех компонентов.

Первым компонентом соли (SALT1) будет являться динамическая константа, которая будет генерироваться при каждом изменении пароля в виде десяти случайных символов. Данная константа будет записываться в базу данных в открытом виде рядом с хешем пароля. Основное назначение данной части «соли» – ввести в заблуждение злоумышленника, у которого получилось скомпрометировать базу аккаунтов пользователей: он будет ошибочно полагать, что «соль» ему известна, хотя это далеко не так.

Второю часть «соли» (SALT2), которая также будет динамической, можно формировать по следующему алгоритму:

- перевод даты создания аккаунта пользователя (должен храниться в таблице аккаунтов в БД) в строку Sdate формата «dd.mm.yyyy hh:MM» (dd – день в виде числа из двух знаков, mm – месяц в виде числа из двух знаков, yyyy – год в четырехзначном формате, hh, MM – соответственно, часы и минуты в формате двух знаков);
- получение строки Slog путем поочередной конкатенации символов (выбираются по одному), составляющих логин пользователя (хранится в таблице аккаунтов), и компонентов строки Sdate (день, месяц, год, часы, минуты); например, если логин пользователя – LOGIN, а дата создания его аккаунта – 11.04.2021 11:04, то полученная строка Slog будет иметь вид «M11Y04L2021O11G04IN»;
- шифрование полученной строки Slog методом таблиц Вижинера, причем для ключа шифрования по таблицам будет использоваться третий компонент «соли» (SALT3).

Таким образом, динамическая часть «соли» будет иметь достаточно сложный алгоритм формирования и, соответственно, хорошую защищенность от компрометации. Последний компонент «соли» (SALT3) будет являться системной константой (12 символов), которая будет храниться не в базе данных, а локально (например, в конфигурационном файле системы). Итоговая «соль» будет являться конкатенацией всех трех компонентов. Таким

образом, перед хешированием в конец пароля будет подмешиваться «соль» общей длиной не менее 42 символов, которая будет формироваться по сложному алгоритму и будет более, чем надежной. Полученный пароль перед помещением в базу данных будет хешироваться методом SHA256. На рисунке 2 показана схема создания хеша пароля перед помещением его в таблицу аккаунтов базы данных.

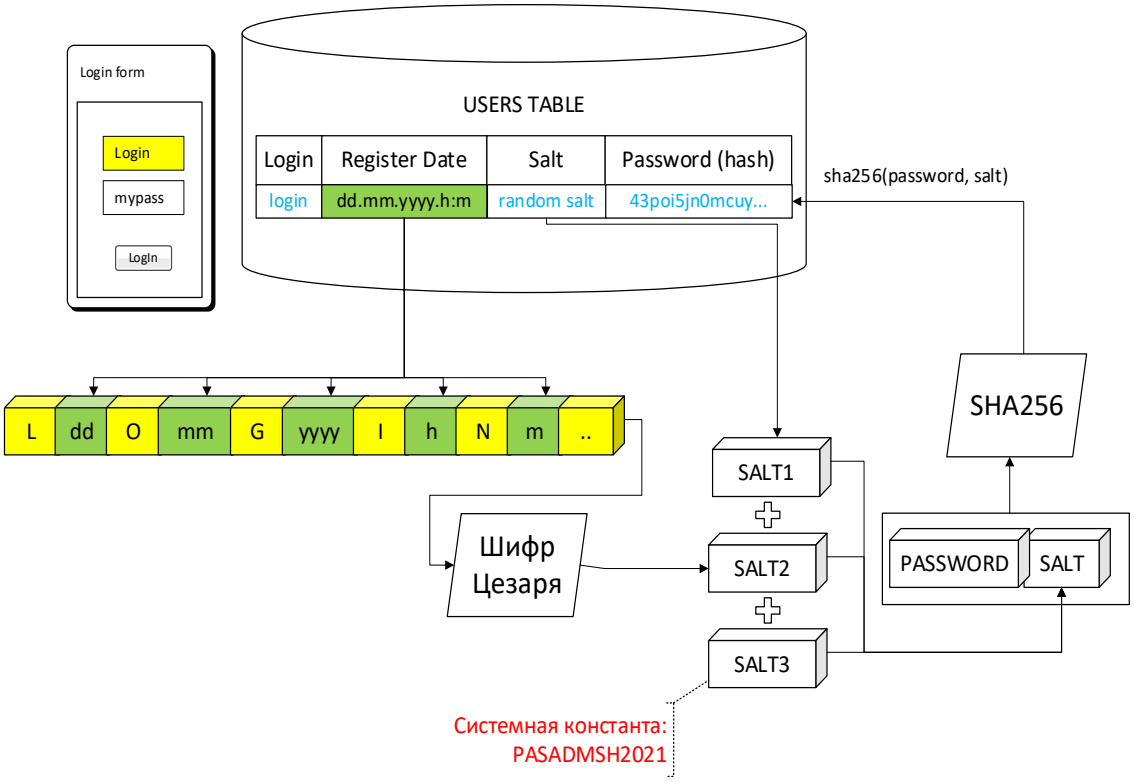

Рисунок 2 – Схема хеширования пароля

Таким образом, описанная концептуальная схема защиты паролей пользователей будет обеспечивать дополнительную надежность и высокую устойчивость к компрометации персональных данных злоумышленниками. На Рисунке 3 приведена UML-диаграмма активности, в соответствии с которой можно реализовывать прецедент авторизации пользователя в информационной системе.

Заключение.

Таким образом, предложенный проект системы защиты персональных данных пользователей способен защитить от:

- методов подбора пароля как ручным способом, так и с использованием специализированных программ;
- получения авторизационных данных пользователей при успешной компрометации базы аккаунтов.

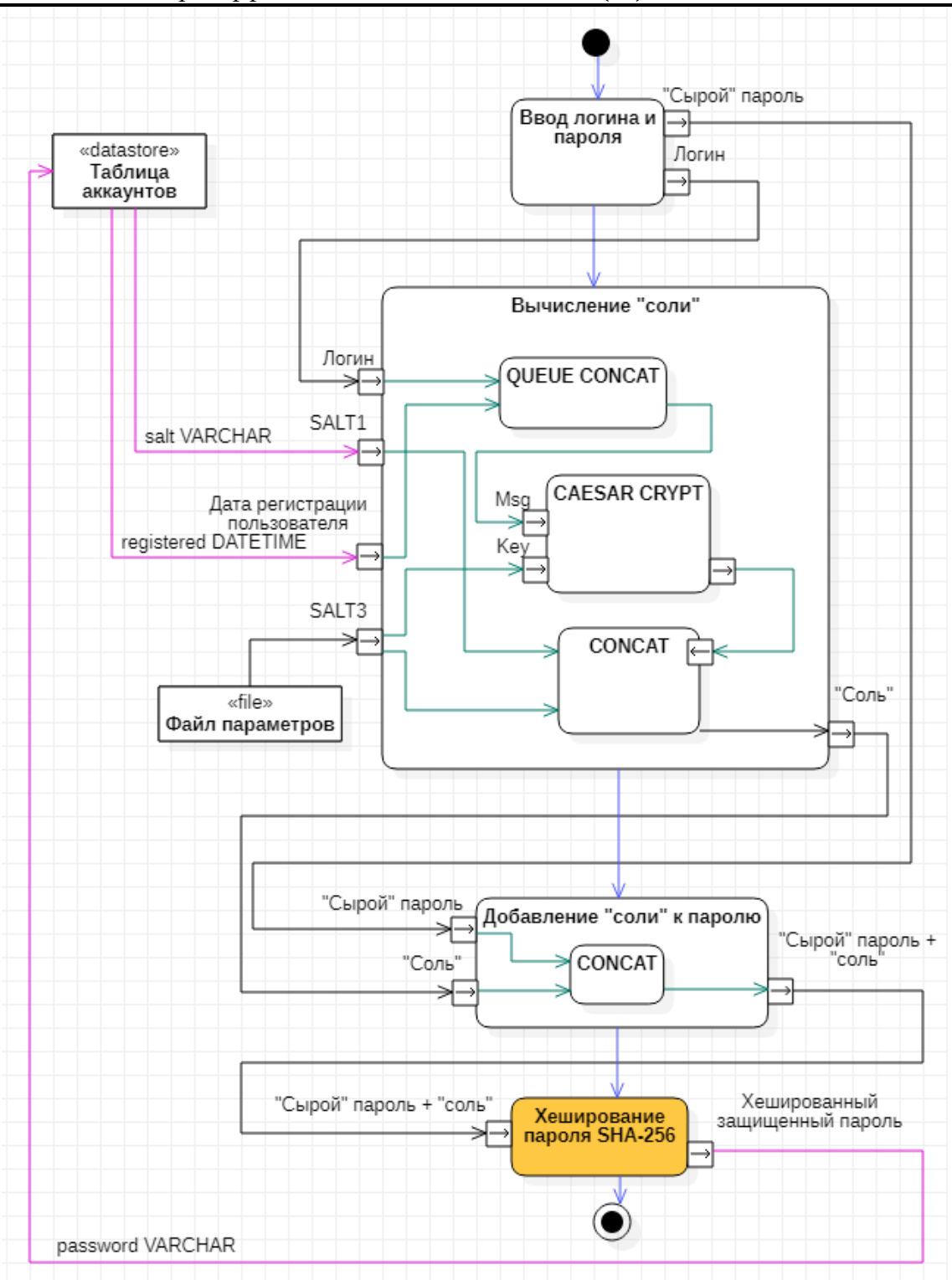

Рисунок 3 – Диаграмма активности прецедента авторизации пользователя в информационной системе

Список литературы

1. ГОСТ Р 34.11-94. Информационная технология (ИТ). Криптографическая защита информации. Функция хеширования / М.: Издательство стандартов, 1994
2. Интернет-технологии.ру. «Солёное» хеширование паролей: делаем правильно [Электронный ресурс] URL: https://www.internet-technologies.ru/articles/solenoe-

heshirovanie-paroley-delaem-pravilno.html (дата обращения: 01.10.2022 г.)
3. Российская Федерация. Законы. О персональных данных. Федеральный закон от 27.07.2006 N 152-ФЗ [принят Государственной Думой 8 июля 2006 г.: одобрен Советом Федерации 14 июля 2006 г.]
4. Ященко, В.В. Введение в криптографию / изд. 4-е доп. – М.: МЦНМО, 2012. – 341 с.
5. Club.CNews.ru. 52% пользователей используют одинаковые пароли на разных сайтах [Электронный ресурс] URL: https://club.cnews.ru/ blogs/entry/52_polzovatelej_ispolzuyut_odinakovye_paroli_na_raznyh_sajtah (дата обращения: 01.10.2022 г.)

References

1. . GOST R 34.11-94. Information technology (IT). Cryptographic protection of information. Hash function / M.: Publishing house of standards, 1994
2. Internet technologies.ru. "Salted" password hashing: doing it right [Electronic resource] URL: https://www.internet-technologies.ru/articles/solenoe-heshirovanie-paroley-delaem-pravilno.html
3. Russian Federation. Laws. About personal data. Federal Law No. 152-FZ of July 27, 2006 [adopted by the State Duma on July 8, 2006: approved by the Federation Council on July 14, 2006]
4. Yashchenko, V.V. Introduction to cryptography / ed. 4th add. – M.: MTsNMO, 2012. – 341 p.
5. Club.CNews.ru. 52% of users use the same passwords on different sites. Club.CNews.ru. 52% of users use the same passwords on different sites [Electronic resource] URL: https://club.cnews.ru/ blogs/entry/52_polzovatelej_ispolzuyut_ odinakovye_paroli_na_raznyh_sajtah (date of access: 01.10.2022)