УДК 004.056.53, 004.422.832

Рекомендации по разработке менеджеров паролей для ОС Андроид

А. В. Черников
Пермский национальный исследовательский государственный университет; г. Пермь, Россия
arsenyperm@mail.ru; ORCID ID 0000-0001-9430-3587, AuthorID 552297

Рассматриваются существующие менеджеры паролей в операционной системе (далее ОС) Андроид: функционал, возможности, проблемы применения. За предмет исследования взяты как платные, так и бесплатные версии менеджеров паролей, как с открытым исходным кодом, так и с закрытым. В результате проведенного анализа делаются выводы и приводятся рекомендации о необходимости или внедрения дополнительных функций в существующие решения, или разработку нового менеджера паролей с исключенными проблемами.

Ключевые слова: *информационная безопасность; менеджер паролей; операционная система Андроид*

Поступила в редакцию 10.10.2021, принята к опубликованию 10.11.2021

Recommendations for developing password managers of Android OS

A. V. Chernikov
Perm State University; Perm, Russia
arsenyperm@mail.ru; ORCID ID 0000-0001-9430-3587, AuthorID 552297

The paper examines the existing password managers in the Android operating system (hereinafter OS): functionality, capabilities, application problems. For the subject of research, both paid and free versions of password managers, both open source and closed, were taken. As a result of the analysis, conclusions are drawn and recommendations are made on the need for either the introduction of additional functions into existing solutions, or the development of a new password manager with excluded problems.

Key words: *information security; password manager; operating system Android*

Received 10.10.2021, accepted 10.11.2021

DOI: 10.17072/1993-0550-2021-4-49-57

Введение

На сегодняшний момент существование человека без информационных технологий невозможно представить. Компьютер, смартфон, планшет являются обязательной частью нашей жизни. Человек повседневно использует множество Интернет-ресурсов: сайты, электронная почта, социальные сети и т.д. При этом для соблюдения правил информационной безопасности для доступа к любым ресурсам требуется ввести логин и пароль (пройти процесс аутентификации/идентификации). Но, как известно, применение логинов и паролей не всегда безопасно, и поэтому существует ряд правил, увеличивающих надежность паролей. Одним из таких правил становится уникальности/неповторяемость пароля – один пароль используется один раз для одного ресурса.

Но представить, что человек будет выполнять это требования и придумывать/запоминать огромное количество паролей невозможно. Поэтому либо данное правило не принимают во внимание, и создаются простые одинаковые/однотипные пароли, либо записывают пароли в блокнот, в текстовый документ (но и при этом, в основном, правило не выполняется).

Решить эту проблему (теоретически) позволяют менеджеры паролей – приложения/программы, которые генерируют/хранят/выдают по требованию пользователя логины пользователей и их пароли [3]. Менеджеры паролей дают пользователям возможности легко и просто генерировать/использовать уникальный и надежный пароль для каждого электронного ресурса, требующего аутентификации по паролю. Теперь пользователю не стоит задумываться о придумывании и запоминании множества логинов и паролей, а достаточно только знать один пароль, с помощью которого он получает доступ к менеджеру паролей. Отличное и главное, простое и удобное решение, но одна решенная задача порождает другие: безопасность самого менеджера паролей и одна из проблем – конфиденциальность данных, содержащихся в менеджере паролей. Необходимо уделять особое внимание безопасному хранению информации и быть уверенным, что всеми данными, которые хранит менеджер паролей, не завладеет злоумышленник [7, 18]. Есть и другая проблема: не все пользователи готовы полностью доверять свои конфиденциальные данные менеджерам паролей [3].

Поэтому проблема безопасного хранения логинов и паролей пользователя, проблема безопасного хранения учетных данных пользователя в менеджерах паролей – крайне важный вопрос в области информационной безопасности на сегодняшний день. Данная проблема актуальна на сегодняшний день еще и потому, что с ростом популярности менеджеров паролей увеличивается и интерес злоумышленников к таким приложениям. Их методы несанкционированного доступа к данным пользователей становятся все более широкими (разрабатываются новые методы атак и организации НСД), поэтому функции защиты информации (во всей области) должны совершенствоваться (не привязываясь только к менеджерам паролей) и быть способными противостоять современным угрозам.

1. Обзор существующих менеджеров паролей

Сегодня для тех или иных ОС разработано большое количество программ/приложений для хранения логинов и паролей, как встроенных в ОС, встроенных в браузер, отдельных приложений и мобильных приложений. Однако существуют и аппаратные и аппаратно-программные комплексы менеджеров паролей – электронные/программно-электронные устройства, которые в памяти хранят логины и пароли. Срок существования на рынке таких программ и/или устройств велик и насчитывает уже два десятилетия, но есть и средства, разработанные недавно (5 лет и менее). Среди них есть менеджеры паролей, завоевавшие популярность и имеющие большую аудиторию пользователей. В рамках данной работы в соответствии с целью исследования будут рассмотрены только несколько таких приложений.

Для удобства выделим отдельные две группы по реализации: менеджеры паролей, имеющие в составе аппаратную часть, и менеджеры паролей, построенные только на программных компонентах.

1.1. Программные менеджеры паролей

Для анализа были выбраны четыре наиболее популярных менеджера паролей [10], отдельно стоит заметить, что все они являются кроссплатформенными и могут работать не только в среде ОС Андроид:

– 1Password;
– LastPass;
– Dashlane;
– KeePass.

Так как выбранные менеджеры паролей являются наиболее популярными, то количество установок их максимально, и, следовательно, имеется большое количество различных отзывов и оценок. К сожалению, они стали и объектами исследований злоумышленников, желающих заполучить логины и пароли пользователей. Поэтому выбранные менеджеры паролей представляют наибольший интерес для работы.

Ниже приведены общие характеристики для менеджеров паролей, представленные в работе [2], по которым необходимо провести сравнение:

– тип аутентификации;
– место хранения данных;

– используемый алгоритм шифрования базы данных;

– наличие генератора паролей;

– возможность восстановления данных;

– возможность синхронизации между устройствами;

– реализация в виде облачного сервиса;

– необходимость в регистрации;

– доступ к исходным кодам приложения.

Среди вынесенных в текст работы характеристик были выделены те, которые в той или иной степени затрагивают проблемы безопасности менеджеров паролей, и проведен анализ того подхода, который был выбран разработчиками к реализации функции.

Стоит отметить, что не все характеристики менеджеров паролей можно найти в открытом доступе, поэтому далее будут приведены те данные, которые можно получить из открытых источников.

Краткая информация по характеристикам программных менеджеров паролей представлена ниже в табл. 1 и табл. 2.

Таблица 1. *Характеристики программных менеджеров паролей ОС Андроид 1Password и LastPass*

	1Password	**LastPass**
Тип аутентификации	Двухфакторная	Двухфакторная
Место хранения данных	Локально/Удаленно	Удаленно
Алгоритм шифрования базы данных	AES-256	AES-256
Наличие генератора случайных паролей	Есть	Есть
Возможность восстановления данных	Есть	Есть
Возможность синхронизации между своими устройствами	Есть	Есть
Облачный сервис	Есть	Есть
Необходимость регистрации	Есть	Есть
Открытый исходный код	Нет	Нет

Таблица 2. *Характеристики программных менеджеров паролей ОС Андроид Dashlane и KeePass*

	Dashlane	**KeePass**
Тип аутентификации	Двухфакторная	Двухфакторная
Место хранения данных	Локально/Удаленно	Локально/Удаленно
Алгоритм шифрования базы данных	AES-256	AES-256
Наличие генератора случайных паролей	Есть	Есть
Возможность восстановления данных	Есть	Нет
Возможность синхронизации между своими устройствами	Есть	Есть
Облачный сервис	Нет	Есть
Необходимость регистрации	Есть	Есть
Открытый исходный код	Нет	Есть

1.1.1. Шифрование данных

Все менеджеры паролей хранят базу данных паролей в зашифрованном виде. Алгоритм шифрования – стандарт AES-256. Пароль от менеджера паролей и ключи шифрования данных хранятся на устройстве пользователя.

1.1.2. Двухфакторная аутентификация

Рассматриваемые менеджеры паролей предоставляют возможность настройки двухфакторной аутентификации для разблокировки приложения при наличии, возможно, организации такого типа аутентификации. В качестве второго этапа, в основном, используется проверка биометрических данных (отпечаток пальца).

1Password использует протокол SRP для аутентификации учетных данных пользователя без отправки пароля от менеджера паролей по сети [1]. Так как SRP протокол эффективно реализует аутентификацию между пользователем и сервером, хранящим информацию о его пароле, то во время передачи пароль украсть невозможно.

1.1.3. Восстановление доступа

Вопрос восстановления учетных данных пользователя и базы данных своих логинов и паролей очень важен для разработчиков и ему уделяется большое внимание. Разработчики решают проблему по-разному.

1Password решает эту проблему следующим образом: созданием семейной или командной учетной записи, и в случае утери пароля от менеджера паролей и секретного-ключа, доступ могут восстановить только люди, которые принадлежат кругу доверенных лиц [1].

KeePass: в случае утери пароля менеджера паролей для базы данных, функция восстановления не реализована, и данные окажутся зашифрованными навсегда [8].

LastPass и **Dashlane**: для Андроид ОС версии предусмотрен сброс пароля с помощью биометрических данных. В остальных случаях расшифровать базу данных паролей не представляется возможным [5, 9].

1.1.4. Открытый исходный код

Все рассматриваемые приложения, за исключением KeePass, являются коммерческими предложениями, поэтому их исходные коды закрыты. Однако разработчики заявляют, что приложения были разработаны с учетом всех стандартов безопасности.

Исходный код **KeePass** размещен на GitHub [8]. Открытый код позволил заинтересованным пользователя заняться его исследованием и усовершенствованием, а некоторые на его основе разработали собственные менеджеры паролей.

1.2. Программно-аппаратные менеджеры паролей

Для анализа были выбраны также четыре наиболее популярных аппаратных менеджера паролей [10]:

– Mooltipass Mini;
– Trezor Password Manager;
– Hideez Key;
– Pastilda.

Аналогично программными менеджерами паролей рассмотрим основные функции, затрагивающие вопросы безопасности данных пользователя.

Краткая информация по характеристикам программно-аппаратных менеджеров паролей представлена ниже в табл. 3 и табл. 4.

Таблица 3. *Характеристики программно-аппаратных менеджеров паролей ОС Андроид Mooltipass Mini и Trezor Password Manager*

	Mooltipass Mini	**Trezor Password Manager**
Тип аутентификации	Двухфакторная	Двухфакторная
Место хранения данных	Локально	Удаленно
Алгоритм шифрования базы данных	AES-256	AES-256
Канал передачи данных	Прямое подключение через USB порт	Прямое подключение через USB порт
Наличие генератора случайных паролей	Есть	Есть
Возможность восстановления данных	Есть	Есть
Возможность синхронизации между своими устройствами	Есть	Есть
Облачный сервис	Есть	Есть
Необходимость регистрации	Есть	Есть
Открытый исходный код	Есть	Нет

Таблица 4. *Характеристики программных менеджеров паролей ОС Андроид Dashlane и KeePass*

	Hideez Key	**Pastilda**
Тип аутентификации	Двухфакторная	Двухфакторная
Место хранения данных	Локально	Локально
Алгоритм шифрования базы данных	AES-256	AES-256
Канал передачи данных	Прямое подключение через BlueTooth	Прямое подключение через USB порт
Наличие генератора случайных паролей	Есть	Есть
Возможность восстановления данных	Нет	Нет
Возможность синхронизации между своими устройствами	Есть	Есть
Облачный сервис	Нет	Есть
Необходимость регистрации	Есть	Есть
Открытый исходный код	Нет	Есть

1.2.1. Хранение и шифрование данных

Все устройства, за исключением **Trezor Password Manager**, хранят данные локально, в собственной памяти устройства в зашифрованном виде. **Trezor** в качестве хранилища зашифрованной базы данных использует удаленное хранилище DropBox.

Разработчики **Pastilda** за основу базы данных паролей взяли открытое решение **KeePass** [19]. Следовательно, алгоритмы шифрования используются аналогичные программному менеджеру паролей **KeePass**.

В остальных устройствах база данных шифруется алгоритмом стандарта AES-256.

1.2.2. Каналы передачи данных

Подходы к реализации каналов передачи данных и представленных программно-аппаратных решений менеджеров паролей различны. Разработчики **Trezor**, **Pastilda** и **Mooltipass** взаимодействует с устройствами через USB порт, подсоединяются также через USB порт, но эмулируют стандартную клавиатуру, **Hideez Key** передает данные по Bluetooth каналу [12].

1.2.3. Восстановление доступа

В данной характеристике **Trezor** предлагает решение по восстановлению доступа к данным путем ввода секретной фразы, состоящей из 24 слов. При первоначальной установке менеджера паролей эта фраза генерируется программой, и пользователю рекомендуется ее сохранить. При утере пароля от менеджера паролей эта фраза гарантированно восстановит доступ к менеджеру паролей [15].

Разработчики **Mooltipass** приняли решение о вводе кода, генерируемого при установке программы, и три неверных попытки ввода кода навсегда заблокируют устройство без возможности восстановления данных [14].

Остальными разработчика функция восстановления не предусмотрена [17].

1.2.4. Открытый исходный код

Pastilda разрабатывалась как решение с открытым исходным кодом.

Mooltipass с самого начала проекта публикуют все, что входит в **Mooltipass**, в репозитории на GitHub.

Разработчики остальных аппаратных менеджеров паролей не предоставляют исходный код менеджера паролей.

1.3. Преимущества и недостатки менеджеров паролей

В результате анализа менеджеров паролей можно выделить следующие достоинства и недостатки программных/программно-аппаратных средств с точки зрения безопасности: менеджеры паролей упрощают работу пользователей с системами аутентификации электронных ресурсов и выводят управление паролями на более высокий уровень безопасности. Но есть и проблемы, связанные с использованием менеджера паролей. Далее рассмотрим подробнее преимущества и недостатки.

Преимущества:

– сложность паролей. При использовании менеджера паролей можно сгенерировать в качестве пароля случайные последовательности, стойкие к различным атакам;

– хранение паролей в зашифрованном виде. Логины и пароли независимо от места хранения хранятся в зашифрованном виде;

– защита от фишинговых атак. Функция автоматического ввода логина-пароля на сайте помогает пользователям защититься от фишинговых атак, поскольку логин и пароль жестко привязаны к доменному имени.

Недостатки:

– ошибки программной реализации, программного кода. При разработке менеджера паролей может быть допущена ошибка, приводящая к уязвимости, и это находится в интересах злоумышленников. Но от этого не застраховано не одно приложение/программа;

– утеря всех паролей одновременно. После того, как пользователь сгенерировал пароли случайными образом через менеджера паролей, он не сможет вспомнить их из-за сложности генерации. Если пользователь забудет или потеряет пароль от менеджера паролей, то потеряет все. В некоторых менеджерах существуют варианты восстановления;

– подверженность атакам злоумышленников. Очевидно, что если пароль от менеджера паролей будет скомпрометирован, то все остальные пароли, хранящиеся в памяти устройства, также будут скомпрометированы.

Но, не смотря на выявленные недостатки, эксперты в области информационной безопасности сходятся во мнении, что использовать доверенные менеджеры паролей для обеспечения безопасности работы с электронными ресурсами надежнее, чем осуществлять запись паролей в файл или блокнот [13].

2. Анализ уязвимостей менеджеров паролей

После анализа существующих менеджеров паролей и выявления их достоинств и недостатков необходимо учесть, что, если эти приложения и устройства могут облегчить жизнь пользователя, избавив от необходимости запоминания множества различных паролей, предоставив удобный интерфейс и дополнительный функционал, то возникает вопрос: почему их популярность невелика? Информация об этом приведена в источнике [2]. И отмечено, что важную роль в желании использования приложения играет психологическое принятие человеком данного решения. Многие пользователи не доверяют менеджерам паролей в силу отсутствия контроля над приложением с их стороны, наличия программных уязвимостей [4] и т.д.

Для примера: группа заинтересованных в IT-безопасности студентов из Дармштадтского института безопасности информационных технологий, входящего в Общество Фраунгофера, провела анализ безопасности самых популярных (на основе количества загрузок) приложений для управления паролями под ОС Android [11]. Исследователями были изучены и проанализированы работы приложений **My Passwords**, **Informaticore Password Manager**, **LastPass**, **Keeper**, **F-Secure KEY**, **Dashlane Password Manager**, **Keepsafe**, **Avast Passwords** и **1Password**. И были выявлены критические ошибки в работе приложений: ряд приложений сохраняли введенные пароли от приложения в открытом виде, ряд других были подвержены воздействию вредоносного ПО и утечке паролей.

Портал **"Xakep.ru"** публиковал ряд статей о найденных в менеджерах паролей уязвимостей. Среди приложений с уязвимостями оказались **LastPass** [20], **Kaspersky Password Manager**, **Sticky Password**, **1Password**, **KeePass**, **RoboForm** [16].

Набирающие в последнее время популярность аппаратные менеджеры паролей также не обеспечивают должную защиту данных [6]. По данным авторов статьи, получить информацию с устройств можно, подключившись напрямую к их аппаратной составляющей на материнской плате.

Стоит отметить, что большинство обнаруженных в упомянутых исследованиях уязвимостей устраняются или частично устранены разработчиками продуктов. Однако это не уменьшает значимости исследований уязвимостей менеджеров паролей.

2.1. Анализ уязвимостей программных менеджеров паролей

Анализ уязвимостей программных менеджеров паролей сводится к анализу и сведению в единый реестр уязвимостей, выявленных специалистами (описанными выше). В результате можно выделить следующие категории уязвимостей:

– связанные с хранением ключей;

– с шифрованием данных;

– с защитой канала передачи информации;

– с использованием встроенного веб-браузера.

Для примера рассмотрим несколько найденных уязвимостей из каждой категории.

2.1.1. Уязвимости, связанные с хранением ключей

– похищение и последующая расшифровка пароля от менеджера паролей. Уязвимость была обнаружена в **My Passwords**. Она позволяла злоумышленнику с физическим контролем над устройством извлечь весь пароль, хранящийся в приложении.

– ключ шифрования данных внедряется в коде приложения. Уязвимость была выявлена в приложении **LastPass 4.0**. Ключ от приложения и PIN-код симметрично шифровались и хранились в общем файле настроек в локальной папке приложения.

– пароль от менеджера паролей хранится в открытом виде. Приложение **F-Secure KEY Password Manager 4.2.8** хранит мастер-пароль в виде простого текста внутри файла /data/data/com.fsecure.key/shared_prefs/ /KeyStorage.xml.

2.1.2. Уязвимости, связанные с шифрованием данных

– заголовки и URL-адреса в базе данных не зашифрованы. В базе данных менеджера паролей **1Password 6.3.3** заголовки и URL-адреса записей веб-сайтов не зашифрованы.

2.1.3. Уязвимости, связанные с защитой канала передачи информации

– реализация небезопасного HTTP-соединения. Менеджер паролей **Avast** взаимодействует с серверной частью через небезопасные HTTP-соединения. Для защиты связи предоставляется собственный криптографический протокол, имеющий серьезные недо-

статки, позволяющие злоумышленнику расшифровать передаваемые данные.

2.1.4. Уязвимости, связанные с использованием встроенного веб-браузера

– чтение личных данных из папки приложения. Встроенный веб-браузер в **1Password Manager 6.3.3** и **LastPass 4.0** позволяет извлекать файлы из каталога личных данных приложения. Что позволяет получить доступ к файлу базы данных и файлу общих настроек приложения.

– использование протокола HTTP вместо HTTPS по умолчанию. Во встроенном веб-браузере **1Password Manager 6.3.3** схема по умолчанию установлена на HTTP.

– утечка пароля поддоменов. Менеджер паролей **1Password Manager 6.3.3** и **Dashlane Password Manager 4.3** при автоматическом заполнении учетных данных использует неверный шаблон для поиска в базе данных нужного URL-адреса.

2.2. Анализ уязвимостей программно-аппаратных менеджеров паролей

Уязвимости, рассмотренные на примере программных менеджеров паролей, также могут встретиться и в аппаратной реализации: пароль от менеджера паролей может храниться в открытом виде, шифрование может использоваться только для части базы данных и т.д. Поэтому в данном разделе стоит выделить только те уязвимости, которые характерны именно для электронных устройств:

– ключи шифрования по умолчанию. В некоторых устройствах используются одинаковые ключи шифрования, которые жестко прописываются в памяти устройства при его производстве.

– уязвимости протоколов беспроводной связи. При передаче информации по беспроводным каналам возникает потенциальная возможность перехвата данных злоумышленником.

– отсутствие физической защиты. Данная уязвимость имеет место быть при использовании электронных устройств, однако возможность ее реализации зависит не от производителя устройства, а от его пользователя.

Таким образом, выше были рассмотрены уязвимости программных и аппаратных менеджеров паролей. В каждой группе уязвимостей были указаны угрозы, для реализации которых могут быть использованы эти уязвимости и последствия их реализации.

Выводы

В результате проведенного анализа уязвимостей существующих менеджеров паролей, проведенного выше, можно сформировать следующие рекомендации, которых необходимо придерживаться при разработке менеджеров паролей:

– необходимо использовать существующие криптографические протоколы, а не создавать и внедрять свои собственные протоколы;

– проверять, действительно ли пароли при разработке должны будут храниться с использованием обратимого шифрования. Обычно достаточно хранить только хэш;

– не использовать жестко запрограммированные ключи симметричного шифрования;

– рекомендуется хранить ключ шифрования базы данных в зашифрованном виде, например, с помощью ключа, полученного применением определенной функции к паролю менеджера паролей;

– менеджер паролей должен шифровать не только учетные данные (имя пользователя и пароль), но и все метаданные;

– не рекомендуется сохранять на устройстве пароль от менеджера паролей или любые его производные в виде открытого текста;

– не рекомендуется хранить ключи шифрования вместе с зашифрованными данными;

– для обмена данными с внешними ресурсами использовать защищенное соединение, например протокол https;

– предусмотреть ограничение количества попыток ввода пароля от менеджера паролей;

– разработать сценарий оповещения пользователя или уничтожения информации в базе данных при обнаружении попытки взлома;

– при автоматическом заполнении веб-форм и предоставлении учетных данных пользователю необходимо сравнивать весь домен веб-ресурса, прежде чем вводить данные в веб-формы. Сравнивать домены только верхнего уровня недостаточно.

Составленные рекомендации по разработке менеджера паролей призваны обратить внимание разработчиков на места в приложении, которые могут содержать потенциальные уязвимости.

Соблюдение данных правил не предполагает создание абсолютно надежного и безопасного менеджера паролей, но направлено на устранение в разрабатываемом приложении наиболее распространенных уязвимостей.

Список литературы

1. *Password:* сайт. Торонто, Канада, 2020. URL: https://1password.com (дата обращения: 10.10.2021).
2. *Alkaldi N.* Why do people adopt, or reject, smartphone password managers? / N. Alkaldi, K. Renaud // IEuroUSEC 2016: The 1st European Workshop on Usable Security, Darmstadt, Germany. 2016.
3. *Ayyagari R.* Why Do Not We Use Password Managers? A Study on the Intention to Use Password Managers / R. Ayyagari // Contemporary Management Research. 2019. P. 227–245.
4. *Bahmanziari T.P.* Is Trust Important in Technology Adoption? A Policy Capturing Approach / T.P. Bahmanziari // Journal of Computer Information Systems. 2003. № 43(4). P. 46–54.
5. *DashLane:* сайт. – Dashlane Inc, 2020. URL: https://www.dashlane.com (дата обращения: 10.10.2021).
6. *Eveleigh P.* Hacking Hardware Password Managers: The RecZone / P. Eveleigh. Текст: электронный // PenTestPartners. Security consulting and testing services [сайт]. 2012. Dec, 6. URL: https://www.pentestpartners.com/security-blog/hacking-hardware-password-managers-the-reczone (дата обращения: 10.10.2021).
7. *Huth A.O.* Password security, protection, and management / A.O. Huth. Текст: электронный // US-CERT: [сайт]. 2012. URL: http://aahuth.com/wp-content/uploads/sites/44/2014/02/PasswordMgmt2012-2.pdf (дата обращения: 10.10.2021).
8. KeePass Password Safe: сайт. 2003–2020. URL: https://keepass.info (дата обращения: 10.10.2021).
9. *LastPass:* сайт. LogMeIn Inc., 2020. URL: https://www.lastpass.com (дата обращения: 10.10.2021).
10. *Moore N.J.* The Best Password Managers for 2020 / N.J. Moore. Текст: электронный // PCMag: [сайт]. 2020. Oct, 1. URL: https://www.pcmag.com/picks/the-best-password-managers (дата обращения: 10.10.2021).
11. *Password* manager apps. Текст: электронный // Fraunhofer Institute for Secure Information Technology: [сайт]. 2017. URL: https://team-sik.org/trent_portfolio/password-manager-apps (дата обращения: 10.10.2021).
12. *Security* and data protection solutions | Hideez: сайт. Hideez Group Inc., 2020. URL: https://hideez.com (дата обращения: 10.10.2021).
13. *TeamSIK*: сайт. TeamSIK, 2019. URL: https://team-sik.org (дата обращения: 10.10.2021).
14. *The Mooltipass* Hardware Password Keeper: сайт. Stephan Electronics, 2018. URL: https://www.themooltipass.com (дата обращения: 10.10.2021).
15. Trezor Hardware Wallet (Official): сайт. SatoshiLabs, 2020. URL: https://trezor.io (дата обращения: 10.10.2021).
16. *Ващило А.* Ищем слабые места современных менеджеров паролей // Хакер: [сайт]. 2014. 8 сент. URL: https://xakep.ru/2014/09/08/password-manager-pentest (дата обращения: 10.10.2021).
17. *Восстановление* аккаунтов членов семьи или команды // 1Password: [сайт]. 2017. URL: https://support.1password.com/ru/recovery (дата обращения: 10.10.2021).
18. *Димова К.В.* Решение проблемы хранения учетных данных пользователя / К.В. Димова, Р.А. Ешенко. // Научно-техническое и экономическое сотрудничество стран АТР в XXI веке. Т. 1. 2009. С. 139–143.
19. *Ларионов И.* Пастильда – открытый аппаратный менеджер паролей // Хабр: [сайт]. 2016. 14 июл. URL: https://habr.com/ru/post/305594 (дата обращения: 10.10.2021).
20. *Нефёдова М.* В менеджере паролей LastPass обнаружили кучу новых уязвимостей // Хакер: [сайт]. 2015. 19 нояб. URL: https://xakep.ru/2015/11/19/lastpass-bugs (дата обращения: 10.10.2021).

References

1. *Password:* sajt. Toronto, Kanada, 2020. URL: https://1password.com (data obrashcheniya: 10.10.2021).
2. *Alkaldi N.* Why do people adopt, or reject, smartphone password managers? / N. Alkaldi, K. Renaud // IEuroUSEC 2016: The 1st European Workshop on Usable Security, Darmstadt, Germany. 2016.
3. *Ayyagari R.* Why Do Not We Use Password Managers? A Study on the Intention to Use Password Managers / R. Ayyagari // Contemporary Management Research. 2019. P. 227–245.

4. *Bahmanziari T.P.* Is Trust Important in Technology Adoption? A Policy Capturing Approach / T.P. Bahmanziari // Journal of Computer Information Systems. 2003. № 43(4). P. 46–54.
5. *DashLane:* sajt. Dashlane Inc, 2020. URL: https://www.dashlane.com (data obrashcheniya: 10.10.2021).
6. *Eveleigh P.* Hacking Hardware Password Managers: The RecZone / P. Eveleigh. Tekst: elektronnyj // PenTestPartners. Security consulting and testing services [sajt]. 2012. Dec, 6. URL: https://www.pentestpartners.com /security-blog/hacking-hardware-password-managers-the-reczone (data obrashcheniya: 10.10.2021).
7. *Huth* A.O. Password security, protection, and management / A.O. Huth. Tekst: elektronnyj // US-CERT: [sajt]. 2012. URL: http://aahuth.com/wp-content/uploads/ sites/44/2014/02/PasswordMgmt2012-2.pdf (data obrashcheniya: 10.10.2021).
8. *KeePass* Password Safe: sajt. 2003-2020. URL: https://keepass.info (data obrashcheniya: 10.10.2021).
9. *LastPass:* sajt. LogMeIn Inc., 2020. URL: https://www.lastpass.com (data obrashcheniya: 10.10.2021).
10. *Moore N.J.* The Best Password Managers for 2020 / N.J. Moore. Tekst: elektronnyj // PCMag: [sajt]. 2020. Oct, 1. URL: https:// www.pcmag.com/picks/the-best-password-managers (data obrashcheniya: 10.10.2021).
11. *Password* manager apps. Tekst: elektronnyj // Fraunhofer Institute for Secure Information Technology: [sajt]. 2017. URL: https://team-sik.org/trent_portfolio/password-manager-apps (data obrashcheniya: 10.10.2021).
12. *Security* and data protection solutions Hideez: sajt. Hideez Group Inc., 2020. URL: https://hideez.com (data obrashcheniya: 10.10.2021).
13. *TeamSIK:* sajt. TeamSIK, 2019. URL: https://team-sik.org (data obrashcheniya: 10.10.2021).
14. 14. https://www.themooltipass.com (data obrashcheniya: 10.10.2021).
15. *Trezor* Hardware Wallet (Official): sajt. SatoshiLabs, 2020. URL: https://trezor.io (data obrashcheniya: 10.10.2021).
16. *Vashchilo A.* Ishchem slabye mesta sovremennyh menedzherov parolej // Haker: [sajt]. 2014. 8 sent. URL: https://xakep. ru/2014/09/08/-password-manager-pentest (data obrashcheniya: 10.10.2021).
17. *Vosstanovlenie* akkauntov chlenov sem'i ili komandy // 1Password: [sajt]. 2017. URL: https://support.1password. com/ru/recovery (data obrashcheniya: 10.10.2021).
18. *Dimova K.V.* Reshenie problemy hraneniya uchetnyh dannyh pol'zovatelya / K.V. Dimova, R.A. Eshenko. // Nauchno-tekhni-cheskoe i ekonomicheskoe sotrudnichestvo stran ATR v XXI veke. T. 1. 2009. S. 139–143.
19. *Larionov I.* Pastil'da – otkrytyj apparatnyj menedzher parolej // Habr: [sajt]. 2016. 14 iyul. URL: https://habr.com/ru/post/305594 (data obrashcheniya: 10.10.2021).
20. *Nefyodova M.* V menedzhere parolej LastPass obnaruzhili kuchu novyh uyazvimostej // Haker: [sajt]. 2015. 19 noyab. URL: https://xakep.ru/2015/11/19/lastpass-bugs (data obrashcheniya: 10.10.2021).

Просьба ссылаться на эту статью:
Черников А.В. Рекомендации по разработке менеджеров паролей для ОС Андроид // Вестник ПГУ. Математика. Механика. Информатика. 2021. № 4 (55). С. 49–57. DOI: 10.17072/1993-0550-2021-4-49-57.

Please cite this article as:
Chernikov A.V. Recommendations for developing password managers of Android OS // Bulletin of Perm University. Mathematics. Mechanics. Computer Science. 2021. № 4 (55). P. 49–57. DOI: 10.17072/1993-0550-2021-4-49-57.