УДК 004.056.5
DOI: 10.26102/2310-6018/2025.48.1.031

Реализация теоретико-множественного подхода для получения численной оценки конфиденциальности данных при использовании модулей блокировки доступа к мобильным приложениям

А.Д. Шульженко✉, Д.М. Курпаченко, М.Ф. Савельев

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Санкт-Петербург, Российская Федерация

Резюме. В работе рассматривается проблема оценки конфиденциальности данных при использовании модулей блокировки доступа к мобильным приложениям. Для примера были выбраны мессенджеры на платформе iOS17. Актуальность исследования обусловлена необходимостью повышения уровня защиты пользовательских данных в условиях растущих угроз информационной безопасности. Основной целью является получение численной оценки. Достижение цели показано на примере сравнительного анализа конфиденциальности данных, обеспечиваемой средствами блокировки приложений VK, Telegram и WhatsApp. Для достижения цели использовались методы теоретико-множественного анализа и экспертных оценок. Были выделены ключевые параметры обеспечения конфиденциальности (тип и длина кода блокировки, использование биометрии, время автоблокировки и др.), нормализованные в диапазоне [0,10]. Итоговая оценка рассчитывалась как сумма значений частных показателей для каждого приложения. Результаты показали, что Telegram обеспечивает наиболее высокий уровень конфиденциальности благодаря возможности использования более сложных кодов блокировки и строгим настройкам защиты. VK уступает Telegram по ряду параметров, но демонстрирует лучшие результаты по сравнению с WhatsApp, если только все параметры не выключены принудительно. Выводы исследования могут быть применены для совершенствования механизмов защиты данных в мобильных приложениях, а предложенный подход – для дальнейших исследований в области информационной безопасности.

Ключевые слова: конфиденциальность данных, блокировка доступа, пин-лок, оценка конфиденциальности, безопасность мессенджеров, персональные данные, теоретико-множественный анализ, автоблокировка приложений, скрытие содержимого уведомлений, защита пользовательских данных.

Для цитирования: Шульженко А.Д., Курпаченко Д.М., Савельев М.Ф. Реализация теоретико-множественного подхода для получения численной оценки конфиденциальности данных при использовании модулей блокировки доступа к мобильным приложениям. *Моделирование, оптимизация и информационные технологии.* 2025;13(1). URL: https://moitvivt.ru/ru/journal/pdf?id=1831 DOI: 10.26102/2310-6018/2025.48.1.031

Implementation of a set-theoretic approach to obtain a numerical estimate of data privacy when using modules for blocking access to mobile applications

A.D. Shulzhenko✉, D.M. Kurpachenko, M.F. Saveliev

Saint Petersburg Electrotechnical University "LETI" named after V.I. Ulyanov (Lenin), Saint Petersburg, the Russian Federation

Abstract. This paper considers the problem of assessing the confidentiality of data when using modules for blocking access to mobile applications. Messengers on the iOS17 platform were selected as an

example. The relevance of the study is due to the need to increase the level of protection of user data in the face of growing threats to information security. The main goal is to obtain a numerical estimate, and the achievement of the goal is shown using the example of a comparative analysis of the confidentiality of data provided by the means of blocking applications VK, Telegram and WhatsApp. To achieve the goal, the methods of set-theoretical analysis and expert assessments were used. Key parameters for ensuring confidentiality (type and length of the lock code, use of biometrics, auto-lock time, etc.) were identified, normalized in the range [0,10]. The final score was calculated as the sum of the values of particle values for each application. The results showed that Telegram provides the highest level of confidentiality due to the ability to use more complex lock codes and strict security settings. VK is inferior to Telegram in a number of parameters, but demonstrates better results compared to WhatsApp, unless all parameters are forcibly disabled. The findings of the study can be used to improve data protection mechanisms in mobile applications, and the proposed methodology can be used for further research in the field of information security.

Keywords: data privacy, access blocking, PIN lock, privacy assessment, messenger security, personal data, set-theoretic analysis, application auto-locking, notification content hiding, user data protection.

For citation: Shulzhenko A.D., Kurpachenko D.M., Saveliev M.F. Implementation of a set-theoretic approach to obtain a numerical estimate of data privacy when using modules for blocking access to mobile applications. *Modeling, Optimization and Information Technology*. 2025;13(1). (In Russ.). URL: https://moitvivt.ru/ru/journal/pdf?id=1831 DOI: 10.26102/2310-6018/2025.48.1.031

Введение

В последнее десятилетие активно растет число пользователей мессенджеров, и по данным компании «Mediascope» за январь 2025 года лидирующие позиции по числу пользователей в России занимают Telegram (далее – Tg), WhatsApp (далее – WA) и Snapchat. Активно продвигает свои продукты ООО «Вконтакте» (социальная сеть vk.com (далее, имея ввиду мобильное приложение, – VK), vk-мессенджер, Сферум). Одновременно совершенствуются возможности злоумышленников по краже данных, которые в соответствии с Федеральным законом 149-ФЗ «Об информации и информационных технологиях» относятся к личной тайне пользователей и в обществе принято называть конфиденциальными. Для этого используются известные и вновь открываемые уязвимости, которыми пополняются такие общедоступные базы данных, как База данных уязвимостей Федеральной службы по техническому и экспортному контролю (и другие).

Для того, чтобы защититься от кражи конфиденциальных данных пользователей, разработчики перечисленных и прочих программных приложений для общения в сети разрабатывают свои средства защиты. По результатам исследований, проводимых Всероссийским центром изучения общественного мнения, Mediascope и Hi-Tech Mail, большинство россиян используют Tg, будучи уверенными в его наивысшей защищенности среди прочих. Этот вывод пользователей основывается на гайдах разработчика. При этом по результатам анализа российских и международных публикаций не было найдено общедоступной численной методики, которая позволила бы этот факт проверить и наглядно сравнить параметр конфиденциальности данных при использовании мессенджеров.

Например, в исследовании [1] оценка безопасности (включая обеспечение конфиденциальности данных) проведена для трех популярных корпоративных мессенджеров, и она заключается в сравнении параметров безопасности по факту их наличия и значений параметров по умолчанию.

В исследовании [2] вывод о безопасности использования мессенджеров Tg и WA строится на основе результатов анализа места внедрения и способа шифрования данных. Показаны вероятные вектора атак при использовании мессенджеров, однако без учета

систем защиты окружения. Вербально утверждается, что безопасность WA ниже, чем Tg, но вопрос – на сколько? Достаточный ли уровень риска, чтобы не доверять этой платформе? – остался открытым. Для того, чтобы ответить на этот и подобные вопросы, необходимо осуществить переход от качественных характеристик к количественным, а также учесть влияние параметров окружения на состояние защищенности.

В рамках текущего исследования акцент был сделан на конфиденциальности данных пользователей. Разработка подхода для получения численной оценки конфиденциальности проводилась одновременно с разработкой ООО «Вконтакте» собственного модуля блокировки приложения (далее – пин-лок) VK для iOS17, поэтому при ее апробации была использована именно эта версия. Сравнение производилось с наиболее популярными мессенджерами – Tg и WA – также реализованными для iOS17. Это позволило проводить адекватное сравнение по параметрам защищенности.

При реализации использован теоретико-множественных подход для перевода качественных характеристик в количественные, введены частные показатели конфиденциальности, шкалы их измерения и учитывается полная группа событий безопасности, то есть действия, которые производятся при попытках нарушения конфиденциальности.

Для проведения адекватного сравнения при реализации подхода учтена возможность варьирования системных настроек безопасности, которые влияют на состояние конфиденциальности данных рассматриваемых приложений.

Важно отметить, что человеческий фактор (вероятность ошибочной настройки) также учтен в подходе.

Статья имеет следующую структуру. Во введении описана общая идея изложенного материала. В разделе «Материалы и методы» описаны объекты оценки, приведен анализ существующих методик оценивания защищенности данных, приведено описание собственного подхода к получению численной оценки. В разделе «Результаты и обсуждение» приведен результат расчетов значений конфиденциальности по выбранным мессенджерам и приведены заключения об адекватности подхода. В разделе «Выводы» приведены ключевые аспекты, определяющие научную ценность статьи, и направления совершенствования мессенджеров.

Материалы и методы

1. Объекты оценки

Объектами для получения численной оценки конфиденциальности данных при использовании пин-локов, выбраны приложения Tg, WA и VK, реализованные для операционной системы iOS17.

В Таблице 1 представлено описание реализованных в этих приложениях параметров безопасности и их возможных значений. На основании этих исходных данных формируется итоговая оценка.

Из представленных данных видно, что код блокировки приложения VK имеет более ограниченный набор вариантов, чем Tg, и в случае атаки перебором будет очевидно взломан гораздо быстрее. Относительно других функциональных особенностей важно обратить внимание на их строгое наличие в Tg, в то время как они либо отсутствуют, либо могут быть отключены в приложении VK, что понижает уровень конфиденциальности данных при его использовании; при этом WA уступает по таким же параметрам VK. Однако Tg не имеет возможности немедленной блокировки приложения после его закрытия и по этому параметру уступает конкурентам. Рассматривая указанные преимущества и недостатки, можно сделать вывод, что Tg предлагает более широкий набор инструментов, чем VK, который, в свою очередь,

выигрывает у WA. Однако с точки зрения удобства использования настроек безопасности преимущество отмечается у приложения VK, что делает продукт привлекательнее для пользователей, чем Tg и WA.

Таблица 1 – Сравнение настроек приложений
Table 1 – Comparison of application settings

Настройка	VK	Telegram	WhatsApp
Тип кода	4 цифры	6 цифр, 4 цифры, буквы+цифры	–
Биометрия	Вкл/Выкл	Вкл/Выкл	Вкл
Автоблокировка	Немедленно, 1 минута, 5 минут, 30 минут	1 минута, 5 минут, 1 час, 5 часов, выключена	Немедленно, 1 минута, 5 минут, 15 минут, 1 час
Скрытие содержимого в режиме многозадачности	Вкл/Выкл	Включено	Включено
Скрытие содержимого уведомление	–	Включено, если приложение заблокировано, выключено иначе	–
Действия в случае невозможности войти	Выход из всех аккаунтов	Удаление приложения и конфиденциальных данных	Удаление приложения

2. Анализ существующих методик оценивания защищенности данных

Перед разработкой собственного подхода к получению численной оценки были проанализированы известные (опубликованные) методики оценки конфиденциальности.

В исследовании [3] оценка конфиденциальности предлагаемого метода аутентификации проводилась в виде эксперимента, где в том числе сравнивалось экспериментальное число успешных взломов рассматриваемых моделей.

В исследовании [4] приводилась оценка уязвимостей различных способов аутентификации, оценка основывалась на экспертном методе.

В исследовании [5] также использовался экспертный метод при оценке конфиденциальности виртуальных ассистентов с точки зрения возможных векторов атак.

В докладе [6] исследователи при сравнении нескольких видов аутентификации использовали результаты эксперимента.

В патентах [7] и [8] рассматривались устройства ввода пароля, их преимущество в обеспечении конфиденциальности оценивалось исключительно с точки зрения конкретных решенных проблем – угроз конфиденциальности.

В исследовании методов аутентификации для слепых [9] использовался опрос для оценки существующих решений, а предлагаемый метод оценивался на основании экспериментальных данных.

В исследовании [10] на основании длительного эксперимента анализировались паттерны использования блокировки на устройствах Android, в том числе на основании экспертного мнения предлагались улучшения, сохраняющие уровень конфиденциальности метода блокировки.

Ни одно из этих решений не предложило математического аппарата, который позволил бы получить сколько-нибудь универсальную численную оценку.

3. Предлагаемый подход к получению численной оценки конфиденциальности данных

Для получения численной оценки конфиденциальности данных при использовании пин-локов мобильных приложений (на примере рассмотренных мессенджеров) в первую очередь рассматриваемые параметры безопасности переведены из формата качественной в формат количественной оценки. Для этого использован теоретико-множественных подход.

В соответствии с этим подходом определен показатель, характеризующий состояние конфиденциальности данных в мобильном приложении для системы iOS, и обозначен далее как V^{iOS}. Этот показатель сложный, а его численное выражение логично зависит от каждой из настроек безопасности, которые перечислены в Таблице 1. Считаем, что эти показатели являются равновесными для обеспечения конфиденциальности данных, поэтому их значения нормированы в диапазоне [0,10]. Основываясь на этих тезисах, частные показатели, характеризующие конфиденциальность, формализованы следующим образом:

1) Показатель, связанный с типом и длиной кода блокировки, обозначен как T соответственно, при этом $T = \{T_1, T_2, T_3\}$, где T_1 – значение при использовании кода блокировки из L = 4 цифр; T_2 – значение при использовании кода блокировки из L = 6 цифр; T_3 – значение при использовании кода длиной L = 6..32 символов из латинского алфавита и цифр. Можно показать, что диапазон значений этого показателя варьируется в промежутке $[T_3^{min}, T_3^{max}]$, где T_3^{min} – значение при использовании кода из 6 символов (то есть L принимает минимальное значение среди возможных для данного типа блокировки), а T_3^{max} – из 32 символов (то есть L принимает максимальное значение среди возможных для данного типа блокировки). При этом информативными являются значения $T_3 = \{T_3^{min}, T_3^{max}\}$, то есть краевые значения для получения верхней и нижней границ диапазона.

Расчет возможных значений этого частного показателя производится с использованием формулы подсчета количества возможных размещений с повторениями:

$$T = \bar{A}_m^n = m^n, \quad (1)$$

где n – число символов в коде, m – размер алфавита символов.

Учитывая тот факт, что при увеличении длины пароля и мощности алфавита количество возможных комбинаций возрастает нелинейно, необходимо использовать логарифмическую шкалу для нормировки полученных значений. При этом в соответствии с теорией подобия, применяемой для оценки безопасности подобных информационных систем, правомерно введение пропорций для приведения логарифмических значений к единому для всех небинарных частных показателей диапазону [0,10].

2) Время автоблокировки обозначено как A, при этом $A \in \{0..300\}$ минут. При определении значения этого частного показателя необходимо руководствоваться двумя тезисами:

во-первых, чем меньше время автоблокировки, тем выше конфиденциальность;

во-вторых, с увеличением времени до автоблокировки приложения вероятность нарушения конфиденциальность возрастает нелинейно, и достигает предела при полном отключении этого параметра. Это равносильно утверждению, которое гласит, что с увеличением времени автоблокировки приложения вероятность сохранения конфиденциальности данных нелинейно уменьшается и достигает минимума при полном отключении этого параметра.

Приведенные тезисы позволяют сделать вывод о правомерности применения инвертированной логарифмической шкалы для оценки значения частного показателя. Шкала, как принято в работе, нормируется в диапазоне [0,10].

3) Возможность использования биометрии обозначена среди частных показателей как B. При этом B – бинарный показатель, множество возможных значений которого, учитывая независимость частных показателей и предположение об их равнозначности, $B = \{10; 0\}$. Это связано с тем, что применение биометрической идентификации либо выключено, либо включено. Важно отметить, что этот параметр несколько упрощен в определении, так как невозможно учесть точность, с которой встроенные датчики распознают биометрический образ – эти сведения относятся к коммерческой тайне разработчиков таких устройств.

4) Скрытие содержимого в режиме многозадачности обозначено как S_{mul}.

5) Скрытие содержимого уведомлений обозначено как S_{not}.

Для последних двух показателей набор возможных значений определяется аналогично показателю B.

Комплексный показатель имеет вид:

$$V^{iOS} = \{T, A, B, S_{mul}, S_{not}\}. \quad (2)$$

Общим для всех частных показателей является необходимость учёта влияния человеческого фактора. Принято, что вероятность некорректного выбора параметра настройки безопасности в приложении, связанная с особенностями перцепции человека, составляет 10%. Таким образом, для общей оценки конфиденциальности введено ужесточение в виде коэффициента 0,9.

Эти частные показатели взаимно независимы, и свертка их значений дает численную оценку конфиденциальности данных при отсутствии попыток несанкционированного доступа. Для того, чтобы учесть в оценке возможность проведения таких попыток, введен соответствующий характеризующий показатель $\bar{V}^{iOS}$.

$$\bar{V}^{iOS} = \{\bar{V}^{ios}_{out}, \bar{V}^{ios}_{deldel}, \bar{V}^{ios}_{del}\}, \quad (3)$$

где $\bar{V}^{ios}_{deldel}$ – удаление и данных, и приложения. Это действие максимально сохраняет конфиденциальность данных в ущерб доступности (что выходит за рамки исследования) и имеет оценку 10. $\bar{V}^{ios}_{out}$ – выход из аккаунта (удаление сессии). Это действие защищает от компрометации текущей сессии. Но при этом вероятность компрометации других сессий сохраняется. Также сохраняются все данные. Оценка этого действия – 7. $\bar{V}^{ios}_{del}$ – удаление приложения. Это действие оценено на 3 балла, так как удаление приложения не равносильно удалению конфиденциальных данных и очистке данных сессии, является наименее слабой защитой. Нивелируется восстановлением приложения или сессии через другую точку входа.

Оценки получены на основе опроса 20 специалистов по защите информации.

Таким образом, итоговая численная оценка (3) строится на исследовании полной группы событий, связанных с конфиденциальностью: эта группа событий представляет собой объединение событий обеспечения конфиденциальности и попыток ее нарушения:

$$V = 0{,}9\, V^{iOS} \cup \bar{V}^{iOS}, \quad (4)$$

где V обозначает оценку конфиденциальности данных в целом.

Свертка значений, учитывая равнозначность и взаимную независимость параметров, а также независимость от порядка их включения, производится простым суммированием частных показателей.

Результаты и обсуждение

По приведенным формулам были рассчитаны значения частных показателей конфиденциальности данных пользователей и получена итоговая численная оценка.

По формуле (1) были получены значения первого частного показателя *T*, который зависит от величины алфавита и длины выборки:

$T_1 = 10^4 = 10000$ (размещения с повторениями на выборке 4 цифр из 10 возможных),

$T_2 = 10^6 = 1000000$ (размещения с повторениями на выборке 6 цифр из 10 возможных).

Для определения T_3 были рассчитаны значения T_3^{min} и T_3^{max}:

$T_3^{min} = (52 + 10)^6 = 56800235584$ (размещения с повторениями на выборке 6 символов из 62 возможных, при этом из них 52 – число символов латинского алфавита если считать различными заглавные и строчные буквы, 10 – число цифр),

$T_3^{max} = (52 + 10)^{32} = 22726579 \times 10^{50}$ (размещения с повторениями на выборке 32 символов из 62 возможных, при этом из них 52 – число символов латинского алфавита, 10 – число цифр).

В результате приведения к логарифмической шкале и нормировки в диапазоне от 0 до 10 были получены следующие значения первого частного показателя:

$$T_3^{max} = \frac{\log_{10} T_3^{max}}{6} \approx 9{,}56;$$

$$T_3^{min} = \frac{\log_{10} T_3^{min}}{6} \approx 1{,}79;$$

$$T_2 = \frac{\log_{10} T_2}{6} = 1;$$

$$T_1 = \frac{\log_{10} T_1}{6} \approx 0{,}67.$$

Расчет возможных значений второго частного показателя показал следующее (для удобства проведения расчетов часы и минуты переведены в секунды и принято, что автоблокировка в период от 0 до 1 секунды считается моментальной).

$A^{18000} = 10 - 2\log_{10}(18000) = 1{,}49$ для блокировки через 300 минут;

$A^{3600} = 10 - 2\log_{10}(3600) = 2{,}888$ для блокировки через 60 минут;

$A^{1800} = 10 - 2\log_{10}(1800) = 3{,}49$ для блокировки через 30 минут;

$A^{900} = 10 - 2\log_{10}(900) = 4{,}092$ для блокировки через 15 минут;

$A^{300} = 10 - 2\log_{10}(300) = 5{,}046$ для блокировки через 5 минут;

$A^{60} = 10 - 2\log_{10}(60) = 6{,}444$ для блокировки через 1 минуту;

$A^{01} = 10 - 2\log_{10}(1) = 10$ для блокировки через [0,1] секунду.

Полученные значения логично иллюстрируют приведенные в описании тезисы, обосновывающие выбор диапазонов для частных показателей.

По третьему, четвертому и пятому частному показателю возможные значения бинарные и пересчету не подлежали. Для S_{not} определено, что отсутствие этого параметра в системе соответствует значению 0, иначе – значению 10.

По полученным возможным значениям частных показателей была произведена свертка в трех случаях настройки безопасности: наихудшем (выбраны наихудшие настройки из возможных), среднем (выбраны наилучшие настройки, не задействованы системные усиления iOS) и наилучшем (выбраны наилучшие настройки и включены системные усиления).

Результаты расчетов приведены в Таблице 2.

Таблица 2 – Значение показателя конфиденциальности данных
Table 2 – The meaning of the data privacy index

Варианты настроек	Tg	VK	WA
худший	28,603	10,762	23,592
средний	51,404	34,603	30
наилучший	54,604	51,604	47,604

Важно отметить, что максимальное значение, которое теоретически может быть достигнуто при использовании формулы (4), составляет 55.

Из Таблицы 2 видно, что применение теоретико-множественного подхода позволяет получить численные оценки показателя конфиденциальности. На данном примере наглядно показано, что при намеренном отключении всех настроек безопасности VK показывает наихудшее обеспечение конфиденциальности данных пользователя. Это происходит из-за отсутствия принудительно включенных функций биометрической идентификации и сокрытия содержимого в режиме многозадачности.

При задействовании максимальных настроек приложений без использования системных настроек значительный уровень конфиденциальности данных обеспечивает Tg, VK имеет среднее значение между ним и WA.

Аналогичный результат показывает использование максимальных настроек с задействованием настроек безопасности системы iOS.

Заключение

Представленный подход к получению численной оценки конфиденциальности данных пользователей при использовании мобильных приложений представляет научную ценность за счет формализации качественных характеристик (соответствующих настройкам безопасности) в количественные показатели. Предложенный подход включает нормализацию и шкалирование параметров безопасности в диапазоне [0,10], что обеспечивает универсальность оценки для различных мобильных приложений. Также новизну составляет учет полной группы событий, связанных с конфиденциальностью данных, включая как параметры защиты, так и возможные действия злоумышленников по получению несанкционированного доступа. Также при формировании подхода учитывается вероятность ошибок пользователей при настройке параметров безопасности, что повышает ее практическую применимость. Результаты исследования демонстрируют возможность сравнения уровня конфиденциальности данных в различных мессенджерах, что продемонстрировано на примере Telegram, WhatsApp и VK на платформе iOS17.

По результатам анализа полученных численных оценок можно сформулировать рекомендации по улучшению свойств безопасности приложений с использованием пин-локов. Для повышения уровня конфиденциальности данных рекомендуется использование кодов блокировки, состоящих из комбинаций букв и цифр, длиной не менее 8 символов, с сочетанием строчных и заглавных букв и цифр. Это позволит увеличить устойчивость к атакам методом перебора и обеспечить более высокий уровень конфиденциальности по приведенной шкале. Также можно рассмотреть возможность внедрения обязательной биометрической аутентификации для доступа к приложению, что повысит уровень конфиденциальности данных.

Рекомендуется реализовать возможность мгновенной блокировки приложения после его закрытия. Как показано в статье, это способствует логарифмическому снижению риска несанкционированного доступа. Дополнительным направлением можно выделить обязательное внедрение функций сокрытия содержимого уведомлений

и в режиме многозадачности, что предотвратит утечку информации при временном доступе к устройству.

Важно отметить (для разработчиков), что возможно не нагружать приложения дублирующим функционалом, а облегчить интеграцию настроек модулей безопасности приложений с системными настройками безопасности.

СПИСОК ИСТОЧНИКОВ / REFERENCES

1. Коренева А.М., Саварин И. Сравнительный обзор безопасности популярных корпоративных мессенджеров. *Инженерный вестник Дона.* 2024;(8):19–40. Koreneva A.M., Savarin I. A comparative review of the security of popular corporate messengers. *Engineering Journal of Don*. 2024;(8):19–40. (In Russ.).
2. Клюева А.А., Пальчастая А.Р. Сравнительный анализ шифрования в мессенджерах. В сборнике: *75-я научно-техническая конференция учащихся, студентов и магистрантов: Тезисы докладов: Часть 4, 22–27 апреля 2024 года, Минск, Беларусь.* Минск: БГТУ; 2024. С. 159.
3. Kausar N., Din I.U., Khan M.A., Almogren A., Kim B.-S. GRA-PIN: A Graphical and PIN-Based Hybrid Authentication Approach for Smart Devices. *Sensors.* 2022;22(4). https://doi.org/10.3390/s22041349
4. Lal N.A., Prasad S., Farik M. A Review of Authentication Methods. *International Journal of Scientific & Technology Research.* 2016;5(11):246–249.
5. Hayashi V.T., Ruggiero W.V. Hands-Free Authentication for Virtual Assistants with Trusted IoT Device and Machine Learning. *Sensors.* 2022;22(4). https://doi.org/10.3390/s22041325
6. Senbagavalli M., Debnathb S., Ramalakshmi K. Secret key verification techniques for graphical password authentication system to avoid shoulder surfing. *Topics in Intelligent Computing and Industry Design.* 2022;3(3):172–177. http://doi.org/10.26480/icpesd.03.2022.172.177
7. Rodriguez R.A., Spring J., Volovik D. *Visual authentication and authorization for mobile devices.* US Patent, No. US8850541B2. 2014.
8. Methenitis M. *System and method for enhancing device passcode security.* US Patent, No. US8850603B2. 2014.
9. Azenkot S., Rector K., Ladner R.E., Wobbrock J.O. PassChords: Secure Multi-Touch Authentication for Blind People. In: *ASSETS '12: Proceedings of the 14th International ACM SIGACCESS Conference on Computers and Accessibility, 22–24 October 2012, Boulder, USA.* ACM; 2013. pp. 159–166. https://doi.org/10.1145/2384916.2384945
10. Harbach M., De Luca A., Egelman S. The Anatomy of Smartphone Unlocking: A Field Study of Android Lock Screens. In: *CHI '16: Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, 07–12 May 2016, San Jose, USA.* New York: Association for Computing Machinery; 2016. pp. 4806–4817. https://doi.org/10.1145/2858036.2858267

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Шульженко Анастасия Дмитриевна, кандидат технических наук, доцент кафедры информационной безопасности, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Санкт-Петербург, Российская Федерация.
e-mail: anastasija_dmitrievna@mail.ru
ORCID: 0000-0002-5950-7039

Anastasia D. Shulzhenko, Candidate of Engineering Sciences, Associate Professor of Information Security Department, Saint Petersburg Electrotechnical University "LETI" named after V.I. Ulyanov (Lenin), Saint Petersburg, the Russian Federation.

Курпаченко Даниил Максимович, студент кафедры информационной безопасности, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Санкт-Петербург, Российская Федерация.

Daniil M. Kurpachenko, student of Information Security Department, Saint Petersburg Electrotechnical University "LETI" named after V.I. Ulyanov (Lenin), Saint Petersburg, the Russian Federation.

Савельев Максим Феликсович, кандидат технических наук, заведующий кафедрой информационной безопасности, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В.И. Ульянова (Ленина), Санкт-Петербург, Российская Федерация.

Maxim F. Saveliev, Candidate of Engineering Sciences, Head of Information Security Department, Saint Petersburg Electrotechnical University "LETI" named after V.I. Ulyanov (Lenin), Saint Petersburg, the Russian Federation.

Статья поступила в редакцию 25.02.2025; одобрена после рецензирования 05.03.2025; принята к публикации 10.03.2025.

The article was submitted 25.02.2025; approved after reviewing 05.03.2025; accepted for publication 10.03.2025.