Научная статья
УДК 004.056.53; DOI: 10.61260/2218-13X-2024-4-120-129

УДОСТОВЕРЕНИЯ С НУЛЕВЫМ РАЗГЛАШЕНИЕМ КАК СРЕДСТВО УМЕНЬШЕНИЯ УТЕЧЕК ДАННЫХ

✉**Дешевов Павел Павлович.**
МИРЭА – Российский технологический университет, Москва, Россия.
Укустов Сергей Сергеевич.
Волгоградский государственный технический университет, г. Волгоград, Россия
✉***pavelpal.d@gmail.com***

Аннотация. Процессы идентификации, аутентификации и авторизации можно осуществлять по-разному. Особенное внимание приковано к процессам, реализованным в парадигме суверенной идентичности. Работа исследует эти процессы на предмет угрозы утечек данных. Производится сравнение со схемой, использующей централизованный провайдер идентичности. Дан обзор соответствующих схем реализации процессов: в суверенной и несуверенной парадигме. Выявлено, что с точки зрения угроз утечки данных схема суверенной идентичности даёт большую безопасность только при использовании технологий доказательства с нулевым разглашением.

Ключевые слова: аутентификация, авторизация, цифровые удостоверения, доказательства с нулевым разглашением, удостоверения с нулевым разглашением

Для цитирования: Дешевов П.П., Укустов С.С. Удостоверения с нулевым разглашением как средство уменьшения утечек данных // Науч.-аналит. журн. «Вестник С.-Петерб. ун-та ГПС МЧС России». 2024. № 4. С. 120–129. DOI: 10.61260/2218-13X-2024-4-120-129.

Scientific article

ZERO-KNOWLEDGE CREDENTIALS AS A WAY TO MINIMIZE DATA LEAKS

✉**Deshevov Pavel P.**
MIREA – Russian technological university, Moscow, Russia.
Ukustov Sergey S.
Volgograd state technical university, Volgograd, Russia
✉***pavelpal.d@gmail.com***

Abstract. Identification, authentication, and authorization processes can be conducted in various ways. Particular attention is given to the processes implemented within the self-sovereign identity paradigm. This paper analyses the processes from a data leak perspective. A comparison is made between self-sovereign identity and a centralized identity provider scheme. An overview of the relevant implementations for these processes is provided: in both the self-sovereign and non-sovereign paradigms. It has been found that, from the data leaks perspective, the self-sovereign identity scheme could only provide superior security if zero-knowledge proof technology is applied.

Keywords: authentication, authorization, digital credentials, zero-knowledge proofs, zero-knowledge credentials

For citation: Deshevov P.P., Ukustov S.S. Zero-knowledge credentials as a way to minimize data leaks // Scientific and analytical journal «Vestnik Saint-Petersburg university of State fire service of EMERCOM of Russia». 2024. № 4. P. 120–129. DOI: 10.61260/2218-13X-2024-4-120-129.

Введение

Текущие инженерные решения предполагают накопление большого количества неанонимизированных данных для обеспечения контроля доступа и высокого качества пользовательского опыта. Такие данные представляют ценность не только для компаний, которые их собирают. Утёкшую к злоумышленникам информацию в дальнейшем используют с целью шантажа, промышленного шпионажа или атак на индивидуальных пользователей, чьи данные собраны.

За последние 10 лет в среднем количество утечек данных увеличивается на 15 % в год. В 2022 г. было украдено 20,12 млрд записей. Стоимость ущерба от инцидентов на данный момент составляет в среднем 160 млн руб. [1–4] и растёт на 15 % в год. Такое развитие делает проблему безопасности пользовательских данных особенно острой.

Стоит обратить внимание на очевидный тезис: данные ценны постольку, поскольку их можно обратить в действие. Всеобъемлющая база данных службы доставки еды [5] с персональными данными, адресами и списком покупок представляет очевидную ценность. Сегрегированные же по цели применения базы данных со списком покупок и адресами доставки, привязанные к случайным идентификаторам, каждая в отдельности представляют значительно меньшую ценность для злоумышленников. Такой подход разделяет даже законодатель. В Федеральном законе от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (ФЗ № 152-ФЗ) [6] указано: «Обработка персональных данных должна ограничиваться достижением конкретных, заранее определённых и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой».

При том, что сегрегация баз данных внутри компании усложняет работу внешних нарушителей, она не способна защитить от внутренних нарушителей. Согласно приведённым выше отчётам [1–4] в 2/3 случаев сотрудники компаний были соучастниками в краже данных. Известно, что не существует «ни программного, ни методического решения, обеспечивающего надёжную защиту от инсайдерских угроз» [7].

Указанные атаки базируются на двух фундаментальных посылках: данные ценны, данные хранятся в контуре одной организации. Соответственно, уменьшение ценности отдельных наборов данных и их раздельное хранение представляются перспективными направлениями уменьшения и внешних, и внутренних угроз конфиденциальности пользовательских данных. В этом контексте стоит отметить происходящие в индустрии и в исследовательском сообществе изменения.

Во-первых, в свете большего внимания общества к проблеме конфиденциальности и появления законов о безопасности персональных данных, таких как ФЗ № 152-ФЗ в России, GDRP в Европе или CCPA в Калифорнии (США), меняется отношение к данным. Вместе с тезисом «данные – это новая нефть» [8] получает всё большее понимание тезис «данные – это обуза» (англ. Data is a liability) [9]. Под вопрос ставят оппортунистский сбор данных с целью анализа «когда-нибудь». В том числе это привело к тому, что для маркетингового анализа применяют обезличенные наборы данных, полученные, в том числе, с помощью методов дифференциальной приватности. Это сводит цели сбора данных, указанные в начале статьи, к контролю доступа – к аутентификации и в широком смысле авторизации, например, имеет ли право данный пользователь на получение специального предложения на следующую покупку.

Во-вторых, получает развитие более глубокая сегрегация данных. Чувствительные данные хранятся под контролем собственника – пользователя или организации, и раскрываются третьим лицам только по требованию.

В-третьих, в последние несколько лет развили высокий уровень готовности технологии доказательств с нулевым разглашением общего назначения zk-SNARK и zk-STARK (ZK от англ. Zero Knowledge – нулевое знание). Такие технологии позволяют

доказать, что некое утверждение верно, не предоставляя при этом информации о самом утверждении. Например, можно доказать, что возраст человека более 18 лет без раскрытия точной даты рождения или иных данных паспорта [10].

В свете этих изменений, особенно развития технологий ZK, актуальным выглядит анализ процессов идентификации, аутентификации и авторизации пользователей на предмет обеспечения конфиденциальности пользовательской информации.

Перед исследованием стоит описать рассматриваемые процессы. При рассмотрении процессов идентификации, аутентификации и авторизации выделяют понятие цифровой идентичности (ЦИ; она же «цифровая личность», англ. digital identity) [11–13] – это набор атрибутов сущности, которые позволяют ей быть уникально идентифицированной или аутентифицированной другой сущностью в цифровой среде. Системы, которые позволяют осуществлять процесс идентификации или аутентификации, называют системами управления цифровой идентификацией (СУЦИ; англ. digital identity management system; было бы правильнее переводить как «системы управления цифровой идентичностью»). Они состоят из трёх компонентов: пользователь – сущность, которую нужно аутентифицировать с помощью провайдера идентичности; провайдер идентичности (ПИ) (англ. identity provider, IP) – сущность, которая осуществляет процесс цифровой идентификации и аутентификации пользователя; сервис (он же «доверяющая сторона», англ. relying party, RP) – сущность, которой нужно получить подтверждение ЦИ пользователя от ПИ. Процесс взаимодействия между ними происходит следующим образом (рис.): 1) пользователь делает запрос на регистрацию своей ЦИ в ПИ; 2) пользователь получает данные, которые способствуют его идентификации и аутентификации у ПИ; 3) пользователь делает запрос сервису, услугами которого хочет воспользоваться; 4) сервис просит пользователя подтвердить свою ЦИ; 5) пользователь подтверждает свою ЦИ у ПИ; 6) ПИ отправляет подтверждение ЦИ пользователя сервису.

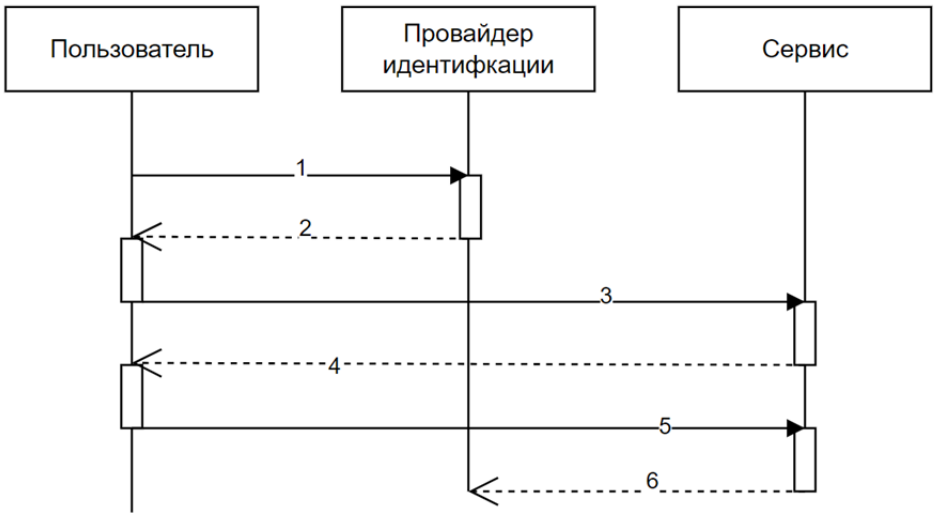

Рис. **Диаграмма взаимодействия в рамках СУЦИ**

Выделяют следующие классы СУЦИ: централизованные (ПИ является частью сервиса); со сторонним ПИ (взаимодействие сервиса и ПИ реализовано по протоколу, например, OIDC [14]), федеративные (сервис может использовать несколько независимых ПИ; взаимодействие осуществляется, например, по протоколу SAML [15]).

Все приведённые выше классы широко распространены. Недостатками этих систем, назовём их несуверенными – причина для такого именования объясняется далее по тексту, – являются:

1) невозможность пользователя самостоятельно управлять своей ЦИ; в конечном счёте ответственность за управление ЦИ лежит на ПИ;

2) централизация точки отказа: ПИ является точкой отказа: он может утратить данные пользователя, данные могут попасть в руки злоумышленников при атаке на ПИ;

3) цензурирование: ПИ может отказать в обслуживании сервису или отдельному пользователю.

Методы исследования

Для решения этих проблем была предложена концепция суверенной идентичности (СИ, англ. self-sovereign identity) [13]. В рамках этой концепции пользователь идентифицируется и аутентифицируется через его/её секретный ключ ассиметричной криптографической системы, а не через ПИ, что нивелирует недостатки несуверенных СУЦИ. Стандарт DID [16] предлагает интероперабельный формат представления приватных ключей и различных методов их использования.

В существующих системах ПИ в дополнение к сигналу аутентификации пользователя передаёт атрибуты пользователя (такие как имя, дата рождения, предпочитаемый язык, страну, количество читателей в социальной сети и т.п.), основываясь на которых сервис может произвести авторизацию и/или улучшить пользовательский опыт. Использование только DID не является абсолютной заменой несуверенных типов СУЦИ, указанных выше: DID не представляет возможности передавать и/или подтверждать атрибуты.

Родственная DID спецификация цифровых удостоверений [17] (англ. Verifiable Credentials или VC) исправляет этот недостаток. Данная спецификация основывается на так называемом «треугольнике доверия»:

– субъект – сущность, обладающая набором характеристик, на основе которой можно воспроизвести ряд утверждений и фактов об этой сущности и представить эти утверждения и факты в виде VC; также может называться «держателем VC», фактически «пользователь»;

– эмитент (англ. issuer) – несёт ответственность за подтверждение фактов о субъекте и создании VC на основе этих фактов, с дальнейшим выпуском созданных VC держателю;

– верификатор (англ. verifier) – проверяет VC, полученные от держателя VC, для построения необходимой логики приложения.

Эмитент выдаёт субъекту цифровое удостоверение, содержащее набор атрибутов – утверждений о субъекте. Субъект предъявляет удостоверение верификатору для проверки. Верификатор проверяет удостоверение и использует полученные атрибуты для авторизации и/или улучшения пользовательского опыта. В какой-то степени это подобно традиционному процессу предоставления справок. Как пример, человек берёт из бухгалтерии справку 2-НДФЛ и предоставляет её в банк для одобрения ипотеки. У банка нет прямой связи с работодателем, но он может проверить справку. Цифровое удостоверение подписано цифровой подписью, содержит DID идентификатор пользователя, а при предоставлении удостоверения пользователь аутентифицирует себя через собственную подпись. Верификатор, таким образом, может воспроизвести логическую связь до доверенного эмитента в быстром полностью цифровом виде.

Отсутствие прямой технической связи между эмитентом и верификатором приводит к нивелированию рисков цензурирования эмитентом верификатора. Поскольку субъект самостоятельно контролирует выданные удостоверения, эмитент не обязан хранить пользовательские данные, и эмитентов для одного типа удостоверений может быть много, снижается риск утечки данных со стороны эмитента. Каждый из эмитентов становится менее ценной целью для атак.

Та же логика справедлива и для верификатора, если он не хранит предъявленных данных. Тем не менее полагаться на это допущение опрометчиво. В отличие от эмитента, исходно владеющего информацией, верификатор является получателем данных.

Спецификация Verifiable Credentials указывает общую структуру цифрового удостоверения. По умолчанию используется полное раскрытие атрибутов и алгоритмы подписи JSON-LD, но оставлен достаточно широкий простор для конкретных реализаций схем раскрытия атрибутов и алгоритмов цифровой подписи. В ходе анализа таких

конкретных версий авторы выявили два основных используемых подхода. При полном раскрытии атрибутов пользователь полностью раскрывает свойства удостоверения. Такой подход нежелательно использовать для чувствительных данных, например, данных паспорта. В подходе с селективным раскрытием атрибутов [18–20] раскрывается лишь часть атрибутов.

Часть схем селективного раскрытия страдает от использования специальных криптографических схем, не использующихся в других приложениях. Все же такие схемы страдают от недостаточного контроля пользователем над раскрываемыми атрибутами. Только эмитент решает, какие атрибуты подлежат полному раскрытию, а какие могут быть раскрыты частично, что существенно ограничивает область применения.

Результаты исследования и их обсуждение

Как указано в предыдущем разделе, для обеспечения сохранности пользовательских данных два направления представляют интерес: уменьшение ценности отдельных наборов данных и их раздельное хранение. Для исследования выбраны процессы идентификации, аутентификации и авторизации, осуществляемые в схеме централизованного несуверенного ПИ и в схеме с цифровыми удостоверениями в контексте СИ, которая включает сценарии полного, частичного и нулевого раскрытия атрибутов через технологии ZK. В анализе применяются риск-ориентированный подход к оценке кибербезопасности [21], а также методы теории информации, в частности, используется мера информации Шеннона [22], понятие номической связи для связи данных и информации [23] и оценки угроз конфиденциальности.

Для обозначения элементов данных используется греческий алфавит. Малые буквы α, β, γ, ... обозначают индивидуальные элементы данных для каждого пользователя, совокупность таких элементов в наборе данных по всем пользователям обозначается большими буквами A, B, Γ, ... и т.д. Набор передаваемых или хранимых элементов данных будем обозначать $\alpha \times \beta$.

Процесс идентификации в схеме с ПИ представляется как предоставление сервису от ПИ элемента идентификационных данных (имени) α и подтверждения (явного через цифровую подпись ПИ или неявного через заранее установленное доверие) π, вместе $\alpha \times \pi$. Практически идентификация является частью аутентификации и не используется отдельно, но такое описание полезно для понимания дальнейших шагов.

Процесс аутентификации в схеме с ПИ представляется как предоставление ПИ от пользователя $\alpha \times \beta$, где β – аутентифицирующие данные (пароль или электронная цифровая подпись), и дальнейшая передача сервису от ПИ $\alpha \times \pi$. При этом на стороне ПИ β сравниваются с проверочными данными γ (соответственно, хеш пароля или публичный ключ) из базы данных. Также учтём, что в базе данных ПИ хранятся «технические» данные δ, важные для управления жизненным циклом ЦИ с точки зрения ПИ, например сигнал о том, что ЦИ может быть обслужена и не заблокирована. Таким образом, на стороне ПИ хранятся данные $A \times \Gamma \times \Delta$.

Без потери общности будем считать, что собственно авторизация, то есть получение сигнала, имеет ли пользователь на действие, осуществляется как вычисление над атрибутами пользователя внутри сервиса или аналогичного ниже «верификатора». При таком допущении процесс авторизации в схеме с ПИ является расширением процесса аутентификации: ПИ передаёт сервису $\alpha \times \varepsilon \times \pi$, где ε – атрибуты пользователя. Таким образом, в целом на ПИ хранится $A \times \Gamma \times \Delta \times E$.

Таким же образом можно описать процессы для схемы суверенной идентичности. Процесс идентификации идентичен схеме с ПИ. Процесс аутентификации же отличается тем, что пользователь передаёт сервису («верификатору» в терминологии суверенной идентичности) $\alpha' \times \beta'$, в котором α' есть публичный ключ пользователя, а β' – цифровая

подпись, подтверждающая владение приватным ключом. Без потери общности можно считать это подмножеством $\alpha' \times \beta'$ из схемы с ПИ.

Процесс авторизации существенно отличается. Эмитент выпускает пользователю α цифровое удостоверение ε', содержащее аналог атрибутов ε, оставляя у себя технические данные δ' и «остаток» атрибутов $residue(\varepsilon')$ для возможного отзыва удостоверения или перевыпуска. Например, для паспортов это имя, фамилия, отчество и дата рождения человека. Таким образом, на стороне эмитента для выпуска удостоверения хранится $A' \times residue(E') \times \Delta'$. Верификатор получает от пользователя удостоверение ε' (или данные, выведенные из удостоверения) в составе $\alpha' \times \beta' \times \varepsilon'$. Перед принятием решения об авторизации верификатор должен проверить применимость удостоверения – оно выдано доверенным эмитентом и не отозвано. Можно считать это восстановлением аналога элемента π. Проверка того, что удостоверение выдано эмитентом осуществляется на основе подписи эмитента, находящейся в составе удостоверения. Проверка отзыва осуществляется через запрос к списку отозванных удостоверений Δ'.

Анализ данных в покое позволяет провести оценку угрозы утечки. В случае схемы с ПИ могут быть раскрыты $A \times \Gamma \times \Delta \times E$ на стороне ПИ, $\alpha \times \beta \times \gamma \times \delta \times \varepsilon$ в случае атаки на пользователя или $N \cdot [A \times E]$ при атаке на сервис. Здесь и далее $N \cdot []$ указывает, что раскрываются только данные по всем N пользователям сервиса. В случае суверенной идентичности атака на эмитента даст $A' \times residue(E') \times \Delta'$, атака на пользователя раскроет $\alpha' \times \delta \times \varepsilon'$, атака на сервис раскроет $N \cdot [A' \times E']$.

Отсюда видно, что применение схемы СИ может привести к уменьшению утечек данных только в том случае, когда $I(residue(E')) < I(E)$, и $I(E') < I(E)$, где $I(.)$ – количество информации, содержащейся в наборе данных. В то время, как проповедники СИ утверждают $I(residue(E')) \equiv 0$, практически (без применения ZK) для целей комплаенса и аудита $I(residue(E')) = I(E') = I(E)$, что делает схемы эквивалентными.

Если анализировать данные в движении, нельзя не отметить, что в процессе жизненного цикла ЦИ выпуск-использование-отзыв, объём задействованных данных существенно отличается. Считая, что использование ЦИ для авторизации происходит M раз, видно, что в схеме ПИ задействовано $A \times \beta \times \Gamma \times \Delta \times \varepsilon$ при выпуске, $M \cdot [A \times \beta \times \Gamma \times \Delta \times E]$ при использовании и $A \times \Gamma \times \Delta \times E$ при отзыве, так как происходит поиск по всей базе. В то же время, для схемы СИ задействованы $A' \times \beta' \times \varepsilon' \times \delta'$ при выпуске, $M \cdot [\alpha' \times \beta' \times \varepsilon' \times \Delta']$ при использовании и $A' \times residue(E') \times \Delta$ при отзыве. Интуиция подсказывает, что схема СИ имеет меньшую поверхность атаки за счёт меньшего количества используемых данных. Практически это обусловлено меньшим количеством данных онлайн: $residue(E')$ в схеме СИ может являться частью холодного хранилища с исключительно высоким уровнем защиты, в то время как $A \times \Gamma \times \Delta \times E$ на стороне ПИ должны быть всегда доступны. Тем не менее такая логика не может привести к решающей победе схемы СИ в контексте утечек данных.

С другой стороны, ранее указано, что схема СИ позволяет осуществлять полное, частичное или нулевое (через ZK) раскрытие атрибутов, в отличие от ПИ, позволяющего осуществлять только полное или частичное раскрытие атрибутов. Можно показать, что нулевое раскрытие атрибутов приводит к существенному уменьшению информации, передаваемой верификатору. Соответственно, увеличивается конфиденциальность данных пользователя при атаке верификатора. Это можно продемонстрировать на достаточно часто встречающемся сценарии в индустрии Веб3: из-за регуляторных ограничений часть услуг предоставляется только не гражданам США. ООН признаёт 193 страны [24]. Как полное, так и частичное (только страна) раскрытие атрибутов приведёт к получению $A = -\sum p \log p = -\sum \frac{1}{193} \log \frac{1}{193} = \log 193 \approx 7{,}6$ бит информации. В то же время

использование ZK позволяет раскрывать только информацию о том, что страна человека не является США, что приводит к получению всего $A - \left(-\sum \frac{1}{192} \log \frac{1}{192}\right) \approx 0{,}02$ бит.

Уже в приведённом примере нельзя не заметить, что получение сигнала авторизации «сервисом может пользоваться только не гражданин США» переносится со стороны верификатора на сторону, производящую доказательство, то есть на пользователя. Фактически происходит перенос вычислений на сторону, владеющую исходными данными, так называемое верифицируемое вычисление. Весь процесс идентификации, аутентификации и авторизации в таком случае сводится к передаче сигнала о корректном вычислении над атрибутами пользователя, но такие вычисления всё ещё далеки от сколько-нибудь практической применимости.

Заключение

В исследовании показано, что с точки зрения утечек данных в процессе идентификации, аутентификации и авторизации схема суверенной идентичности и использование провайдера идентичности не имеют отличий при использовании полного или частичного раскрытия атрибутов пользователя. Использование же технологий доказательства с нулевым разглашением в приложении к цифровым удостоверениям как часть схемы суверенной идентичности позволяет значительно уменьшить влияние утечки данных со стороны верификатора за счёт уменьшения информации, которой он владеет.

Список источников

1. Отчет об исследовании утечек информации ограниченного доступа в I половине 2022 г. // INFOWATCH: разработчик решений для обеспечения информационной безопасности. URL: https://www.infowatch.ru/sites/default/files/analytics/files/otchyot-ob-utechkakh-dannykh-za-1-polugodie-2022-goda_1.pdf (дата обращения: 05.02.24).

2. Утечки информации ограниченного доступа в мире и в России, первое полугодие 2023 г. // INFOWATCH: разработчик решений для обеспечения информационной безопасности. URL: https://www.infowatch.ru/sites/default/files/analytics/files/utechki-informatsii-ogranichennogo-dostupa-v-mire-i-rossii-za-pervoe-polugodie-2023-goda.pdf (дата обращения: 05.02.24).

3. Гайсина А.Р., Филатова Т.А. Особенности утечек информации ограниченного доступа в Российской Федерации // Национальная безопасность и стратегическое планирование. 2024. № 1 (45). С. 46–59. DOI: 10.37468/2307-1400-2024-1-46-59. EDN MQEZZF.

4. Варзин С.А., Матвеев В.В. Обеспечение информационной безопасности в системе здравоохранения // Национальная безопасность и стратегическое планирование. 2023. № 3 (43). С. 19–56. DOI: 10.37468/2307-1400-2024-2023-3-19-56. EDN ONKEFE.

5. Денис @denis-19. В свободном доступе выложили архив сервиса «Яндекс.Еда» с данными заказов клиентов, «Яндекс» ранее подтвердил утечку // Хабр. 2022. 2 марта. URL: https://habr.com/ru/news/654039/ (дата обращения: 05.02.2024).

6. О персональных данных: Федер. закон от 27 июля 2006 г. № 152-ФЗ. URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 31.07.2024).

7. Шугаев В.А., Алексеенко С.П. Классификация инсайдерских угроз информации // Вестник Воронежского института МВД России. 2020. № 2. С. 143–153.

8. Palmer M. Data is the New Oil. 2006. 3 нояб. URL: https://ana.blogs.com/maestros/2006/11/data_is_the_new.html (дата обращения: 31.07.2024).

9. Buterin V. Control as Liability. 2019. 9 мая. URL: https://vitalik.eth.limo/general/2019/05/09/control_as_liability.html (дата обращения: 31.07.2024).

10. Goldreich O., Oren Y. Definitions and properties of zero-knowledge proof systems // Journal of Cryptology. 1994. Vol. 7. № 1. P. 1–32.

11. Кузьмин А.М., Свичкарь Д.А., Хенкин П.В. Мошенничество с использованием синтетических цифровых личностей // Современные информационные технологии и ИТ-образование. 2023. Т. 19. № 2. С. 251–261.

12. Кондаков А.М., Костылева А.А. Цифровая идентичность, цифровая самоидентификация, цифровой профиль: постановка проблемы // Вестник Российского университета дружбы народов. Сер.: Информатизация образования. 2019. Т. 16. № 3. С. 207–218. DOI: 10.22363/2312-8631-2019-16-3-207-218

13. Preukschat A., Reed D. Self-Sovereign Identity: Decentralized digital identity and verifiable credential. Maning, 2021. 504 p.

14. OpenID Connect Core 1.0. Спецификация. URL: https://openid.net/specs/openid-connect-core-1_0.html (дата обращения: 31.07.2024).

15. SAML 2.0 Core. Спецификация. URL: https://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf (дата обращения: 31.07.2024).

16. Decentralized Identifiers (DIDs) v1.0 // The World Web Wibe Consortium (W3C). URL: https://www.w3.org/TR/did-core (data obrashcheniay: 05.02.24).

17. Verifiable credentials Data Model v2.0 // The World Web Wibe Consortium (W3C). URL: https://www.w3.org/TR/vc-data-model-2.0 (дата обращения: 05.02.24)

18. Selective disclosure of claims from multiple digital credentials / Š.B. Ramić [et al.] // University of Sarajevo Faculty of Electrical Engineering Sarajevo Bosnia and Herzegovina, 2024. 13 p.

19. The BBS Signature Scheme // Identity Foundation DIF. URL: https://identity.foundation/bbs-signature/draft-irtf-cfrg-bbs-signatures.html. (дата обращения: 02.05.24).

20. Selective Disclosure for JWTs (SD-JWT) // IETF Datatracker. URL: https://datatracker.ietf.org/doc/html/draft-ietf-oauth-selective-disclosure-jwt (дата обращения: 02.05.2024).

21. Парьев С.Е., Правиков Д.И., Карантаев В.Г. Особенности применения риск-ориентированного подхода для обеспечения кибербезопасности промышленных объектов // Безопасность информационных технологий. 2020. Т. 27. № 4. С. 37–52. ISSN 2074-7136.

22. Верещагин Н.К., Щепин Е.В. Информация, кодирование и предсказание. М.: ФМОП, МЦНМО, 2012. 236 с.

23. Ziller A., Mueller T.T., Braren R., Rueckert D., Kaissis G. Privacy: An Axiomatic Approach // Entropy. 2022. Т. 24. № 5. Ст. 714. ISSN 1099-4300. DOI: 10.3390/e24050714.

24. Рост численности государств – членов ООН // Организация Объединенных Наций. URL: https://www.un.org/ru/about-us/growth-in-un-membership (дата обращения: 31.07.2024).

References

1. Otchet ob issledovanii utechek informacii ogranichennogo dostupa v I polovine 2022 g. // INFOWATCH: razrabotchik reshenij dlya obespecheniya informacionnoj bezopasnosti. URL: https://www.infowatch.ru/sites/default/files/analytics/files/otchyot-ob-utechkakh-dannykh-za-1-polugodie-2022-goda_1.pdf (data obrashcheniya: 05.02.24).

2. Utechki informacii ogranichennogo dostupa v mire i v Rossii, pervoe polugodie 2023 g. // INFOWATCH: razrabotchik reshenij dlya obespecheniya informacionnoj bezopasnosti. URL: https://www.infowatch.ru/sites/default/files/analytics/files/utechki-informatsii-ogranichennogo-dostupa-v-mire-i-rossii-za-pervoe-polugodie-2023-goda.pdf (data obrashcheniya: 05.02.24).

3. Gajsina A.R., Filatova T.A. Osobennosti utechek informacii ogranichennogo dostupa v Rossijskoj Federacii // Nacional'naya bezopasnost' i strategicheskoe planirovanie. 2024. № 1 (45). S. 46–59. DOI: 10.37468/2307-1400-2024-1-46-59. EDN MQEZZF.

4. Varzin S.A., Matveev V.V. Obespechenie informacionnoj bezopasnosti v sisteme zdravoohraneniya // Nacional'naya bezopasnost' i strategicheskoe planirovanie. 2023. № 3 (43). S. 19–56. DOI 10.37468/2307-1400-2024-2023-3-19-56. EDN ONKEFE.

5. Denis @denis-19. V svobodnom dostupe vylozhili arhiv servisa «Yandeks.Eda» s dannymi zakazov klientov, «Yandeks» ranee podtverdil utechku // Habr. 2022. 2 marta. URL: https://habr.com/ru/news/654039/ (data obrashcheniya: 05.02.2024).

6. O personal'nyh dannyh: Feder. zakon ot 27 iyulya 2006 g. № 152-FZ. URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (data obrashcheniya: 31.07.2024).

7. Shugaev V.A., Alekseenko S.P. Klassifikaciya insajderskih ugroz informacii // Vestnik Voronezhskogo instituta MVD Rossii. 2020. № 2. S. 143–153.

8. Palmer M. Data is the New Oil. 2006. 3 noyab. URL: https://ana.blogs.com/maestros/2006/11/data_is_the_new.html (data obrashcheniya: 31.07.2024).

9. Buterin V. Control as Liability. 2019. 9 maya. URL: https://vitalik.eth.limo/general/2019/05/09/control_as_liability.html (data obrashcheniya: 31.07.2024).

10. Goldreich O., Oren Y. Definitions and properties of zero-knowledge proof systems // Journal of Cryptology. 1994. Vol. 7. № 1. P. 1–32.

11. Kuz'min A.M., Svichkar' D.A., Henkin P.V. Moshennichestvo s ispol'zovaniem sinteticheskih cifrovyh lichnostej // Sovremennye informacionnye tekhnologii i IT-obrazovanie. 2023. T. 19. № 2. S. 251–261.

12. Kondakov A.M., Kostyleva A.A. Cifrovaya identichnost', cifrovaya samoidentifikaciya, cifrovoĭ profil': postanovka problemy // Vestnik Rossiĭskogo universiteta druzhby narodov. Ser.: Informatizaciya obrazovaniya. 2019. T. 16. № 3. S. 207–218. DOI: 10.22363/2312-8631-2019-16-3-207-218

13. Preukschat A., Reed D. Self-Sovereign Identity: Decentralized digital identity and verifiable credential. Maning, 2021. 504 p.

14. OpenID Connect Core 1.0. Specifikaciya. URL: https://openid.net/specs/openid-connect-core-1_0.html (data obrashcheniya: 31.07.2024).

15. SAML 2.0 Core. Specifikaciya. URL: https://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf (data obrashcheniya: 31.07.2024).

16. Decentralized Identifiers (DIDs) v1.0 // The World Web Wibe Consortium (W3C). URL: https://www.w3.org/TR/did-core (data obrashcheniay: 05.02.24).

17. Verifiable credentials Data Model v2.0 // The World Web Wibe Consortium (W3C). URL: https://www.w3.org/TR/vc-data-model-2.0 (data obrashcheniya: 05.02.24)

18. Selective disclosure of claims from multiple digital credentials / Š.B. Ramić [et al.] // University of Sarajevo Faculty of Electrical Engineering Sarajevo Bosnia and Herzegovina, 2024. 13 p.

19. The BBS Signature Scheme // Identity Foundation DIF. URL: https://identity.foundation/bbs-signature/draft-irtf-cfrg-bbs-signatures.html (data obrashcheniya: 02.05.24).

20. Selective Disclosure for JWTs (SD-JWT) // IETF Datatracker. URL: https://datatracker.ietf.org/doc/html/draft-ietf-oauth-selective-disclosure-jwt (data obrashcheniya: 02.05.2024).

21. Par'ev S.E., Pravikov D.I., Karantaev V.G. Osobennosti primeneniya risk-orientirovannogo podhoda dlya obespecheniya kiberbezopasnosti promyshlennyh ob"ektov // Bezopasnost' informacionnyh tekhnologij. 2020. T. 27. № 4. S. 37–52. ISSN 2074-7136.

22. Vereshchagin N.K., Shchepin E.V. Informaciya, kodirovanie i predskazanie. M.: FMOP, MCNMO, 2012. 236 s.

23. Ziller A., Mueller T.T., Braren R., Rueckert D., Kaissis G. Privacy: An Axiomatic Approach // Entropy. 2022. T. 24. № 5. St. 714. ISSN 1099-4300. DOI: 10.3390/e24050714.

24. Rost chislennosti gosudarstv – chlenov OON // Organizaciya Ob"edinennyh Nacij. URL: https://www.un.org/ru/about-us/growth-in-un-membership (data obrashcheniya: 31.07.2024)

Информация о статье:
Статья поступила в редакцию: 20.10.2024; одобрена после рецензирования: 17.11.2024;
принята к публикации: 20.11.2024
Information about the article:
The article was submitted to the editorial office: 20.10.2024; approved after review: 17.11.2024;
accepted for publication: 20.11.2024

Сведения об авторах:
Дешевов Павел Павлович, преподаватель кафедры КБ-4 «Интеллектуальные системы информационной безопасности» МИРЭА – Российского технологического университета (119454, Москва, пр. Вернадского, д. 78), email: pavelpal.d@gmail.com, https://orcid.org/0000-0001-6675-2692, SPIN-код: 8797-6900
Укустов Сергей Сергеевич, старший преподаватель кафедры системы автоматизированного проектирования и поискового конструирования Волгоградского государственного технического университета (400005, г. Волгоград, пр. Ленина, д. 28), email: sergey@ukstv.me, https://orcid.org/0009-0001-5639-9319

Information about the authors:
Deshevov Pavel P., lecturerof the department of KB-4 «Intelligent information security systems department» of MIREA – Russian technological university (119454, Moscow, Vernadsky pr., 78), email: pavelpal.d@gmail.com, https://orcid.org/0000-0001-6675-2692, SPIN: 8797-6900
Ukustov Sergey S., senior lecturer at Systems of computer-aided design and exploratory construction department, Volgograd state technological university (400005, Volgograd, Lenina ave, 28), email: sergey@ukstv.me, https://orcid.org/0009-0001-5639-9319