Научная статья
УДК 004.056
https://doi.org/10.24143/2072-9502-2024-4-60-69
EDN ESPOWD

Механизмы обеспечения конфиденциальности в децентрализованных публичных системах

Алексей Владимирович Ненашев

Самарский государственный технический университет,
Самара, Россия, alexvlnenashev@gmail.com

ООО «ТХЕООЛ»,
Самара, Россия

Аннотация. Рассматриваются механизмы обеспечения конфиденциальности и подавления цифрового следа пользователей в публичном децентрализованном облачном сервисе обработки контента. Этот сервис представляет собой универсальную децентрализованную операционную систему, предназначенную для защиты распределенных вычислений. Представлена модель взаимодействия между пользователями и поставщиками вычислительных ресурсов. В моделировании участвовали система управления метаданными, подсистема поиска и подсистема распределения задач и вознаграждений. Предложены и обоснованы механизмы защиты конфиденциальности. Обсуждаются их ограничения и возможности применения. Защита конфиденциальности выполняется путем маскировки и преобразований персональных данных участников сети, технических данных их узлов и криптографических методов защиты вычислений в децентрализованном облаке. Предлагаемая система защиты конфиденциальности закрывает подсистемы управления пользователями, разграничения доступа, транспортных протоколов, биллинга и данных от владельцев вычислительных ресурсов, обслуживающих сервис. Модель защиты конфиденциальности включает систему сложного распределения задач и их частей между техническими узлами. Для защиты пользователя от деанонимизации по IP-адресу в нее включена подсистема обфусцирующей маршрутизации, которая позволяет скрыть метаданные пользователя от его контрагентов внутри сервиса и от владельцев телекоммуникационной инфраструктуры, обслуживающих сервис. Для защиты от идентификации по метаданным смарт-контрактов и взаимодействий с узлами-исполнителями в сервис интегрирован алгоритм подмены счетов и пользовательских идентификаторов. Этот же алгоритм позволяет защищать данные пользователя от других пользователей при взаимодействиях различных типов, если эти взаимодействия организованы через подсистему смарт-контрактов сервиса. Перечисленные подсистемы формируют алгоритмическую прослойку, позволяющую полностью абстрагировать клиентов системы от владельцев облачной инфраструктуры сервиса, что, в свою очередь, позволяет пользователям безопасно хранить и обрабатывать данные внутри сервиса даже в случае, когда технические узлы сервиса принадлежат недоверенным и/или прямо скомпрометированным владельцам.

Ключевые слова: децентрализованный сервис, распределенный реестр, обфускация, маршрутизация, гомоморфное шифрование, защита информации, конфиденциальность

Благодарности: работа выполнена в интересах исследовательской компании ООО «ТХЕООЛ». ООО «ТХЕООЛ» – аккредитованный участник проекта Сколково, резидент технопарка «Жигулевская долина», резидент НПЦ БАС Самара. ООО «ТХЕООЛ» ведет разработки систем безопасных коммуникаций и связи при поддержке Фонда «Сколково», Фонда содействия инновациям, Фонда НТИ и Самарского государственного технического университета.

Для цитирования: *Ненашев А. В.* Механизмы обеспечения конфиденциальности в децентрализованных публичных системах // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2024. № 4. С. 60–69. https://doi.org/10.24143/2072-9502-2024-4-60-69. EDN ESPOWD.

Original article

Mechanisms for ensuring confidentiality in decentralized public systems

Aleksei V. Nenashev

Samara State Technical University,
Samara, Russia, alexvlnenashev@gmail.com

THEOOL, LLC,
Samara, Russia

Abstract. The system for privacy protection and suppression of users' digital footprint in a public decentralized cloud content processing service is considered. This service is a universal decentralized operating system designed to protect distributed computing. The model of the interaction between users and computing resource providers is presented. The modeling involved a metadata management system, a search subsystem, and a task and reward distribution subsystem. The privacy protection mechanisms are proposed and justified. The limitations and possibilities of their application are discussed. The obtained model protects by masking transformations of personal data of network participants and technical data of their nodes, cryptographic methods of protection of computations in a decentralized cloud. The proposed privacy protection system protects the subsystems of user management, access delimitation, transport protocols, billing, and data from the owners of computing resources serving the service. The privacy protection model includes a system of tasks executing with complex distribution task parts between technical nodes. To protect the user from deanonymization by IP address, it includes an obfuscating routing subsystem, which allows the hiding of the user's metadata from his counterparties within the service and from the owners of the telecommunications infrastructure servicing the service. To protect against identification by smart contract metadata and interactions with performer nodes, the service has an integrated algorithm for substituting accounts and user identifiers. The same algorithm allows the protection of user data from other users during interactions of various types if these interactions are organized through the smart contract subsystem of the service. The listed subsystems form an algorithmic layer that allows complete abstraction of the system's clients from the owners of the service's cloud infrastructure, which in turn will enable users to safely store and process data within the service even in cases where the technical nodes of the service belong to untrusted and/or directly compromised owners.

Keywords: decentralized service, distributed registry, obfuscation, routing, homomorphic encryption, information protection, confidentiality

Acknowledgment: the work was carried out in the interests of the research company TheOoL LLC. TheOoL LLC is an accredited participant in the Skolkovo project, a resident of the Zhigulevskaya Dolina Technopark, a resident of the BAS Samara SPC. TheOoL LLC develops secure communications and communication systems with the support of the Skolkovo Foundation, the Innovation Promotion Foundation, the STI Foundation and the Samara State Technical University.

For citation: Nenashev A. V. Mechanisms for ensuring confidentiality in decentralized public systems. *Vestnik of Astrakhan State Technical University. Series: Management, computer science and informatics*. 2024;4:60-69. (In Russ.). https://doi.org/10.24143/2072-9502-2024-4-60-69. EDN ESPOWD.

Введение

Проблемы и противоречия современного интернета, построенного в концепции Web2.0, умноженные на процесс слияния виртуального и реального миров через постепенное проникновение во все сферы производства и жизни технологий «интернета вещей» и концепции «интернета всего», привели к существенному увеличению значимости угроз информационной безопасности [1]. В особенности это касается информационных систем интернета (ИСИ). Как правило, угрозы осуществляются:

1) через внешние по отношению к ИСИ каналы (провайдеров интернета, операторов связи, которые обеспечивают передачу данных от абонента к ИСИ, и их персонал);

2) владельцев облачной инфраструктуры, на которой исполняются алгоритмы ИСИ, и их персонал;

3) владельцев ИСИ и их персонал;

4) разработчиков программного обеспечения ИСИ, которые часто оставляют уязвимости и «черные ходы», – в качестве дополнительного источника угроз.

Угрозы реализуются как в результате намеренных действий, так и в результате ошибок. Таким образом, при проектировании и реализации системы защиты информации ИСИ необходимо решить задачу полного перекрытия источников угроз 1–4, причем, если задача перекрытия угроз 1 типа в целом решена в централизованных ИСИ, реализация защиты от источников угроз 2 типа частично решена, то для источников угроз 3 и 4 типа решение фактически отсутствует. Такая ситуация приводит к непрерывному потоку инцидентов на ИСИ, в том числе управляющих объектами критической инфраструктуры [2]. Все это приводит к существенному росту расходов на информационную безопасность и покрытие ущерба от инцидентов. Это, в свою очередь, стимулирует инженеров на поиск способов снижения этих затрат, в том числе через изменение подходов к организации информационных систем.

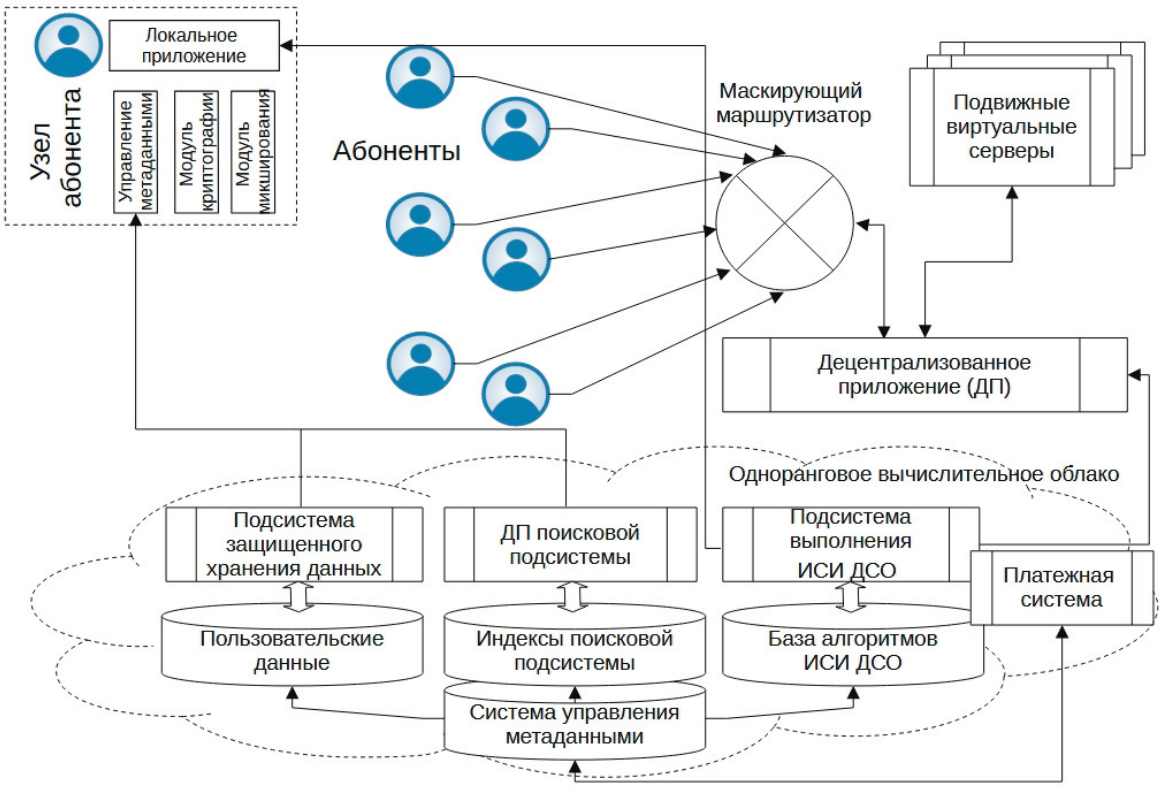
Широкое распространение при создании облачных сервисов нового типа получила концепция построения сервисов в одноранговой децентрализованной архитектуре с управлением на базе технологии распределенных реестров [3]. Следование этой концепции означает децентрализацию сервисов в техническом, а также в организационно-правовом смысле, т. к. их компоненты, выполняющие единую функцию, могут иметь разных владельцев. Для управления взаимодействиями они объединяются в форме децентрализованных автономных организаций (ДАО) [4, 5]. Роль органа управления в ДАО выполняет принятый участниками алгоритм, который определяет правила взаимодействия в рамках

конкретной ДАО. Целостность этих правил надежно обеспечивается свойствами распределенного реестра и алгоритмов консенсуса, что математически и эмпирически, на протяжении 14 лет, доказано первым ДАО – сетью децентрализованных финансов Bitcoin [6].

При проектировании и создании такого рода децентрализованных публичных систем (ДПС) крайне важно обеспечить должную защиту обрабатываемых в этих системах данных. При этом следует учитывать не только необходимость управления доступом к данным со стороны различных групп пользователей и защиту от внешних по отношению к ДПС угроз, как в аналогичных системах с централизованным управлением, но и максимальную защиту данных от внутренних акторов системы. Это обусловлено ее публичным характером, что означает, во-первых, децентрализацию не столько по географии, сколько по множеству взаимно независимых владельцев компонентов системы. Во-вторых, публичность системы означает возможность свободного присоединения к ней новых обслуживающих узлов с независимыми владельцами и новых пользователей. Эти факторы требуют исключить участие в работе подсистемы информационной безопасности ДПС обслуживающего персонала (автоматизации процессов) и обеспечения максимальной анонимизации акторов системы, исключения между ними информационного обмена любого типа, кроме случаев, когда такой обмен необходим самому актору, происходит с его согласия и полностью им контролируется.

Архитектура и модель ДПС

Архитектуру и функционирование ДПС рассмотрим на примере децентрализованного сервиса облачного хранения и обработки контента (ДСО).



Архитектура ДСО [1, 7]

DCS architecture [1, 7]

Рассматриваемая система обладает всеми особенностями современных децентрализованных сервисов [3, 8], поэтому рассмотрение предмета настоящей работы на ее примере считаем показательным и релевантным. Основой ДСО является программное обеспечение (ПО) децентрализованного высокоскоростного облака серверов, которое реализует оверлейную среду обработки защищаемых сведений без доступа к данным со стороны провайдеров и владельцев серверов. Это ПО реали-

зует управляющие алгоритмы ДСО и является основой для функционирования открытого сообщества в организационной форме децентрализованной автономной организации (ДАО) [4, 5], обслуживающей интересы объединений пользователей с распределенной географической и/или организационной структурой. Архитектура ДСО включает децентрализованные компоненты: вычислительное облако для выполнения пользовательских децентрализованных приложений (ПДП); хранилище данных; поисковую подсистему; встроенную платежную систему – систему управления метаданными (СУМ); технические подсистемы (автоматы поддержания целостности и доступности данных, автоматы оптимизации работы облака данных по производительности и надежности).

Для обеспечения целостности метаданных используется технология распределенных реестров [9, 10]. Конкретные вычислительные задачи назначаются узлам облака ДСО, которые подразделяются на 2 основных класса: абонентские узлы (АУ) и технические узлы (ТУ). На АУ происходит исполнение пользовательского интерфейса (ПИ) ПДП и взаимодействие с ДСО через ТУ с функцией маршрутизаторов ДСО. Сеть ТУ можно представить множеством узлов [1, 11]:

$$S_t \equiv S_m \cup S_d \cup S_s \cup S_{ss} \equiv \left\{X_1,\ \ldots, X_i,\ \ldots, X_\xi\right\}; X_i = \left\{a,\, b,\, c\right\};\ i = \overline{1\ldots\xi}\,, \tag{1}$$

где S_m – ТУ с функцией узла метаданных (УМ); S_d – ТУ, исполняющие алгоритмы консенсуса распределенного реестра ДСО; S_s – ТУ, непосредственно исполняющие задачи ПДП; S_{ss} – ТУ, обслуживающие поисковую подсистему; X_i – множество доступных ресурсов конкретного ТУ [11, 12]; ξ – общее количество ТУ в облаке; a – количество свободных мест в очереди узла; b – быстродействие узла; c – доступное пространство дисковой подсистемы узла.

Для каждого АУ поддерживаются 2 индекса-списка абонентов в поисковой подсистеме ДСО: A – список абонентов, которые зарегистрированы как пользователи конкретного ПДП; A_o – список абонентов в состоянии «онлайн». Определим множества A и A_o:

$$A = \left\{a_1,\ \ldots,\ a_n\right\}; A_o = \left\{a_1,\ \ldots,\ a_k\right\};\ a_i = \left\{id_i,\ t_i,\ Q_i^s,\ t_i^{\max}\right\}, \tag{2}$$

где a_i – абонент в списке, характеризуемый временем жизни t_i, $t_i^{\max}$ – максимальным временем хранения, статическим публичным ключом алгоритма криптографии эллиптических кривых (ECC) [13] Q_i^s и уникальным идентификатором id_i, при этом диапазон изменения индекса i определяется принадлежностью к определенному списку:

$$i = \overline{1\ldots n}\,\middle|\, a_i \in A,\ i = \overline{1\ldots k}\,\middle|\, a_i \in A_0\ ;\ n = \left|A\right|;\ \ k = \left|A_0\right|.$$

Здесь АУ и ТУ содержат множество идентификаторов абонентов, принадлежащих их владельцам:

$$U = \left\{u_1,\ \ldots,\ u_r\right\};\ u_j = \left\{id_j,\, d_j^s,\, Q_j^s\right\};\ Q_j^s = \ d_j^s G;\ j = \overline{1\ldots r}, \tag{3}$$

где id_j – уникальный идентификатор абонента; d_j^s – статический закрытый ключ абонента; Q_j^s – статический открытый ключ абонента; G – опорная точка эллиптической кривой, общая для сети ДСО; r – количество абонентов, которое обслуживает конкретный узел. Один из $u_j = \left\{id_j,\, d_j^s,\, Q_j^s\right\} \in U$ назначается владельцем узла в качестве идентификатора узла в сети ДСО, а его id_j используется в качестве адреса узла.

Списком A управляет поисковая система ДСО и АУ для каждого подключенного в АУ ПДП. При запуске АУ, по его запросу и для каждого ПДП A, на множествах (2), (3) выполняется следующий функционал:

$$\left\{t_j = 0 \,|\, id_j \in A\right\};\ \left\{f : \mathrm{U} \to \left\{a = \left\{id_j,\ t_j = 0,\ Q_j^s,\ t_j^{\max}\right\} \in A\right\} | \, id_j \notin A\right\};\ j = \overline{1\ldots r}.$$

Таким образом, при запуске АУ узел проверяет наличие записей о зарегистрированных на нем u_j в множестве A зарегистрированной на нем ПДП и создает либо обновляет необходимые записи индекса.

Список A_o требует постоянного мониторинга активности абонентов со стороны ПДП. К управлению этим списком, кроме поисковой подсистемы, подключаются вычислительные процессы, запускаемые в рамках ПДП на выделенных для конкретного ПДП УМ. Из них ПДП назначает узлу два контролирующих УМ (КУМ) из (1), в обязанность которых входит продление времени жизни

записи об активности абонента в поисковой подсистеме ДСО:

$$f: S_m \to \left\{ \{\text{КУМ}_1,\ \text{КУМ}_2\} \mid \max_{a,\,b} S_m \right\}.$$

Запись о назначенных абоненту КУМ также вносится в поисковую подсистему. Последующая коммуникация абонента с другими пользователями ПДП осуществляется через КУМ. Для каждого *j*-го абонента на множествах (2), (3) выполняется следующий функционал:

$$f: U \to \left\{ a = \left\{ id_j,\ t_j = 0,\ Q_j^s,\ t_j^{\max} = 2,\ \{\text{КУМ}_1,\ \text{КУМ}_2\} \right\} \in A_o \right\} \mid id_j \notin A_o,\ j = \overline{1 \ldots k},$$

причем КУМ опрашивают абонента с установленной ПДП периодичностью и обновляют A_o. При этом КУМ не обрабатывает данные ПДП, а обеспечивает первоначальную коммутацию и взаимодействие с выделенными ПДП ТУ из множества S_d.

При прямом включении АУ КУМ вынужденно обладают информацией об идентификаторе клиента на транспортном уровне, что потенциально создает угрозу компрометации пользователя.

Как пользователь ПДП абонент ставит вычислительные задачи облаку ТУ. Непосредственные вычисления, хранение и обработка данных осуществляются ТУ выделенными ДСО для обслуживания задач конкретного ПДП. Функционирование ТУ требует затрат ресурсов, поэтому ДАО ДСО мотивирует их владельцев на поддержание ТУ в рабочем состоянии и выполнение требований к качеству сервиса (*Q*oS) через биллинговую подсистему встроенной платежной системы ДСО [14], которая функционирует на смарт-контрактах. Через нее абоненты передают плату за использованные вычислительные ресурсы владельцам ТУ. В качестве адреса для перечисления платы используется специально выделенный id_j ТУ.

Для получения произвольного задания ТУ формирует оферту в сторону произвольного заказчика (публичную оферту) при регистрации аппаратного узла исполнителя в ДСО. В момент регистрации ТУ получает рейтинг $\varepsilon_j(t_i)$, который определен как отношение функций доступности $d(t_i)$ и производительности $r\left(t_i, \bar{X}_j\right)$ узла и изменяется со временем:

$$\varepsilon_j(t) = r\left(t_i, \bar{X}_j\right) / d\left(t_i,\right), \tag{4}$$

где $t_i = t_{i-1} + \delta,\ i = \overline{0 \ldots k}$ – дискретный момент времени в промежутке $[t_0, t_k]$, t_0 – момент регистрации узла исполнителя в сети; t_k – момент исключения узла исполнителя из сети, δ – дискретный шаг; $\bar{X}_j$ – вектор доступных ресурсов ТУ в момент t_i с учетом очереди заданий [11, 14]; $j = \overline{1 \ldots \xi}$ – порядковый номер (идентификатор) узла ξ_j среди ξ, доступных в системе ТУ.

Требования ДСО по $d(t_i)$ в (4) установлены неравенством $0{,}9 \le d(t_i)$. Коэффициент доступности $d(t_i)$ рекурсивно определяется функционалом

$$d\left(t_i\right) = \begin{cases} 1,\ r \le 1; \\ d_r,\ r > 1,\ d_r \ge 0{,}9; \\ 0,\ r > 1,\ d_r \le 0{,}9, \end{cases} \tag{5}$$

где

$$d_r = \begin{cases} \left(\sum_0^{i-1} d\left(t_{i-1}\right) + F\left(\xi_j\right) - d\left(t_{i-r}\right) \right) / (i - r);\ r = i - (i \bmod 100) \ne i; \\ \left(\sum_0^{i-1} d\left(t_{i-1}\right) + F\left(\xi_j\right) \right) / i;\ r = i - (i \bmod 100) = i, \end{cases},$$

где $F\left(\xi_j\right)$ – булева функция доступности *j*-го узла в момент t_i.

Если $d(t_i) = 0$, ТУ будет принудительно удален из сети.

Затем ТУ формирует вектор цен за использование вычислительных ресурсов узла $\bar{C}_j^c$, $\left|\bar{C}_j^c\right| = \left|\bar{X}_j\right|$, получает назначенную ему очередь непринятых заданий $\psi_j(t_i)$ и максимально допустимое количество непринятых заданий $\varphi_j \ge \left|\psi_j(t_i)\right|$.

Из публичных оферт ТУ $P_j(t_i) = \left\{ \varepsilon_j(t_i),\ \bar{C}_j^c,\ \bar{X}_j, \psi_j(t_i), \varphi_j \right\}$ с учетом (4) и (5) формируется множество K публичных оферт на продажу вычислительных ресурсов, доступных в момент времени t_i:

$$K = \left\{ \begin{matrix} P_1(t_i) \\ \ldots \\ P_\xi(t_i) \end{matrix} \right\}. \tag{6}$$

Здесь АУ размещает в ДСО вычислительную задачу $L_m = \left\{ l_1^m,\ \ldots,\ l_n^m \right\},\ m = \overline{1, \ldots, \xi_q}$, которая дробится на элементарные подзадачи $l_r^m,\ r = \overline{1, \ldots, n}$,

задает требования к облаку ДСО и параметры доступа $B_m = \left\{B_1^m, ..., B_n^m\right\}$, $m = \overline{1, ..., \xi_q}$, определяет максимальный уровень цен $C_m = \left\{\bar{C}_1^m, ..., \bar{C}_n^m\right\}$, $m = \overline{1, ..., \xi_q}$, указывает время жизни вычислительной задачи в сети T_m, кратное δ, и требования к QoS через указание нижнего порога рейтинга ТУ ε_m, причем $\left|L_m\right| = \left|B_m\right| = \left|C_m\right|$, формирует задания, пригодные к исполнению, отдельным ТУ $w_r^m = \left\{T_m, \varepsilon_m, l_r^m, B_r^m, \bar{C}_r^m\right\}$, $r = \overline{1, ..., n}$ и связывает их в суперзадание

$$W_m = \left\{T_m, \varepsilon_m, L_m, B_m, C_m\right\} \quad (7)$$

с общим адресом для начисления и списания платежей m и правилами их дальнейшего распределения по субсчетам r, $r = \overline{1, ..., n}$. Затем из (6) отбирает подходящего исполнителя

$$P = \min_{\sum \bar{C}_j^c} \left\{P_j\left(t_i\right) \mid \left(\varepsilon_m \geq \varepsilon_j\left(t_i\right)\right) \wedge \left(\varphi_j \geq \left|\psi_j\left(t_i\right)\right|\right) \wedge \left(\sum \bar{C}_j^c \leq \sum \bar{C}_r^m\right) \wedge \left(\forall B_r^m \leq \forall \overline{V_j}\right)\right\}$$

для каждой $w_r^m \in W_m$ и помещает ее в очередь непринятых заданий узла-исполнителя $w_r^m \Rightarrow \psi_j\left(t_i\right)$. На следующем шаге ($t = t_{i+1}$) генерируются смарт-контракты, утвержденные ТУ-исполнителями:

$SK_m = F_{SK}\left(\left\{sk_1^m, ..., sk_n^m\right\}\right)$, $sk_r^m = F_{sk}\left(w_r^m, P\right)$, $r = \overline{1, ..., n}$,

где F_{SK} – скрипт смарт-контракта на исполнение W_m, а F_{sk} – скрипты субконтрактов на исполнение w_r^m с конкретными ξ_j.

В W_m входит исчерпывающий список заданий, включающий задания на маршрутизацию данных, обработку метаданных, хранение и передачу данных, распределенные вычисления и т. п., которые выполняются ТУ в рамках поставленной перед ДСО пользовательской задачи.

Защита конфиденциальности данных и участников ДПС

Широко известно, что существует три класса угроз информационной безопасности: конфиденциальности, целостности и доступности [15–18]. Противодействие угрозам доступности и целостности в ДПС подробно рассмотрены в работах [1, 7, 11, 12, 14] и др. В настоящей работе рассмотрим защиту конфиденциальности ДПС.

Из представленной модели объекта защиты можно определить источники угроз. Во-первых, это внешние по отношению к ДСО источники (ИУ-1): интернет-провайдеры, обеспечивающие функционирование публичной сети, поверх которой функционирует ДСО. Они имеют возможность анализировать трафик между узлами ДСО и фиксировать факты и метаданные подключения узлов ДСО к облаку (IP-адреса, отпечатки аппаратного обеспечения узлов) [19, 20]. Во-вторых, опасность представляют потенциально скомпрометированные ТУ (ИУ-2), например, оснащенные заведомо модифицированным на сбор данных ПО узла ДСО. Из-за публичного и открытого характера ДАО ДСО, как указывалось выше, вероятность внедрения в ДСО таких ТУ крайне высока. Скомпрометированный ТУ имеет возможность сбора метаданных поставленных ему задач и АУ заказчиков, сбора данных, переданных ему в рамках задач по их пересылке либо хранению, а также данных в рамках порученных этому ТУ вычислений (операций с метаданными, смарт-контрактами, платежами, вычислений ПДП).

Для нейтрализации угроз конфиденциальности в ДСО применяются методы обфускации данных: замена, перемешивание и шифрование. Перемешивание реализовано прямо на этапе постановки задачи облаку ДСО (7), когда для каждого $w_r^m \in W_m$ назначается отдельный ТУ, с которым АУ открывает персональный сеанс связи. В рамках такого сеанса трафик между узлами ДСО шифруется криптостойкими алгоритмами [12, 13, 21] с применением сеансовых ключей. Новая пара ключей генерируется для каждого нового сеанса связи между узлами ДСО. Несомненно, ИУ-1, обеспечивающий АУ «последнюю милю», сможет перехватить трафик всех сеансов. Эту ситуацию предотвратить технически невозможно, однако использование уникальных ключей шифрования для каждого сеанса (каждого куска задания W_m) делает процесс расшифровки крайне затруднительным (практически невероятным) из-за доказанной криптостойкости используемых алгоритмов шифрования. Все ИУ-1 на втором и последующих «прыжках» IP-маршрутизации [22] уже получат только часть трафика, связанного с конкретным W_m. Перехват ИУ-1 трафика от ТУ, находящегося в зоне его действия, кажется абсолютно бессмысленным, т. к. любой ТУ владеет только «кусками» от различных W_m, если не учитывать перехват метаданных подключения, что создает возможность деанонимизации участников сеансов, определения их географического положения и установления фактов взаимодействия между абонентами сети, что представляет оперативный интерес даже без раскрытия сущности таких взаимодействий [23]. Метаданные подключения могут (и будут) собирать как ИУ-1, так и ИУ-2.

Вестник Астраханского государственного технического университета.
Серия: Управление, вычислительная техника и информатика. 2024. № 4
ISSN 2072-9502 (Print), ISSN 2224-9761 (Online)
Компьютерное обеспечение и вычислительная техника

Для защиты от перехвата ИУ-1 и ИУ-2 метаданных подключений в ДСО реализован алгоритм обфусцирующей маршрутизации (ОМ), построенный на принципах, применяемых в сети I2P [24]. Взаимодействие АУ с облаком происходит через цепочку случайно выбранных ТУ – маршрутизаторов, которые не выполняют никакой функции в рамках W_m, кроме маскировки реального адреса клиента от ТУ – исполнителя sk_r^m. В цепь маршрутизации всегда входят как минимум 2 маршрутизатора. Для каждого сеанса связи выстраивается уникальная цепь маршрутизации, в которой реальный IP клиента знает только первый маршрутизатор в цепи, а все последующие узлы ДСО никакими сведениями об АУ не обладают, причем ОМ выполняется по id_j (3). Для целей маршрутизации каждому отдельному сеансу генерируется уникальный u_j абонента, а протокол маршрутизации ДСО отображает id_j сеанса как еще один маршрутизатор в цепочке доступа к множеству U идентификаторов, используемых на АУ. Такой подход блокирует перехват со стороны ИУ-1 и затрудняет анализ таблиц маршрутизации со стороны ИУ-2, однако в случае принадлежности ТУ одному владельцу ИУ-2 по-прежнему получает сведения о местоположении и взаимодействиях всех абонентов ДСО.

Именно поэтому считается критически важным реализовать и поддерживать ДАО ДСО в режиме максимальной децентрализации, в первую очередь по владельцам ТУ. Идеальная ситуация – транснациональное облако бесконечно большого количества ТУ, в котором каждый ТУ принадлежит отдельному владельцу. В таком случае вероятность сговора владельцев ТУ стремится к нулю. А за счет географической и транснациональной децентрализации снижаются возможности анализа трафика ДСО со стороны ИУ-1.

Независимо от степени децентрализации ДАО ДСО ИУ-2 могут собирать сведения о деятельности абонентов. Наибольшую опасность представляют ИУ-2, владеющие УМ, т. к. на УМ обрабатываются сведения о W_m: идентификаторах контрагентов, типах заданий (чтение, запись, передача, хранение) и т. п. Анализ этих сведений позволяет выявить идентификаторы абонентов в таблицах маршрутизации, вычислить связи между абонентами, связать результаты вычислений, производимых в открытом виде с конкретными абонентами, что в случае деанонимизации абонента по третьим, не связанным с функционированием ДСО, каналам, может привести к полному раскрытию коммуникаций.

Для предотвращения такой ситуации в ДПС следует использовать алгоритм замены контрагента в смарт-контрактах перед передачей на УМ. В частности, в ДСО этот алгоритм реализуется следующим образом:

1. Со стороны исполнителя генерируется виртуализирующая сущность $\Lambda_c = \{\omega_c, \Omega_c\}$, где $\omega_c = \{id_c, d_c^s, Q_c^s\}$ – идентификатор исполнителя, содержащий его закрытый ключ d_c^s, открытый ключ Q_c^s и идентификатор id_c, он же основной адрес для получения вознаграждений; $\Omega_c = F(\omega_c)$ – множество псевдоадресов начисления вознаграждений, генерируемых для каждого смарт-контракта, принятого ТУ-исполнителем.

2. Со стороны заказчика генерируется аналогичная сущность $\Lambda_z = \{\omega_z, \Omega_z, W_z\}$, $\omega_z = \{id_z, d_z^s, Q_z^s\}$, W_z – множество адресов действующих смарт-контрактов и $\Omega_z = F(\omega_z, W_z)$ – множество псевдоадресов для перечисления вознаграждений.

3. При осуществлении платежей во встроенной платежной системе ДСО для каждого $w_r^z \in W_z$ записывается абстрактное движение средств $\omega_z^m \to \omega_c^m$, $\omega_z^m \in \Omega_z$, $\omega_c^m \in \Omega_c$, при этом выполняется движение $id_z \to id_c$, которое верифицируется только сторонами смарт-контракта и группой из 3 случайно отобранных узлов консенсуса, которые подтверждают правомерность списания с id_z-счета «в никуда» и зачисления на id_c-счет «из ниоткуда». Таким образом, информация о заказчиках и исполнителях вычислительных задач становится недоступной для внешнего анализа.

Для защиты вычислений всех типов используем полностью гомоморфное шифрование (ПГШ), которое позволяет выполнять операции с зашифрованными аргументами и получать зашифрованный результат. В настоящее время на рынке доступны несколько библиотек, реализующих логические, математические и текстовые операции на базе алгоритмов ПГШ. В рассматриваемой ДСО используем реализацию ПГШ ZAMA [25], которая изначально разрабатывалась для применения в ДПС. Несмотря на существенное увеличение вычислительной сложности операций [25], применение ПГШ позволяет исключить перехват результатов вычислений со стороны ИУ-2. Однозначно следует применять ПГШ для закрытия критической информации: вычислений на метаданных, обработки таблиц маршрутизации ОМ и т. п. Перекрытие ПГШ вычислений ПДП возможно по решению абонента. При этом для абонента существенно возрастает стоимость выполняемых вычислений [14, 25].

Информация, размещаемая в ДСО на хранение или передаваемая между абонентами и не требую-

щая дополнительной обработки, передается и хранится в зашифрованном виде. Для шифрования используются криптостойкие алгоритмы [12, 13]. Совместный доступ к данным абоненты осуществляют через передачу ключей доступа [12, 14]. Онлайн-коммуникации между абонентами осуществляются с использованием сеансовых идентификаторов.

Заключение

Таким образом, в ДСО обеспечивается защита конфиденциальности данных и абонентов методами обфускации данных. Перекрывается доступ к данным, алгоритмам и цифровым следам абонентов со стороны ИУ-1 и ИУ-2. Фактически ДСО позволяет исполнять ПДП на уровне безопасности, сравнимом с уровнем безопасности в корпоративных централизованных автоматизированных информационных системах, непосредственно поверх публичных сетей.

Здесь ПДП в ДПС представляют ИСИ в децентрализованном исполнении. Защита пользователей и их данных от угроз, создаваемых провайдерами Интернета, операторами связи и их персоналом, обеспечивается на уровне централизованных ИСИ, однако с существенно меньшими затратами на системы защиты информации [7]. В отличие от централизованных ИСИ и при исполнении ПДП в представленной (либо аналогичной) ДСО, для них решена проблема угроз пользовательской информации, создаваемых владельцами вычислительных ресурсов, владельцами ПДП (ИСИ) и разработчиками ПО.

Владельцы вычислительных ресурсов и владельцы ПДП полностью отстраняются от пользовательских данных в открытом (дешифрованном) виде криптографической подсистемой, обфусцирующей маршрутизацией и алгоритмами запутывания метаданных. Одновременно они сохраняют возможность получать вознаграждение за свою работу.

Угрозы со стороны разработчиков купируются в первую очередь за счет публичности программного кода и процесса имплементации изменений. Заинтересованные участники ДАО могут непосредственно влиять на этот процесс через алгоритмы СУМ, проводя самостоятельную экспертизу программного кода с последующим оповещением сообщества и голосованием за или против изменений. Это позволяет перекрыть угрозу злонамеренного создания «черных ходов» и привлечь значительные ресурсы к выявлению и устранению ошибок, порождающих уязвимости в программном коде. При этом внедрение уязвимостей в программный код ДСО несет угрозу только на АУ. Наличие программных закладок в ТУ не несет угрозы получения злоумышленником пользовательских данных в дешифрованном виде. Все ключи шифрования хранятся строго у пользователей. Однако при поражении уязвимостью значительной части ТУ возможна частичная деанонимизация пользователей. Такая ситуация возможна при низкой степени децентрализации ДСО, когда злоумышленник контролирует значительную часть облака.

Внедрение систем подобного типа при обеспечении максимальной децентрализации позволит существенно снизить издержки обеспечения информационной безопасности и ущерб от инцидентов.

Список источников

1. Nenashev A. V. Secure serverless internet (TheOoL.net) // AIP Conference Proceedings. 2023. V. 2700. P. 070010. DOI: 10.1063/5.0125509.

2. Davidoff S. Data Breaches: Crisis and Opportunity. Boston: Addison-Wesley Professional, 2019. 464 p.

3. Murthy C. V. N. U. B., Shri M. L., Kadry S., Lim S. Blockchain Based Cloud Computing: Architecture and Research Challenges // IEEE Access. 2020. V. 8. P. 205190–205205. DOI: 10.1109/ACCESS.2020.3036812.

4. Schillig M. Some Reflections on the Nature of Decentralized (Autonomous) Organizations // King's College London Law School Research Paper Forthcoming. 2021. DOI: 10.2139/ssrn.3915843.

5. Kaal Wulf A. A Decentralized Autonomous Organization (DAO) of DAOs. 2021. DOI: 10.2139/ssrn.3799320.

6. Lashkari B., Musilek P. A Comprehensive Review of Blockchain Consensus Mechanisms // IEEE Access. 2021. V. 9. P. 43620–43652. DOI: 10.1109/ACCESS.2021.3065880.

7. Nenashev A., Khryashchev V. The Economics of Introducing the Peer-To-peer System of Storage and Processing of Protected Information at an Enterprise // Complex Systems: Control and Modeling Problems: Proceedings 2019 21st International Conference, CSCMP 2019. Samara: Institute of Electrical and Electronics Engineers Inc., 2019. P. 769–772. DOI: 10.1109/CSCMP45713.2019.8976720.

8. Wang Qin, Li Rujia, Wang Qi, Chen Shiping, Ryan Mark, Hardjono Thomas. Exploring Web3 From the View of Blockchain // arXiv. 2022. V. 2206. P. 08821. DOI: 10.48550/ARXIV.2206.08821.

9. Rajput S., Singh A., Khurana S., Bansal T., Shreshtha S. Blockchain Technology and Cryptocurrenices // 2019 Amity International Conference on Artificial Intelligence (AICAI). Dubai, United Arab Emirates, 2019. P. 909–912. DOI: 10.1109/AICAI.2019.8701371.

10. Singhal B., Dhameja G., Panda P. S. How Blockchain Works // Beginning Blockchain. Berkeley, CA: Apress, 2018. P. 31–148. DOI: 10.1007/978-1-4842-3444-0_2.

11. Nenashev A. V., Tolstenko A. Yu., Oleshko R. S. Model of the peer-to-peer distrib-uted system for securable information storage and processing without traffic prioritization (TheOoL project) // III International Workshop on Modeling, Information Processing and Computing (MIP: Computing-2021). Krasnoyarsk: CEUR-WS, 2021. V. 2899. P. 141–150. DOI: 10.47813/dnit-mip3/2021-2899-141-150.

12. Nenashev A. V., Tolstenko A. Y. Video Conferencing Subsystem of the Secure Serverless Internet (TheOoL.Net) // Society 5.0. Springer, Cham., 2023. V. 437.

URL: https://doi.org/10.1007/978-3-031-35875-3_22 (дата обращения: 12.06.2024).

13. Schneier B. Applied Cryptography: Protocols, Algorithms and Source Code in C, 20th Anniversary Edition. New Jersey: John Wiley & Sons, Inc., 2015. 784 p.

14. Nenashev A. V., Oleshko R. S. Mathematical Model of Billing for TheOoL DAO // Hybrid Methods of Modeling and Optimization in Complex Systems: European Proceedings of Computers and Technology. European Publisher, 2023. V. 1. P. 11–18. URL: https://doi.org/10.15405/epct.23021.2 (дата обращения: 12.06.2024).

15. Peltier T. R. Information Security Risk Analysis. Auerbach Publications, 2010. 496 p.

16. Bidgoli H. Handbook of Information Security, Threats, Vulnerabilities, Prevention, Detection, and Management (Handbook of Information Security). Hoboken: Wiley, 2006. V. 3. 1152 p.

17. Kotak J., Habler E., Brodt O., Shabtai A., Elovici Y. Information Security Threats and Working from Home Culture: Taxonomy, Risk Assessment and Solutions // Sensors. 2023. V. 23 (8). P. 4018. DOI: 10.3390/s23084018.

18. Harshavardhan A., Vijayakumar T., Mugunthan S. R. Blockchain Technology in Cloud Computing to Overcome Security Vulnerabilities // 2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC). Palladam, India, 2018. P. 408–414. DOI:10.1109/I-SMAC.2018.8653690.

19. Komisarek M., Pawlicki M., Kozik R., Hołubowicz W., Choraś M. How to Effectively Collect and Process Network Data for Intrusion Detection? // Entropy. 2021. V. 23 (11). P. 1532. DOI: 10.3390/e23111532.

20. Rudikowa L., Myslivec O., Sobolevsky S., Nenko A., Savenkov I. The development of a data collection and analysis system based on social network users' data // Procedia Computer Science. 2019. V. 156. P. 194–203. DOI: 10.1016/j.procs.2019.08.195.

21. Ferguson N., Schroeppel R., Whiting D. A simple algebraic representation of Rijndael // Selected Areas in Cryptography: Proc. SAC 2001, Lecture Notes in Computer Science #2259. Springer Verlag, 2001. P. 103–111.

22. Aweya J. IP Routing Protocols. Fundamentals and Distance-Vector Routing Proto-cols. CRC Press, 2021. 324 p.

23. Belykh A., Tolstoguzov O. Network intelligence as a necessity of the new time. MPRA Paper No. 111528, posted 14 Jan 2022, University Library of Munich, Germany. 2021. URL: https://mpra.ub.uni-muenchen.de/111528/1/MPRA_paper_111528.pdf (дата обращения: 29.05.2024).

24. Hoang N. P., Kintis P., Antonakakis M., Polychronakis M. An Empirical Study of the I2P Anonymity Network and its Censorship Resistance // Proceedings of the Internet Measurement Conference. ACM, 2018. DOI: 10.1145/3278532.3278565.

25. Smart N. P. Practical and Efficient FHE-Based MPC // Cryptography and Coding. IMACC 2023. Lecture Notes in Computer Science. Springer, Cham., 2023. V. 14421. P. 263–283. URL: https://doi.org/10.1007/978-3-031-47818-5_14 (дата обращения: 06.06.2024).

References

1. Nenashev A. V. Secure serverless internet (TheOoL.net). *AIP Conference Proceedings*, 2023, vol. 2700, p. 070010. DOI: 10.1063/5.0125509.

2. Davidoff S. *Data Breaches: Crisis and Opportunity*. Boston, Addison-Wesley Professional, 2019. 464 p.

3. Murthy C. V. N. U. B., Shri M. L., Kadry S., Lim S. Blockchain Based Cloud Computing: Architecture and Research Challenges. *IEEE Access*, 2020, vol. 8, pp. 205190-205205. DOI: 10.1109/ACCESS.2020.3036812.

4. Schillig M. *Some Reflections on the Nature of Decentralized (Autonomous) Organizations*. King's College London Law School Research Paper Forthcoming, 2021. DOI: 10.2139/ssrn.3915843.

5. Kaal Wulf A. *A Decentralized Autonomous Organization (DAO) of DAOs. 2021*. DOI: 10.2139/ssrn.3799320.

6. Lashkari B., Musilek P. A Comprehensive Review of Blockchain Consensus Mechanisms. *IEEE Access*, 2021, vol. 9, pp. 43620-43652. DOI: 10.1109/ACCESS.2021.3065880.

7. Nenashev A., Khryashchev V. The Economics of Introducing the Peer-To-peer System of Storage and Processing of Protected Information at an Enterprise. *Complex Systems: Control and Modeling Problems: Proceedings 2019 21st International Conference, CSCMP 2019.* Samara, Institute of Electrical and Electronics Engineers Inc., 2019. Pp. 769-772. DOI: 10.1109/CSCMP45713.2019.8976720.

8. Wang Qin, Li Rujia, Wang Qi, Chen Shiping, Ryan Mark, Hardjono Thomas. Exploring Web3 From the View of Blockchain. *arXiv*, 2022, vol. 2206, p. 08821. DOI: 10.48550/ARXIV.2206.08821.

9. Rajput S., Singh A., Khurana S., Bansal T., Shreshtha S. Blockchain Technology and Cryptocurrenices. *2019 Amity International Conference on Artificial Intelligence (AICAI).* Dubai, United Arab Emirates, 2019. Pp. 909-912. DOI: 10.1109/AICAI.2019.8701371.

10. Singhal B., Dhameja G., Panda P. S. *How Blockchain Works. Beginning Blockchain*. Berkeley, CA, Apress, 2018. Pp. 31-148. DOI: 10.1007/978-1-4842-3444-0_2.

11. Nenashev A. V., Tolstenko A. Yu., Oleshko R. S. Model of the peer-to-peer distributed system for securable information storage and processing without traffic prioritization (TheOoL project). *III International Workshop on Modeling, Information Processing and Computing (MIP: Computing-2021).* Krasnoyarsk, CEUR-WS, 2021. Vol. 2899. Pp. 141-150. DOI: 10.47813/dnit-mip3/2021-2899-141-150.

12. Nenashev A. V., Tolstenko A. Y. *Video Conferencing Subsystem of the Secure Serverless Internet (TheOoL.Net). Society 5.0.* Springer, Cham., 2023. Vol. 437. Available at: https://doi.org/10.1007/978-3-031-35875-3_22 (accessed: 12.06.2024).

13. Schneier B. *Applied Cryptography: Protocols, Algorithms and Source Code in C, 20th Anniversary Edition.* New Jersey, John Wiley & Sons, Inc., 2015. 784 p.

14. Nenashev A. V., Oleshko R. S. Mathematical Model of Billing for TheOoL DAO. *Hybrid Methods of Modeling and Optimization in Complex Systems: European Proceedings of Computers and Technology*. European Publisher, 2023. Vol. 1. Pp. 11-18. Available at: https://doi.org/10.15405/epct.23021.2 (accessed: 12.06.2024).

15. Peltier T. R. *Information Security Risk Analysis*. Auerbach Publications, 2010. 496 p.

16. Bidgoli H. *Handbook of Information Security, Threats, Vulnerabilities, Prevention, Detection, and Management (Handbook of Information Security).* Hoboken, Wiley, 2006. Vol. 3. 1152 p.

17. Kotak J., Habler E., Brodt O., Shabtai A., Elovici Y. Information Security Threats and Working from Home Culture: Taxonomy, Risk Assessment and Solutions. *Sensors*, 2023, vol. 23 (8), p. 4018. DOI: 10.3390/s23084018.

18. Harshavardhan A., Vijayakumar T., Mugunthan S. R. Blockchain Technology in Cloud Computing to Overcome Security Vulnerabilities. *2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*. Palladam, India, 2018. P. 408-414. DOI: 10.1109/I-SMAC.2018.8653690.

19. Komisarek M., Pawlicki M., Kozik R., Hołubowicz W., Choraś M. How to Effectively Collect and Process Network Data for Intrusion Detection? *Entropy*, 2021, vol. 23 (11), p. 1532. DOI: 10.3390/e23111532.

20. Rudikowa L., Myslivec O., Sobolevsky S., Nenko A., Savenkov I. The development of a data collection and analysis system based on social network users' data. *Procedia Computer Science*, 2019, vol. 156, pp. 194-203. DOI: 10.1016/j.procs.2019.08.195.

21. Ferguson N., Schroeppel R., Whiting D. A simple algebraic representation of Rijndael. *Selected Areas in Cryptography: Proc. SAC 2001, Lecture Notes in Computer Science #2259*. Springer Verlag, 2001. Pp. 103-111.

22. Aweya J. IP Routing Protocols. *Fundamentals and Distance-Vector Routing Protocols*. CRC Press, 2021. 324 p.

23. Belykh A., Tolstoguzov O. *Network intelligence as a necessity of the new time. MPRA Paper No. 111528, posted 14 Jan 2022, University Library of Munich, Germany. 2021*. Available at: https://mpra.ub.uni-muenchen.de/111528/1/MPRA_paper_111528.pdf (accessed: 29.05.2024).

24. Hoang N. P., Kintis P., Antonakakis M., Polychronakis M. An Empirical Study of the I2P Anonymity Network and its Censorship Resistance. *Proceedings of the Internet Measurement Conference*. ACM, 2018. DOI: 10.1145/3278532.3278565.

25. Smart N. P. *Practical and Efficient FHE-Based MPC. Cryptography and Coding. IMACC 2023. Lecture Notes in Computer Science*. Springer, Cham., 2023. Vol. 14421. Pp. 263-283. Available at: https://doi.org/10.1007/978-3-031-47818-5_14 (accessed: 06.06.2024).

Статья поступила в редакцию 06.07.2024; одобрена после рецензирования 08.10.2024; принята к публикации 16.10.2024
The article was submitted 06.07.2024; approved after reviewing 08.10.2024; accepted for publication 16.10.2024

Информация об авторе / Information about the author

Алексей Владимирович Ненашев – доцент кафедры управления и системного анализа теплоэнергетических и социотехнических комплексов; Самарский государственный технический университет; директор; ООО «ТХЕООЛ»; alexvlnenashev@gmail.com

Aleksei V. Nenashev – Assistant Professor of the Department of Control and System Analysis of Thermal Power and Sociotechnical Complexes; Samara State Technical University; Director; THEOOL, LLC; alexvlnenashev@gmail.com