**Известия СПбГЭТУ «ЛЭТИ». 2024. Т. 17, № 2. С. 97–103**
LETI Transactions on Electrical Engineering & Computer Science. 2024. Vol. 17, no. 2. P. 97–103

УДК 20.53.19, 28.23.13 Научная статья

https://doi.org/10.32603/2071-8985-2024-17-2-97-103

# Система мониторинга безопасности технологических операций на основе квантового блокчейна

**Д. Е. Воробьева**

АО «Невское проектно-конструкторское бюро», Санкт-Петербург, Россия

dinvor@mail.ru

**Аннотация.** Системы генерации квантовых ключей обычно рассматриваются только как основа квантовых телекоммуникаций с применением квантовой криптографии. В настоящее время вопросы безопасности техногенной среды существования человека в условиях четвертой промышленной революции реализуются в рамках проекта Сейфнет Национальной технологической инициативы РФ. Одним из основных направлений работ в рамках данного проекта является разработка программно-аппаратного обеспечения на основе использования квантовых ключей и технологии блокчейн. Выполнение тестирования разработок базируется на киберполигоне Сейфнет под эгидой правительства Санкт-Петербурга на площадке ИТЦ «Ингрия». Рассматривается одна из таких разработок – система мониторинга технологической безопасности для АСУ ТП на основе квантового блокчейна.

**Ключевые слова:** квантовые системы мониторинга безопасности, квантовый блокчейн, генерация квантового ключа

**Для цитирования:** Воробьева Д. Е. Система мониторинга безопасности технологических операций на основе квантового блокчейна // Изв. СПбГЭТУ «ЛЭТИ». 2024. Т. 17, № 2. С. 97–103. doi: 10.32603/2071-8985-2024-17-2-97-103.

**Благодарность.** Выражаю признательность заведующему кафедрой «Информационная безопасность» СПбГЭТУ «ЛЭТИ» д-ру техн. наук доценту Воробьеву Е. Г. за помощь в выполнении исследования и за критические замечания в адрес статьи.

Original article

# A Security Monitoring System for Quantum Blockchain-Based Technological Operations

**D. E. Vorobyova**

JSC «Nevskoye Design Bureau», Saint Petersburg, Russia

dinvor@mail.ru

**Abstract.** Quantum key generation systems are usually considered only as the basis of quantum telecommunications using quantum cryptography. Currently, the issues of safety of the techno genic environment of human existence in the conditions of the fourth industrial revolution are being implemented within the framework of the Safenet project of the National Technology Initiative of the Russian Federation. One of the main areas of work within the framework of this project is the development of software and hardware based on the use of quantum keys and block chain technology. Development testing is based on the Safenet cyber polygon under the auspices of the Government of St. Petersburg at the Ingria ETC site. One of such developments – a system for monitoring technological security for ICS based on a quantum block chain is considered.

**Keywords:** quantum security monitoring systems, quantum block chain, quantum key generation

**For citation:** Vorobyova D. E. A Security Monitoring System for Quantum Blockchain-Based Technological Operations // LETI Transactions on Electrical Engineering & Computer Science. 2024. Vol. 17, no. 2. P. 97–103. doi: 10.32603/2071-8985-2024-17-2-97-103.

**Acknowledgements.** The author expresses his gratitude to Dr. E. G. Vorobyev, Head of the Information Security Department of the LETI University (St. Petersburg), Dr. Sci. (Engineering), Associate Professor, for his assistance in the research process and for his critical comments on the manuscript.

**Введение.** Актуальность темы данной статьи обусловлена необходимостью защиты значимых объектов критической информационной инфраструктуры в условиях целенаправленных атак при отсутствии шаблонов безопасности для заранее неизвестных программно-технических воздействий на низкоуровневое промышленное оборудование.

В Россию ежегодно ввозится значительное количество иностранных процессоров, контроллеров и других типов низкоуровневого оборудования, которое используется в промышленном и технологическом оборудовании. При этом из-за отсутствия полноценного описания архитектуры, микропрошивок, системы микрокоманд и т. д. затрудняется или делается полностью невозможной разработка шаблонов безопасности для систем защиты информации, что важно, в частности, при реализации центров реагирования на инциденты информационной безопасности в организациях. Режим информирования при взаимодействии с Государственной системой обнаружения и предупреждения компьютерных атак (ГосСОПКА) в таких условиях становится неэффективным, особенно для атак, заранее неизвестных.

В настоящее время назрел переход от теоретических исследований к нормальной схеме разработки и производства квантовых изделий и сервисов на их основе, к которым относится генерация и распределение квантовых ключей и технологии блокчейн [1]. Распределенный реестр представляет собой почти идеальную систему удаленного контроля любых событий, а квантовые ключи могут рассматриваться как уникальная эталонная характеристика при применении метода эталонных характеристик для построения механизмов защиты.

Для достижения поставленной цели создания системы мониторинга безопасности необходимо решить следующие задачи:

– предложить способ использования системы распределения квантовых ключей – точнее, квантового блокчейна для формирования эталонных характеристик элементов технической системы;

– предложить модель процесса мониторинга;

– оценить возможность применения автоматического информирования ГосСОПКА об опасных отклонениях в работе технологического оборудования.

**Способ использования квантового блокчейна для мониторинга безопасности выполнения операций технологическим оборудованием.** Проведенный анализ безопасности функционирования технологических процессов показывает, что наиболее опасны угрозы подмены отдельных устройств в технологической цепочке и изменение функционирования устройств, выражающееся в изменении выходной информации. В данной статье рассматриваются только компьютерные элементы устройств промышленного оборудования.

Архитектура предлагаемой системы мониторинга на основе квантового блокчейна приведена на рис. 1. Рассмотрим этапы функционирования такой системы.

Система QKD предприятия генерирует уникальные квантовые ключи, но в связи с необходимостью их накапливания в виде файла возникает задача подтверждения их генерирования именно данной системой QKD. Для этого необходимо сформировать уникальную эталонную характеристику (ЭХ) программно-аппаратной среды QKD (например, компьютера, входящего в ее состав). Затем формируется хеш-функция от ЭХ и квантового ключа. Результат помещается в распределенный реестр ведомственного или глобального блокчейна для возможности контроля извне в любой момент времени.

Следующей задачей служит закрепление в блокчейне последовательности подключения устройств в некоей технологической цепочке. Для этого нужно сформировать ЭХ каждого такого устройства, а также хеш-функцию от такой ЭХ и квантового ключа, сгенерированного для данного устройства. Полученные данные в нужной последовательности заносятся в блокчейн для дальнейшего контроля отклонения от правильной последовательности операций и защиты от подмены устройств.


*Рис. 1.* Архитектура системы мониторинга на основе квантового блокчейна
*Fig. 1.* Quantum block chain-based monitoring system architecture

Последней задачей становится контроль правильности выходной информации устройства. Для этого необходимо, как в случае с обучением нейросети, провести правильное выполнение процесса и сформировать хеш-функции от блока выходной информации и квантового ключа устройства. Полученные данные в правильной последовательности заносятся в блокчейн для дальнейшего контроля. Информация о любых отклонениях от нормы должна в реальном масштабе времени под управлением специальной программы поступать в режиме автоматического информирования в ГосСОПКА.

Отличия данной системы от аналогов заключаются в использовании:

– собственной оригинальной блокчейн-платформы ООО «Кьювуд» (РФ) (не копирующей западные аналоги) для создания децентрализованных онлайн-сервисов на базе блокчейна (децентрализованных приложений), работающих на базе умных контрактов. Она реализована как единая децентрализованная виртуальная машина, при этом идеология майнинга заменена на применение квантового аналога удостоверяющего центра, когда формирование квантовых ключей требуется как средство идентификации и аутентификации, а принадлежность ключей данной системе генерации доказывается хешированием эталонной характеристики устройства и самого квантового ключа на основе блокчейн. В результате данные ключи можно использовать с гарантией от подмены;

– разработанных универсальных электронных многофункциональных минитерминалов, имеющих выходы на оптоволокно и стандартные сетевые разъемы, а также запрограммированных на выполнение сервисов квантовой связи, возможность подключения к квантовой системе генерации ключей и формирования смартконтрактов как в международной системе блокчейн [2], так и в собственной.

Данная система не требует никаких знаний о причинах неправильного поведения контролируемой технической системы. Используется шаблон правильного поведения, занесенный в блокчейн.

**Модель системы мониторинга технологической безопасности на основе квантовых блокчейн-технологий.**

*Постановка задачи*. Перспективная система мониторинга, параметры и эксплуатационно-технические параметры (ЭТП) которой описываются вектором $\mathbf{A}'_{k'}$ ведет наблюдение признака $\pi_{\text{м}}(t)$ неправильного поведения процесса $\hat{\Pi}(t)$ (параметры выходного сигнала контролируемого устройства). Признак $\pi_{\text{м}}(t)$ доступен для наблю-

дения периодически в течение интервалов времени $(t'_i, t''_i]$ длительностью, $\tau_i, [i=1(1)\ldots]$ разделенных паузами $(t''_{i-1}, t'_i]$ длительностью $\theta_i, [i=1(1)\ldots]$. Совокупность (объединение) паузы $(t''_{i-1}, t'_i]$ и интервала $(t'_i, t''_i]$ наблюдения, т. е. $(t''_{i-1}, t'_i] \cup (t'_i, t''_i] \cong (t''_{i-1}, t''_i]$, имеет длительность $T_i = \theta_i + \tau_i, [i=1(1)]$ и называется циклом наблюдения [1].

Параметры и ЭТП процесса мониторинга описываются вектором $\mathbf{A}''_{k''}$, характеристики условий проведения операции – векторами $\mathbf{B}'_{l'}$ (условия функционирования) и $\mathbf{B}''_{l''}$ (условия применения сенсорного устройства). Качество результатов операции мониторинга описывается в симплексной канонической форме и характеризуется вектором

$$\hat{\mathbf{Y}}_3 = \hat{y}_1, \hat{y}_2, \hat{y}_3,$$

где $\hat{y}_1$ – целевой эффект; $\hat{y}_2$ – суммарный расход операционных ресурсов различных видов; $\hat{y}_3$ – операционное время.

Для достижения цели операции должен быть получен целевой эффект за время, не превосходящее $\hat{z}_2$. За счет повторных наблюдений признака $\pi_м(t)$ и изменений интенсивности его проявления темп $\dot{y}_2(t)$ освоения вводимых в операцию ресурсов изменяется во времени.

Обнаруженный признак $\pi_м(t)$ идентифицируется с некоторой вероятностью $P_{ид}$.

*Требуется*: построить математическую модель операционной системы мониторинга (ее элементов), позволяющую решать задачи анализа качества сенсора и процесса мониторинга и их синтеза по критериям требуемой или максимальной эффективности операции.

Начнем формализацию операционной ситуации с построения временных диаграмм процессов, протекающих в системе мониторинга, с помощью индикаторов – селекторов временных интервалов, на которых соответствующие процессы протекают.

Введем реализации индикаторов процессов:

$\Pi_п(t)$ – индикатор *процесса проявления* признака $\pi_м(t)$; $\Pi_н(t)$ – индикатор *процесса наблюдения* признака $\pi_м(t)$; $\Pi_р(t)$ – индикатор *процесса результативного функционирования сенсора* в процессе мониторинга; $t_п$ – момент начала проявления признака $\pi_м(t)$; $\pi$ – длительность проявления признака $\pi_м(t)$; $\tau_i$ – длительность $i$-го сеанса наблюдения признака $\pi_м(t)$; $\theta_i$ – длительность $i$-й паузы в наблюдениях; $\nu_i$ – реализованная длительность $i$-го сеанса наблюдения.

Процесс $\hat{\Pi}_н(t)$ наблюдений регулярный, т. е. сеансы наблюдений проводятся через равные интервалы времени $\theta_i, [i=1(1)]$ и имеют одинаковые длительности $\tau_i = \tau_c\ [i=1(1)]$. Далее определяется спецификация операционных эффектов – атрибутов процесса мониторинга. Введем следующие обозначения.

В терминах рассматриваемой задачи темп $\dot{y}_2(t)$ освоения ресурсов определяет интенсивность $\lambda(t)$ наблюдения, т. е. $\dot{y}_2(t) = \alpha\lambda(t)$, $\alpha$ – коэффициент, имеющий размерность расходуемых ресурсов (объема памяти средств наблюдения, объемов носителей информации и т. п.).

Пусть $\varphi_{\hat{\theta}}(\theta)$ – плотность распределения интервала времени $\hat{\theta}$ между последовательными наблюдениями признака $\pi_м(t)$, а $R_{\hat{\theta}}(\theta)$ – дополнительная функция его распределения, тогда

$$\lambda(t) = \frac{\Phi_{\hat{\theta}}(t+0)}{R_{\hat{\theta}}(t)} = \varphi_{\hat{\theta}/\hat{t}}(0;t). \qquad (1)$$

Как видно из (1), интенсивность $\lambda(t)$ наблюдения имеет смысл условной плотности вероятности наблюдения признака в момент $t+0$, т. е. это значение условной плотности распределения момента $\hat{\theta}$ наблюдения признака $\pi_м(t)$ при условии, что он не наблюдался уже в течение времени $t$. Эта функция аналогична интенсивности (опасности) отказа. Если поток событий ординарный, то $\lambda(t)$ численно равна интенсивности (плотности) потока событий (наблюдений).

Из (1) следует

$$\varphi_{\hat{\theta}}(\theta) = \lambda(\theta) e^{-\int_0^\theta \lambda(t)\,dt}, \quad R_{\hat{\theta}}(\theta) = e^{-\int_0^\theta \lambda(t)\,dt}.$$

Интеграл

$$\int_0^\tau \lambda(t)\,dt = \Lambda(t) \qquad (2)$$

называется ведущей функцией потока наблюдений или потенциалом наблюдения и в случае ординарного потока наблюдений численно равен математическому ожиданию числа наблюдений признака $\pi_м(t)$ за время $\tau$.

Поскольку в общем случае при нестационарном потоке наблюдений потенциал наблюдения зависит от момента $t_0$ начала отсчета интервала $(0, \tau]$, более удобна ведущая функция вида

$$\Lambda(t) = \Lambda(\tau, t_0) = \int_{t_0}^{t_{0+\tau}} \lambda(t)\,dt =$$

$$= \int_0^{\tau} \lambda(t_0 + t)\,dt = \Lambda(t_0 + t) - \Lambda(t_0).$$

В дальнейшем будет использоваться форма потенциала наблюдения.

Соотношение (2) определяет вероятность $P(\hat{\theta} > \nu) = R_{\hat{\theta}}(\nu)$ того, что за время $\nu$ признак $\pi_м(t)$ наблюдаться не будет, поэтому вероятность того, что за время $\nu$ он будет наблюдаться, составляет

$$P_н(\nu) = P(\hat{\theta} \le \nu) = 1 - R_{\hat{\theta}}(\nu) =$$

$$= 1 - e^{-\int_0^{\nu} \lambda(t)\,dt} = 1 - e^{-\lambda(\nu)}.$$

Поскольку результаты наблюдения идентифицируются лишь с вероятностью идентификации $P_{ид}$, то вероятность вскрытия (определения) признака $\pi_м(t)$ будет определяться соотношением

$$\upsilon = P_н P_{ид} = P_{ид}\left(1 - e^{-\Lambda(\nu)}\right). \qquad (3)$$

В дальнейшем для простоты будем считать идентификацию идеальной, т. е. $P_{ид} = 1$, а поток наблюдений – стационарным, т. е. $\lambda(t) = \lambda = \text{const}$. Тогда потенциал наблюдения

$$\Lambda(\nu) = \int_0^{\nu} \lambda(t)\,dt = \lambda\nu$$

и (3) примет вид

$$\upsilon = \upsilon(\nu) = 1 - e^{-\lambda\nu}.$$

Вероятность $\upsilon$ представляет собой целевой эффект процесса мониторинга сенсора и имеет смысл доли вскрытых и идентифицированных объектов наблюдения, обладающих признаком $\pi_м(t)$. Полное время наблюдения признака $\pi_м(t)$ определяется равенством

$$\nu = \sum_{i=1}^{m(\tau)} \nu_i,$$

где $m(\tau)$ – число сеансов наблюдения, реализованных за операционное время $(\tau) = \tau(\upsilon)$, т. е. за время набора целевого эффекта не менее $\upsilon$; $\nu_i$ – реализованная длительность $i$-го сеанса наблюдения.

Тогда количество расходуемых в ходе наблюдения ресурсов

$$r(\nu) = y_2(\nu) = \int_0^{\nu} \dot{y}_2(t)\,dt = \alpha \int_0^{\nu} \lambda(t)\,dt = \alpha\lambda\nu,$$

т. е. количество расходуемых в ходе наблюдения ресурсов пропорционально времени $\nu$ наблюдения. При этом функция реальной эффективности имеет выражение

$$\upsilon = \upsilon(r) = 1 - e^{-\lambda\nu} = 1 - e^{-r(\nu)/\alpha}.$$

Таким образом, время $\nu$ наблюдения представляет собой обобщенный показатель расходуемых ресурсов, а суммарная длительность

$$\tau_c = \int_{t_0}^{t_0+\tau} \Pi(t)\,dt$$

сеансов наблюдения на периоде $(t_0,\ t_0 + \tau]$ проведения операции мониторинга характеризует их запас в сенсоре. При этом время $\tau_{li}$, $[i = 1(1)m - 1]$ всех сеансов наблюдения, проведенных на интервале $(t_0,\ t_0 + \tau]$, используется результативно, т. е. $\nu_{li} = \tau_{li}$, $[i = 1(1)m - 1]$ где $m$ – номер сеанса, в котором наблюдение заканчивается (не обязательно в конце $m$-го сеанса).

Итак, из постановки задачи следует, что в ходе наблюдения расходуются все имеющиеся в системе мониторинга сенсора ресурсы $\hat{y}_2 \le \hat{z}_2$, т. е. наблюдается «эффект поглощения». Поскольку при этом $(\hat{y}_2 \le \hat{z}_2) \cong$ ДА то вероятность достижения цели мониторинга

$$P_{д.ц} = P\left[(\hat{\upsilon} \le \hat{\upsilon}_T) \cap (\hat{\tau} \le \hat{\tau}_\partial)\right],$$

т. е. целевой эффект достигается за оперативное время, не выходящее из интервала допустимых значений ($\hat{\tau}_\partial$), и, следовательно, для оценивания эффективности процесса наблюдения модель показателя качества его результатов будет описываться функцией распределения $\Phi_{\hat{\nu},\,\hat{\tau}}(\upsilon, \tau)$ случайного вектора $< \hat{\upsilon}, \hat{\tau} >$.

Поскольку в рамках рассматриваемой задачи все аспекты показателя качества результатов процесса мониторинга выражаются через его временные характеристики, то вначале целесообразно найти закон распределения случайного вектора $<\hat{\upsilon},\hat{\tau}>$, т. е. $\Phi_{\hat{\nu},\hat{\tau}}(\nu,\tau)=P\left[\left(\hat{\nu}\geq\nu\right)\bigcap\left(\hat{\tau}\leq\tau\right)\right]$, а затем перейти к функции распределения $\Phi_{\hat{\upsilon},\hat{\tau}}(\upsilon,\tau)=P\left[\left(\hat{\upsilon}\geq\upsilon\right)\bigcap\left(\hat{\tau}\leq\tau\right)\right]$

Закон распределения запишем в виде

$$\Phi_{\hat{\nu},\hat{\tau}}(\nu,\tau)=P\left[\left(\hat{\nu}\geq\nu\right)\bigcap\left(\hat{\tau}\leq\tau\right)\right]=$$

$$=P\left(\hat{\nu}\geq\nu\right)\bigcap\left(\hat{\tau}\leq\frac{\tau}{\hat{\nu}}\geq\nu\right)=R_{\hat{\nu}}(\nu)F_{\hat{\tau}\perp\hat{\nu}}(\tau;\nu),$$

где $R_{\hat{\nu}}(\nu)$ – дополнительная функция распределения времени $\hat{\nu}$ наблюдения; $F_{\hat{\tau}\perp\hat{\nu}}(\tau;\nu)$ – условная функция распределения операционного времени $\hat{\tau}$ относительно (при условии) события $\left(\hat{\nu}\geq\nu\right)$.

Вероятность $P\left(\hat{\nu}\geq\nu\right)=R_{\hat{\nu}}(\nu)$ обусловлена взаимным расположением на временной оси момента $\hat{t}_{\text{п}}$ начала проявления наблюдаемого признака и моментов $\hat{t}_i$ начала сеансов его наблюдения, а также длительностями $\hat{\nu}_i$ сеансов наблюдения и длительностью $\hat{\pi}$ проявления наблюдаемого признака.

Разработчику системы защиты при анализе модели атак нужно будет определить максимально допустимое время реагирования системы мониторинга, пока указанная атака еще не нанесет неприемлемого ущерба. Оперативность обмена системы мониторинга с ГосСОПКА в режиме информирования определяется нормативными требованиями 8-го Центра ФСБ.

**Оценка применимости предлагаемой системы в практических целях.** На основе приведенных данных заказчику может быть предложена также разработка «под ключ» системы мониторинга технологических процессов предприятия или технической системы, отличием которой служит обеспечение невозможности подмены устройств в технологических цепочках (на основе опознавания на квантовых ключах [3]–[6]), а также подтверждения и отслеживания последовательности операций в процессах (за счет проверки в блокчейне).

Данный подход впервые позволяет автоматизировать контроль работоспособности низкоуровневого сетевого и компьютерного оборудования в автоматизированных и, особенно, в автоматических и роботизированных системах, когда необходимо анализировать команды управления в протоколах M2M, шаблонов для сигнатурного анализа которых просто не существует.

При применении предлагаемого решения в реальном масштабе времени возможна проверка любой операции, пошедшей неправильно, выявление источника опасной команды и неправильно сработавшего устройства, а главное – блокировка выполнения данной злонамеренной или случайной команды. Информация о инциденте может быть автоматически в реальном масштабе времени заведена в систему информирования ГосСОПКА, что позволяет правильно реализовать собственный CERT предприятия. То же самое можно применить и для процессов управления бизнес-процессами верхнего уровня (функциональных отделов) бизнес-процессов предприятия.

Для реализации требуется определить на основе модели актуальных угроз точки, требующие отслеживания, и разместить в них сенсоры и средства реагирования – предлагаемые микротерминалы с программной надстройкой блокчейн (рис. 2).

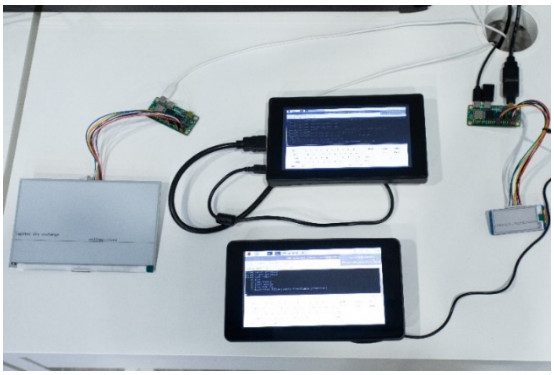

*Рис. 2.* Микротерминалы с программной надстройкой блокчейн
*Fig. 2.* Microterminals with blockchain software add-on

Данная система мониторинга не требует встраивания в действующие программно-аппаратные средства, за исключением самого факта подключения к телекоммуникационным системам.

Возможна разработка программной системы анализа инцидентов на основе полученной от нашей системы мониторинга информации с расчетом последствий каждого нарушения для экономической безопасности предприятия заказчика и включения в бизнес-аналитику.

Моделирование атак на технические системы, применяемые предприятием-заказчиком с установленной предлагаемой системой мониторинга и реагирования, а также проверка корректности встраивания может проводиться на средствах киберполигона ИТЦ «Ингрия» (Санкт-Петербург).

**Заключение.** Разработанная модель системы мониторинга была предложена к реализации в виде программного комплекса, применяемого в электронных коммутационных устройствах, разрабатываемых ООО «Кьювуд» в интересах проекта Сейфнет НТИ РФ и апробирована на площадке киберполигона ИТЦ «Ингрия» (Санкт-Петербург) в 2022 г. Применение предложенной технологии мониторинга позволяет сделать следующий шаг к квантовым системам безопасности, а также к безопасной техногенной среде существования человека.

## Список литературы

1. Буйневич М. В., Олаоде А. Д. Состав и содержание элементов модели оценки устойчивости и безопасности ТКС // Сб. науч. тр. «Актуальные проблемы информационной безопасности». СПб.: СПбГИЭУ, 2012. С. 204–207.

2. Олаоде А. Д. Материалы НКР. СПб.: Изд-во СПбГЭТУ «ЛЭТИ», 2018. 180 с.

3. Малавалли Рагхавендра Сума, Перумал Мадхумати. Оптимальная быстрая генерация и распределение квантовых ключей // Науч.-техн. вестн. информационных технологий, механики и оптики. 2022. Т. 22, № 1. С. 101–113.

4. Pang-Wei Tsai, Chun-Wei Tsai, Chia-Wei Hsu, Chu-Sing Yang. Network Monitoring in Software-Defined Networking: A Rev. // IEEE Systems J. 2018. Vol. 12, no. 4. P. 3958–3969. doi: 10.1109/JSYST.2018.2798060.

5. Schiavon M., Vallone G., Villoresi P. Experimental realization of equiangular three-state quantum key distribution. CNR, Padova, Italy: Padova istituto di fotonica e nanotecnologie, 2021. P. 1–5.

6. Lightweight authentication for quantum key distribution / E. O. Kiktenko, A. O. Malyshev, M. A. Gavreev, A. A. Bozhedarov, N. O. Pozhar, M. N. Anufriev, A. K. Fedorov // IEEE Transaction on Information Theory. 2020. Vol. 66, no. 10. P. 6354–6368. doi: 10.1109/TIT.2020.2989459.

## Информация об авторе

**Воробьева Диана Евгеньевна** – ведущий программист АО «Невское проектно-конструкторское бюро», Галерный проезд, д. 3, Санкт-Петербург,199226, Россия.
E-mail: dinvor@mail.ru

## References

1. Bujnevich M. V., Olaode A. D. Sostav i soderzhanie jelementov modeli ocenki ustojchivosti i bezopasnosti TKS // Sb. nauch. tr. «Aktual'nye problemy informacionnoj bezopasnosti». SPb.: SPbGIJeU, 2012. S. 204–207. (In Russ.).

2. Olaode Ajodele Dzh. Materialy NKR. SPb.: Izdanie SPbGJeTU «LJeTI», 2018. 180 s. (In Russ.).

3. Malavalli Raghavendra Suma, Perumal Madhumati. Optimal'naja bystraja generacija i raspredelenie kvantovyh kljuchej // Nauch.-tehn. vestn. Informacionnyh tehnologij, mehaniki i optiki. 2022. T. 22, № 1. S.101–113. (In Russ.).

4. Pang-Wei Tsai, Chun-Wei Tsai, Chia-Wei Hsu, Chu-Sing Yang. Network Monitoring in Software-Defined Networking: A Rev. // IEEE Systems J. 2018. Vol. 12, no. 4. P. 3958–3969. doi: 10.1109/JSYST.2018.2798060.

5. Schiavon M., Vallone G., P. Villoresi. Experimental realization of equiangular three-state quantum key distribution. CNR, Padova, Italy: Padova istituto di fotonica e nanotecnologie, 2021. P. 1–5.

6. Lightweight authentication for quantum key distribution / E. O. Kiktenko, A. O. Malyshev, M. A. Gavreev, A. A. Bozhedarov, N. O. Pozhar, M. N. Anufriev, A. K. Fedorov // IEEE Transaction on Information Theory. 2020. Vol. 66, no. 10. P. 6354–6368. doi: 10.1109/TIT.2020.2989459.

## Information about the author

**Diana E. Vorobyova** – Leading programmer of JSC «Nevskoye Design Bureau», Galerny Proezd, 3, Saint Petersburg, 199226, Russia.
E-mail: dinvor@mail.ru

Статья поступила в редакцию 15.08.2023; принята к публикации после рецензирования 10.12.2023; опубликована онлайн 26.02.2024.

Submitted 15.08.2023; accepted 10.12.2023; published online 26.02.2024.