УДК 004.056

Виктор С. Горбатов[1], Игорь Ю. Жуков[2], Владислав В. Кравченко[3], Дмитрий И. Правиков[4]
*[1,2]Национальный исследовательский ядерный университет «МИФИ»,*
*Каширское ш., 31, Москва, 115409, Россия*
*[2]АО «РАМЭК-ВС»,*
*5-й Верхний пер., 1, корп. 2, лит. А, Санкт-Петербург, 194292, Россия*
*[2,3,4]РГУ нефти и газа (НИУ) им. И.М. Губкина*
*Ленинский пр-кт, 65, корп. 1, Москва, 119296, Россия*
*[1]e-mail: VSGorbatov@mephi.ru, https://orcid.org/0000-0001-9998-9733*
*[2]e-mail: i.zhukov@inbox.ru, https://orcid.org/0000-0002-4429-8799*
*[3]e-mail: vladislavkravc4enko@yandex.ru, https://orcid.org/0000-0002-5387-5746*
*[4]e-mail: dip@gubkin.pro, https://orcid.org/0000-0001-5217-4537*

# ТЕХНОЛОГИЧЕСКАЯ ПЛАТФОРМА РЕАЛИЗАЦИИ КОНЦЕПЦИИ СЕТИ КИБЕРБЕЗОПАСНОСТИ

*DOI: http://dx.doi.org/10.26583/bit.2023.4.01*

*Аннотация.* Аналитический обзор методов и современных средств противодействия компьютерным атакам на распределенную информационную инфраструктуру показывает, что одним из перспективных решений данной проблемы является практическое воплощение концепции «Cybersecurity Mesh» (сети кибербезопасности»). Она предполагает применение такого подхода, который устранит специфические угрозы, связанные с фактическим «размыванием» физических границ корпоративной информационной системы, путем перехода к точечной защите любого удаленного объекта. Для обеспечения необходимого функционала такого надёжного и безопасного соединения объектов критической информационной инфраструктуры (КИИ) предложено в качестве технологической основы сети кибербезопасности использовать единую облачную платформу, объединяющую нескольких достаточно хорошо известных и уже используемых решений. К ним относятся: мобильная связь стандарта 5G, пограничный сервис безопасного доступа (SASE) и сервис расширенного обнаружения и реагирования (XDR).В данной работе проведен анализ особенностей указанных основных элементов такой платформы применительно к реализации концепции сети кибербезопасности распределенной КИИ в аспекте реализации ее функционала. Рассмотрены вопросы необходимой программной перестройки корпоративного сегмента Интернета в условиях невозможности полного контроля его физической инфраструктуры. Такая задача решается путем создания поверх традиционной Интернет инфраструктуры соответствующего киберуровня, технологически реализуемого на основе трех основных его компонент: киберконтроля, киберузла и узла доверия. Подробно описаны функциональные требования к этим компонентам, а также технологические модульные решения по переходу к точечной защите каждого объекта КИИ. Полученные результаты проведенного исследования могут стать методологической основой для перехода к стадии проектирования конкретной корпоративной сети кибербезопасности после обязательного проведения технико-экономического обоснования на основе анализа рисков, так как практическая реализация анализируемых предложений представляет собой сложный и дорогостоящий процесс, особенно при условии необходимой перестройки существующих систем сетевой безопасности.

*Ключевые слова: кибератака, кибербезопасность, критическая информационная инфраструктура, сеть кибербезопасности, сетевые технологии, технологическая платформа, точечная защита.*

*Для цитирования: ГОРБАТОВ Виктор С. и др. ТЕХНОЛОГИЧЕСКАЯ ПЛАТФОРМА РЕАЛИЗАЦИИ КОНЦЕПЦИИ СЕТИ КИБЕРБЕЗОПАСНОСТИ. Безопасность информационных технологий, [S.l.], т. 30, № 4, с. 25–38, 2023. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2023.4.01.*

Viktor S. Gorbatov[1], Igor Y. Zhukov[2], Vladislav V. Kravchenko[3], Dmitry I. Pravikov[4]
*[1,2]National Nuclear Research University MEPHI (Moscow Engineering Physics Institute),*
*Kashirskoe sh., 31, Moscow, 115409, Russia*

*[2]JSC «RAMEK-VS»,*
*5th upper lane,1, building 2, Litera A, St. Petersburg, 194292, Russia*
*[2,3,4]National University of Oil and Gas «Gubkin University»,*
*Leninsky Ave. 65, building 1, Moscow, 119991, Russia*
*[1]e-mail: VSGorbatov@mephi.ru, https://orcid.org/0000-0001-9998-9733*
*[2]e-mail: i.zhukov@inbox.ru, https://orcid.org/0000-0002-4429-8799*
*[3]e-mail: vladislavkravc4enko@yandex.ru, https://orcid.org/0000-0002-5387-5746*
*[4]e-mail: d_pravikov@mail.ru, https://orcid.org/0000-0001-5217-4537*

# Technological platform for the implementation of the cybersecurity network concept ("Cybersecurity Mesh")

*DOI: http://dx.doi.org/10.26583/bit.2023.4.01*

*Abstract.* An analytical review of methods and modern means of countering computer attacks on distributed information infrastructure shows that one of the promising solutions to this problem is the practical implementation of the concept of "Cybersecurity Mesh" (cybersecurity networks"). It involves the application of such an approach that will eliminate specific threats associated with the actual "blurring" of the physical boundaries of the corporate information system by switching to point protection of any remote object. To provide the necessary functionality for such a reliable and secure connection of critical information infrastructure (CII) objects, it is proposed to use a single cloud platform combining several well-known and already used solutions as the technological basis of a cybersecurity network. These include: 5G standard mobile communications, Secure Access Border Service (SASE) and Advanced Detection and Response Service (XDR). This paper analyzes the features of these main elements of such a platform in relation to the implementation of the concept of a distributed CII cybersecurity network in terms of the implementation of its functionality. Further, the issues of the necessary software restructuring of the corporate segment of the Internet in the conditions of the impossibility of full control of its physical infrastructure are considered. Such a task is solved by creating an appropriate cyber level on top of the traditional Internet infrastructure, technologically implemented on the basis of its three main components: cyber control, cyber node and trust node. Functional requirements for these components are described in detail, as well as technological modular solutions for the transition to point protection of each CII object.
The obtained results of the conducted research can become a methodological basis for the transition to the design stage of a specific corporate cybersecurity network after the mandatory feasibility study based on risk analysis, since the practical implementation of the analyzed proposals is a complex and expensive process, especially if the necessary restructuring of existing network security systems.
*Keywords: cyberattack, cybersecurity, critical information infrastructure, cybersecurity network, network technologies, technology platform, point protection.*
*For citation: GORBATOV Viktor S. et al. Technological platform for the implementation of the cybersecurity network concept ("Cybersecurity Mesh"). IT Security (Russia), [S.l.], v. 30, no. 4, p. 25–38, 2023. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2023.4.01.*

## Введение

Предыдущие результаты анализа перспективного подхода по обеспечению сетевой безопасности, изложенного в концепции «Cybersecurity Mesh» (сеть кибербезопасности) [1], определяют явную актуальность перехода к новой, более гибкой модульной архитектуре безопасности корпоративной критической информационной инфраструктуры (КИИ). По замыслу авторов концепции такой подход позволит обеспечить противодействие специфическим угрозам, связанным с фактическим «размыканием периметра» информационной системы, например, в случае доступа с удаленных объектов КИИ с учетом различного рода ограничений как технического, так и экономического характера. Соответствующая методология технологической реализации указанной концепции подразумевает переход от построения единого защищенного цифрового

периметра всей информационной инфраструктуры к точечной защите ее любого объекта: пользовательских приложений, устройств интернета вещей, киберфизических систем и процессов. Для обеспечения необходимого функционала такого надёжного и безопасного соединения объектов КИИ предложено в [2] в качестве технологической основы сети кибербезопасности использовать единую облачную платформу, объединяющую нескольких достаточно хорошо известных технологий: мобильной связи стандарта 5G, пограничного сервиса безопасного доступа (SASE) и расширенного обнаружения и реагирования (XDR).

В данной работе проведен анализ особенностей основных элементов такой платформы применительно к реализации концепции сети кибербезопасности распределенной КИИ. Кроме этого, рассмотрены вопросы необходимой программной перестройки корпоративного сегмента Интернета в условиях невозможности полного контроля его физической инфраструктуры, а также технологические модульные решения по переходу к точечной защите каждого объекта КИИ.

Полученные результаты проведенного исследования могут стать методологической основой для перехода к стадии проектирования конкретной корпоративной сети кибербезопасности, представляющей собой сложный и дорогостоящий процесс, особенно при условии необходимой перестройки существующих систем сетевой безопасности.

## 1. Основные элементы технологической платформы

Приведем краткий анализ особенностей включения той или иной технологии как составного элемента в единую технологическую платформу сети кибербезопасности.

### 1.1 Мобильная связь стандарта 5G

Важной отличительной особенностью технология мобильной связи пятого поколения является обеспечение мобильности по более надежным протоколам передачи данных, защищенных новейшими алгоритмами шифрования [3–4]. В широко используемых в настоящее время сетях связи стандарта 4G каждому пользователю или устройству присваивается международный идентификатор мобильного абонента (International Mobile Subscriber Identity – IMSI). Этот идентификатор передается с помощью обычного текста, что позволяет атакам типа IMSI – ловушки (IMSI catchers) находить, идентифицировать и отслеживать действия пользователей путем перехвата пакетов данных [5].

Спецификации функционала безопасности стандарта 5G не допускают передачи в открытом виде идентификатора пользователя или устройства. Постоянный идентификатор абонента (Subscription Concealed Identifier – SUPI) не только зашифрован, но и передается с помощью другого уровня шифрования, что гарантирует столь необходимую повышенную конфиденциальность передачи данных.

При этом, с позиций обеспечения сетевой безопасности на основе принципа нулевого доверия все базовые элементы КИИ, включая сети связи стандарта 5G, по-прежнему, должны рассматриваться как ненадёжные. Поэтому доступ должен запрашиваться и предоставляться в каждой конечной точке системы на основе принципа: «никому не доверяй. Аутентифицировать необходимо всех» [5].

### 1.2 Пограничный сервис безопасного доступа

Модель Secure Access Service Edge (SASE) – это возможность объединения пользовательских сетевых сервисов и безопасность инфраструктуры в единую

комплексную услугу[1]. Переход на удалённую модель работы и рост популярности у пользователей облачных сервисов объективно снижают уровень традиционной модели защиты, предполагающей применение общего контура сетевой безопасности. Сервисы SASE «сдвигают» оказание услуги безопасности на уровень пользователей и позволяют практически безгранично масштабировать такую услугу. Все основные преимущества технологии SASE и ее предназначение, например, в концепции Edge computing (подвида распределенных вычислений на уровне пользователей), представлены в [6–7].

Представляется, что данная технология имеет хорошие перспективы развития, хотя современные решения для обеспечения пограничной сетевой безопасности пока не способны обеспечить необходимые уровни скорости, производительности и безопасности в аспекте контроля доступа. То есть на данный момент SASE – качественный, а не количественный этап развития сетевых технологий и соответствующих бизнес-стратегий.

Терминология SASE появилась только в 2019 г., где под термином SASE понимают новый пакет технологий, включающий:

- SD-WAN (Software-Defined Wide Area Network или программно-определяемая распределенная сеть) – класс решений для централизованного управления территориально распределенными сетями (WAN)[2];
- SW (Security Web Gateway, также известные как веб-фильтры – это программно-аппаратные комплексы (ПО + сервер), разработанные и оптимизированные для соблюдения политик веб-безопасности компании и контроля доступа пользователей к веб-сайтам)[3];
- CASB (Cloud Access Security Broker или брокер безопасного доступа в облачных системах – унифицированный инструмент безопасности для выявления потенциальных рисков[4];
- ZTNA (Zero Trust Networks или сетевой доступ с нулевым доверием)[5];
- FWaaS (Firewall-as-a-Service или брандмауэр как услуга)[6].

Совокупность таких технологических решений дает возможность идентифицировать данные, вредоносное ПО, а также способно дешифровать контент на линейной скорости с непрерывным мониторингом сессий на предмет адекватного уровня риска и доверия[1].

Главным отличием SASE от других технологических стратегий является размещение механизмов управления сетевой безопасностью в пограничной с внешней средой зоне. В отличие от большинства традиционных моделей с централизованным управлением безопасностью концепция SASE исключает потребность в сервисах с индивидуальной конфигурацией и управлением. Вместо этого предоставляется стандартизированный набор сетевых сервисов и услуг безопасности с функционалом,

[1]What Is a Secure Access Service Edge (SASE)? URL: https://www.cisco.com/c/en/us/products/security/what-is-sase-secure-access-service-edge.html (дата обращения: 10.07.23).
[2]Что такое SD-WAN и нужен ли он вашей сети? URL: https://www.kaspersky.ru/blog/what-is-sd-wan/34943/ (дата обращения 10.07.2023).
[3] Kaspersky Security для интернет-шлюзов. URL: https://www.kaspersky.ru/small-to-medium-business-security/internet-gateway (дата обращения: 10.07.2023).
[4]What Is a CASB? URL:https://www.cisco.com/c/en/us/products/security/what-is-a-casb.html (дата обращения: 10.07.2023).
[5] What Is a zero trust (ZTNA)? URL: https://www.cisco.com/c/en/us/products/security/zero-trust-network-access.html (дата обращения: 10.07.2023).
[6]Что такое брандмауэр как услуга (FWaaS)? URL: https://www.fortinet.com/resources/cyberglossary/firewall-as-a-service-fwaas (дата обращения: 10.07.2023).

позволяющим создать надёжную и эффективную сетевую архитектуру в зоне объединения сети и облака.

С другой стороны, концепция безопасного доступа Edge или SASE, представляет собой архитектурную модель корпоративной сетевой безопасности, разработанную для поддержки потребностей пользователей в быстром доступе к приложениям и цифровым ресурсам. В этом аспекте архитектуру SASE надо рассматривать как объединение сервисов сетевой и облачной безопасности в высокопроизводительную (эффективную) single-pass (однопроходную архитектуру) с единым управлением.

Single-pass архитектура SASE позволяет одномоментно просматривать и проверять зашифрованный трафик, что уменьшает задержку передачи данных и гарантирует, что сами механизмы проверки и политики не увеличивают эту задержку[7].

Целесообразно сравнить single-pass (однопроходную архитектуру) с multi-pass (многопроходной архитектурой). На рис. 1 по данным[1] показан наихудший случай при multi-pass подходе.

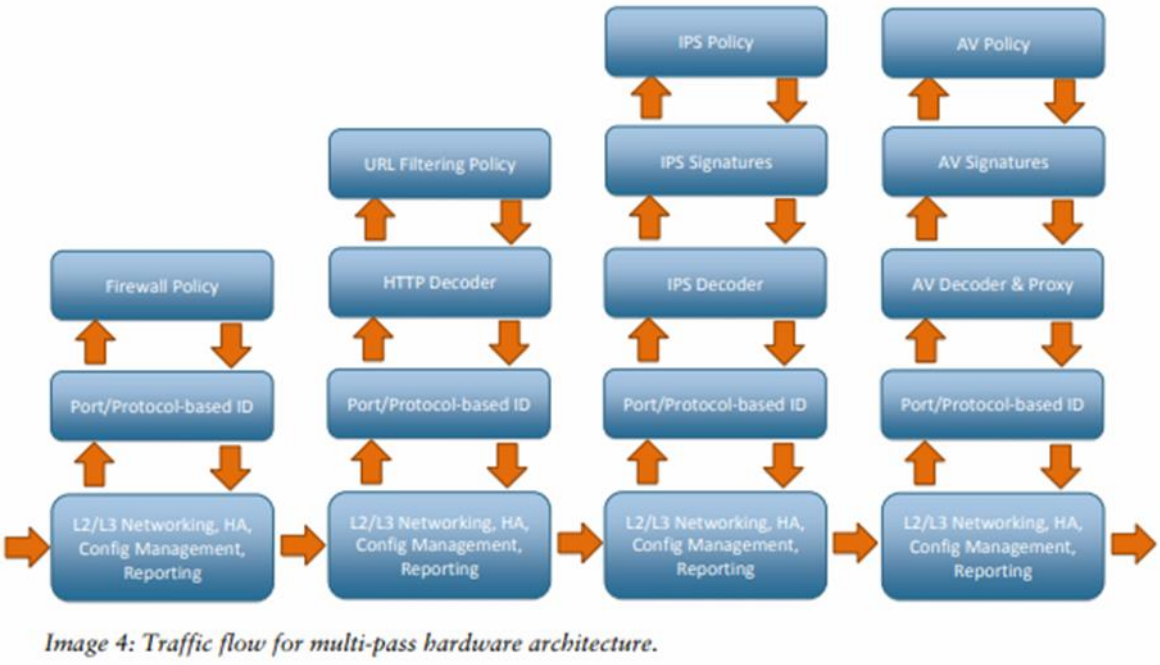


*Рис. 1. Наихудший случай при multi-pass подходе*
*Fig. 1. The worst case with the multi-pass approach*

При этом предполагается, что каждую функцию выполняют отдельные устройства, что приводит к многократным «проходам» через различные элементы сетевого уровня: классификатора трафика, декодеров, механизмов сигнатур и правил парольных политик. Каждый из этих «проходов» создает дополнительную обработку данных, вводит задержку, снижает пропускную способность. Следовательно, увеличиваются эксплуатационные (операционные) расходы.

[7] Single Pass Cloud Engine (SPACE): The Key to Unlocking the True Value of SASE. URL: https://www.catonetworks.com/blog/single-pass-cloud-engine-space-the-key-to-unlocking-the-true-value-of-sase (дата обращения: 10.07.2023).

В итоге подход single-pass архитектуры означает, что одномоментное выполнение всех задач (за один проход) происходит гораздо быстрее, что и определяет ее преимущество в аспекте рентабельности применения.

Таким образом, представляется, что совместное применение технологий 5G и SASE создает довольно перспективную технологическую платформу сетевой безопасности.

В то же время, современные геополитические условия предъявляют еще более повышенные требования к интегрированным инструментам сетевой безопасности КИИ, суть которых состоит в необходимости перманентного решения таких основных вопросов как: уменьшение времени реагирования на угрозы; уменьшение перегруженностью уведомлениями; предотвращение сложных многоэтапных атак.

Перспективным направлением решения этих проблем является достаточно новая технология расширенного обнаружения и реагирования на угрозы сетевой безопасности, обозначаемая в англоязычных публикациях аббревиатурой XDR (Extended Detection and Response).

### 1.3 Расширенное обнаружение и реагирование

Отличительные особенности технологии типа XDR как наиболее перспективного подхода по сравнению с традиционными способами защиты периметра корпоративной сети уже подробно рассмотрены в аналитическом обзоре [1]. Главное преимущество данной технологии – применение элементов технологии искусственного интеллекта (ИИ) таким образом, чтобы не только идентифицировать инциденты, но и проводить их автоматизированную аналитическую обработку. Это позволяет обеспечить наиболее точную и быструю реакцию по управлению инцидентами. С учетом этого аспекта рассматриваемая в данной работе технологическая платформа приобретает дополнительные черты intelligent (разумного, интеллектуального) средства.

Таким образом, рассматриваемая технологическая реализация концепции сети кибербезопасности КИИ на основе объединения решений мобильной связи стандарта 5G, SASE и XDR в единую, масштабируемую и интеллектуальную платформу будет создавать более значительный уровень сетевой защищенности корпоративной КИИ. Это хорошо согласуется с оценочными данными лучших решений по безопасности корпоративных сетей[8] за 2020 г., где, все эти три технологии занимают «передовые» позиции, а такая технология как SASE признается наилучшей.

## 2. Перестройка корпоративного сегмента Интернета

Следующим шагом по технологической реализации функционала сети кибербезопасности [2] является предложение по перестройке программной части корпоративного сегмента Интернет. В традиционной публичной инфраструктуре этой глобальной мировой среды в силу естественного фактора общедоступности возникает проблема обеспечения безопасного удаленного доступа при невозможности ее физического контроля. Обычно она решается, например, с использованием виртуального слоя VPN, что имеет серьезные недостатки, приведенные в [2], на основе публикаций [8–10].

[8] Panetta K. The Top 8 Security and Risk Trends We're Watching. URL: https://www.gartner.com/smarterwithgartner/gartner-top-security-and-risk-trends-for-2021 (дата обращения: 10.12.2022).
[9]Gartner. URL: www.gartner.com (дата обращения: 06.01.2022).
[10]Лаборатория Касперского. URL: www.kaspersky.ru (дата обращения: 06.01.2022).
[11]Издание Anti-Malware.ru. URL: www.anti-malware.ru (дата обращения: 25.03.2022).

Другой подход по технологической реализации концепции Cyber Mesh состоит в создании некоего интеллектуального киберуровня защищенного взаимодействия удаленных объектов КИИ [11] «поверх» общедоступной программно-аппаратной среды (рис. 2, составленный с использованием данных[8,9,10,11] [12]).

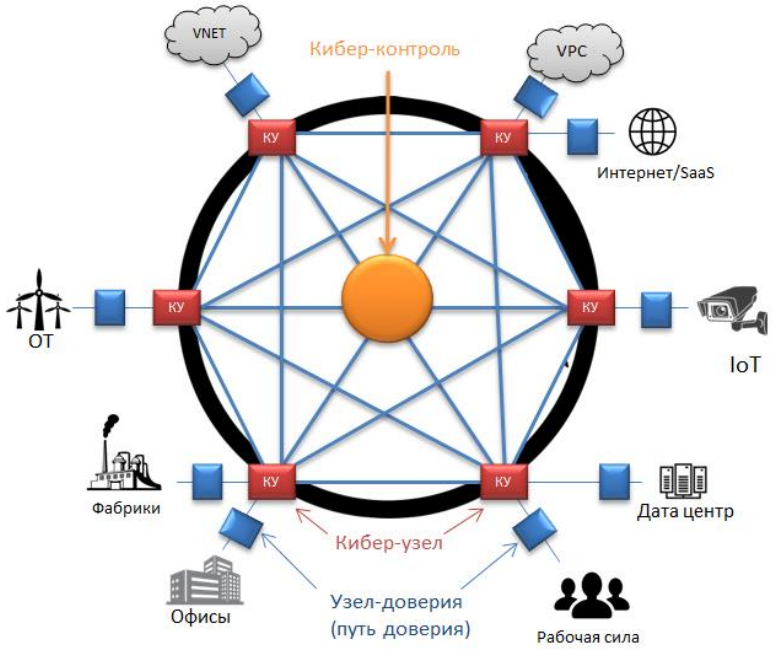


*Рис. 2. Взаимодействие компонентов сети кибербезопасности*
*Fig. 2. Interaction of cybersecurity network components*

Основная идея, закладываемая в создание указанного киберуровня, состоит в том, что обеспечивается передача данных не только по протоколу TCP/IP, но и по любому другому, необходимому для выполнения транзакции. Например, по протоколам интернета вещей или киберфизических устройств. Иными словами, сеть кибербезопасности в этом случае – распределенное архитектурное решение защиты корпоративной информационной среды в отличие от использования традиционной Интернет инфраструктуры.

Перейдем к общему описанию технологических особенностей указанного выше киберуровня, который предлагается реализовать в виде взаимодействующих трёх компонентов (модулей), создающих основу проектирования сети кибербезопасности и условно называемых как киберконтроль, киберузел и узел доверия.

Модуль киберконтроля – принципиально отсутствующий в публичной Интернет инфраструктуре, создается в виртуальной реальности как аналог «мозга» корпоративной сети. Его основной функционал – централизация и согласованность политики безопасности с целью ее принудительного применения (обеспечения) на всех объектах корпоративной КИИ, связанных на основе модулей, называемых киберузлом.

Киберузел в нашем представлении – это модуль с функционалом виртуального маршрутизатора, который обеспечивает реализацию механизмов проверки и контроля. Его отличие от обычных устройств состоит в том, что этому модулю доступны идентификационные данные объекта, подключающегося к корпоративной КИИ. Использование этих данных на основе элементов ИИ данного модуля для определения идентичности субъектов и/или объектов КИИ порождает новое качество, которое можно назвать «интеллектуальной сетевой безопасностью». В концепции сети кибербезопасности предполагается устранение необходимости прохождения всех данных

через дата-центры. Так, например, если пользователь захочет обратиться к Internet/SaaS, то у него должна быть возможность сделать это напрямую. Это достигается размещением киберузлов непосредственно в «точках присутствия» объектов с обязательным контролем их идентичности. То есть весь трафик проверяется и перенаправляется по мере необходимости через базовую публичную Интернет инфраструктуру, но дополненную интеллектуальный уровнем (слоем) сервисов безопасности поверх публичного сегмента. Такой подход в определенной степени снижает задержку доступа к корпоративным цифровым активам независимо от месторасположения объекта КИИ.

Третий компонент программной перестройки – это модуль, названный узлом доверия, который обеспечивает необходимое защищенное взаимодействие всех объектов КИИ. Иными словами – это устройство виртуальной связи, настроенное для использования архитектуры обмена данными с нулевым доверием. Создание узлов доверия также предполагает, что все сообщения и транзакции становятся «невидимыми» в публичном сегменте Интернета, поскольку должно существовать несколько уровней шифрования и контроля качества обслуживания.

На рис. 3, составленном с использованием данных[2,3,8] [12, 13], более подробно представлен технологический состав каждого описанного выше компонента.


*Рис. 3. Основные компоненты киберуровня корпоративной КИИ*
*Fig. 3. The main components of the cyber level of the corporate CII*

## 3. Точечная защита объектов корпоративной КИИ

Перейдем далее к более подробному технологическому описанию киберуровня сети кибербезопасности в аспекте обеспечения практической реализации ее важнейшей особенности, а именно, консолидации точечной защиты любого объекта КИИ цифрового «предприятия» в виде единого облачного сервиса (рис. 4, составленный на основе данных[2,3,8,9,11] [12]).

Как указано выше такая консолидация в основном реализуется двумя компонентами. Первый компонент – киберконтроль, который служит «мозгом» киберуровня, централизующим политику безопасности, а также осуществляющим «оркестрацию» (управление) и распределение принудительного применения указанной политики. Второй – совокупность киберузлов, реализующих инспекционные и «правоприменительные» механизмы контроля и обеспечения соблюдения политик, территориально распределённая в местоположениях объектов корпоративной КИИ (At the Edge).

Контроль удаленного доступа поддерживается модулем сервиса XDR, организованном в виде централизованной службы с целью межуровневого обнаружения и реагирования на компьютерные атаки. Этот модуль собирает и в автоматизированном режиме сопоставляет данные по нескольким контурам безопасности, таким как

пограничные конечные точки, серверные облачные рабочие нагрузки, сама КИИ. Соответственно подобные сервисы также должны быть централизованы, чтобы XDR служба обеспечивала более быстрое обнаружение атак, а аналитика безопасности улучшала расследование и время реагирования на инциденты.

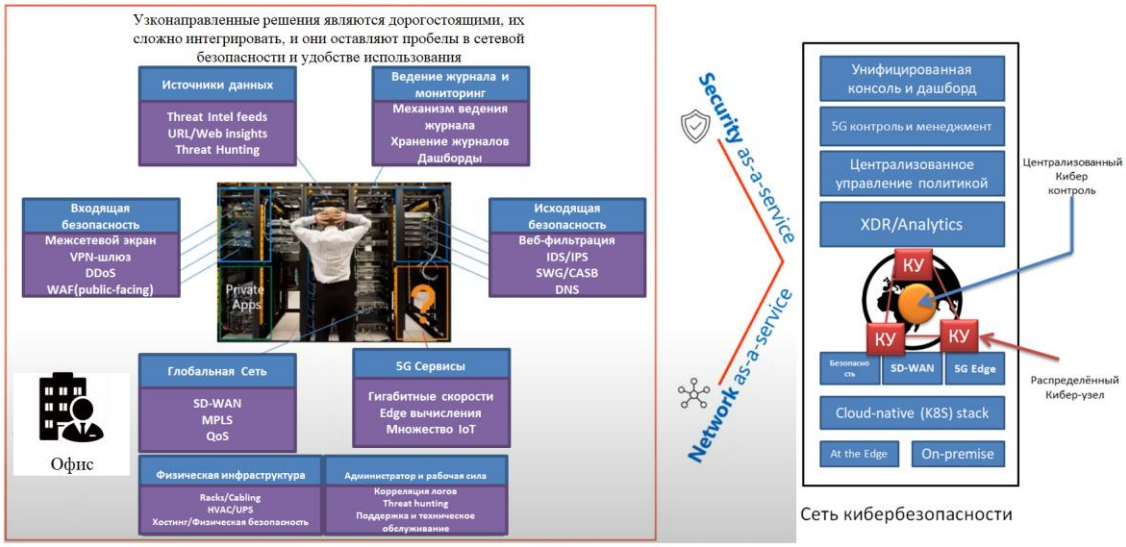


*Рис. 4. Консолидация точечных решений в сети кибербезопасности*
*Fig. 4. Consolidation of point solutions in the cybersecurity network*

С учетом интеграции этих элементов с сервисами связи стандарта 5G реализуется единая облачная служба кибербезопасности в концепции Cyber Mesh, удовлетворяющая потребности современных цифровых «предприятий» в интегрированной платформе безопасного доступа в корпоративное киберпространство.

Как указывалось ранее, в функционале сети кибербезопасности должны быть предоставлены на единой технологической платформе сервисы SASE (службы безопасного доступа Edge), XDR (расширенного обнаружения и реагирования), а также услуги связи стандарта 5G (рис. 5, составленный по данным[2,3,8,9,10] [12]).

Услуги SASE предоставляются в двух видах: первая часть обеспечивает безопасный частный доступ (secure private access), а вторая часть – безопасный доступ в публичную Интернет инфраструктуру (secure internet access). Таким образом, всего будет четыре технологических сервиса, два из которых являются частью SASE, а затем XDR и 5G сервисы.

Модуль киберконтроля, централизующий «оркестрацию» выполнения политики безопасности, технологически реализуется путем объединения консоли и панели мониторинга (console и dashboard), а также XDR службы с элементами ИИ для соответствующей аналитики данных, собираемых с конечных точек присутствия объектов корпоративной КИИ.

Далее рассмотрим технологическую реализацию модуля киберузла, обеспечивающего точечную защиту с нулевым доверием, которая является базовым элементом в новой концепции встроенной сетевой безопасности (network security). Это предполагает включение в данный модуль облачного брандмауэра, а также веб-шлюза (secure Web Gateway) для полного веб-контроля, фильтрации URL-адресов, фильтрации веб-категорий и всех веб-защит. Кроме этого должен быть брокер безопасности облачного

доступа [9] или CASB (cloud access security broker) для управления приложениями. Поскольку основной функционал киберузлов – принудительное исполнение политики безопасности, то они также должны контролировать корпоративный цифровой опыт, такой как действия пользователей, идентификацию активов (ресурсов) и контекст (обстановка). Облачные возможности SD-WAN также предоставляются с киберузлов, поэтому обеспечение таких процессов, как маршрутизация приложений, формирование трафика, управление трафиком, SaaS acceleration[10] (ускорение доставки приложений) – также функционал киберузла. В отличие от централизованного киберконтроля модули киберузлов имеют глобальное территориальное распределение в зависимости от пользовательских потребностей с целью минимизации задержки доступа к корпоративным ресурсам. Поэтому сеть кибербезопасности может быть развёрнута в виде «Bare metal» co-location[11] (колокация) инфраструктуры, чтобы создать как можно больше «точек присутствия» или киберузлов.

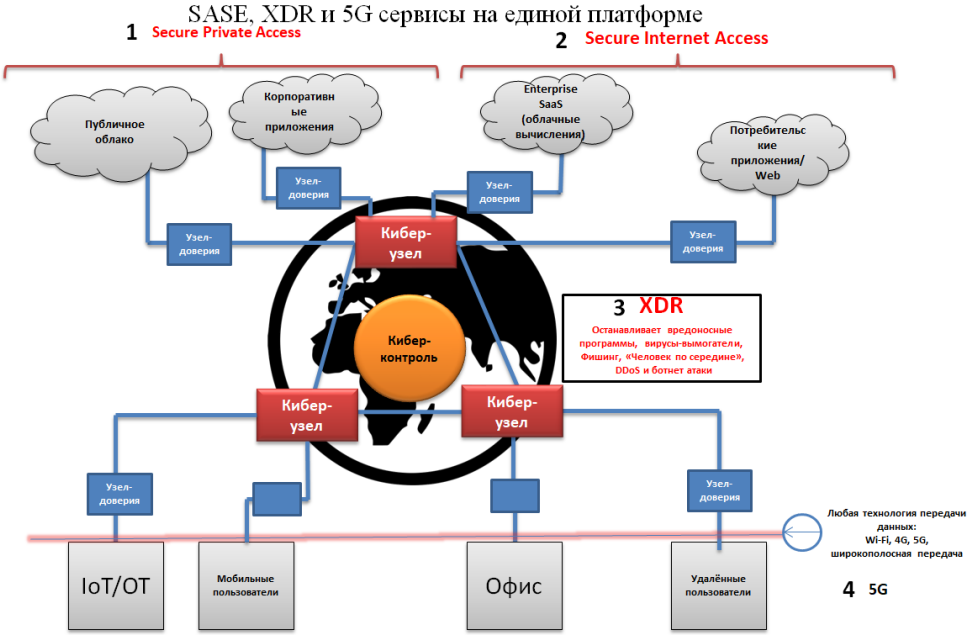


*Рис. 5. Технологическая схема сети кибербезопасности*
*Fig. 5. Technological scheme of the cybersecurity network*

Взаимодействие описанных выше основных компонент киберуровня технологически обеспечивается совокупностью узлов доверия, создаваемой на основе архитектуры с нулевым доверием с обязательной идентификацией объектов корпоративной КИИ. Это предполагает установку соответствующих средств аппаратной защиты, например, устройств с TPM (Trusted Platform Module)[12] модулем, либо защиту на аппаратном и программном уровне с помощью технологии DID[13].

[9] Брокер безопасности облачного доступа. URL: https://rt-solar.ru/products/solar_inrights/blog/3264/ (дата обращения: 14.07.2023).
[10] Акселератор SaaS. URL: https://www.riverbed.com/products/saas-accelerator/ (дата обращения: 14.07.2023).
[11] Bare metal» co-location. URL: https://cloud.google.com/bare-metal/docs/(дата обращения: 14.07.2023).
[12] Основы доверенного платформенного модуля. URL: https://learn.microsoft.com/ru-ru/windows/security/hardware-security/tpm/tpm-fundamentals/ (дата обращения: 14.07.2023).
[13] DID: технология децентрализованной идентификации. URL: https://gagarin.news/ru/news/did-a-decentralized-identifier/(дата обращения: 14.07.2023).

Далее, очевидно, путь доверия должен иметь шифрование на сетевом уровне как меру противодействия множеству атак, например, несанкционированному анализу трафика, удалению файлов. Поэтому нормативным требованием для защиты на сетевом уровне в данном случае является использование протокола IPsec [8, 9, 13, 14], который позволяет осуществлять подтверждение подлинности, проверку целостности и шифрование IP-пакетов. Сетевое шифрование имеет решающее значение для защиты онлайн-деятельности, личных данных и деловой информации, так как методы кибератак, используемые злоумышленниками сложны и развиваются. Поэтому уже недостаточно шифровать только сообщения между серверами. Для полновесной защиты требуются более жёсткие меры, обеспечивающие сквозной многоуровневый путь доверия (рис. 6, составленный по данным[5] [8, 9, 14, 15]), что предполагает использование не одного, а нескольких протоколов шифрования: IPSec; IKE; TLS 1.3; GRE.

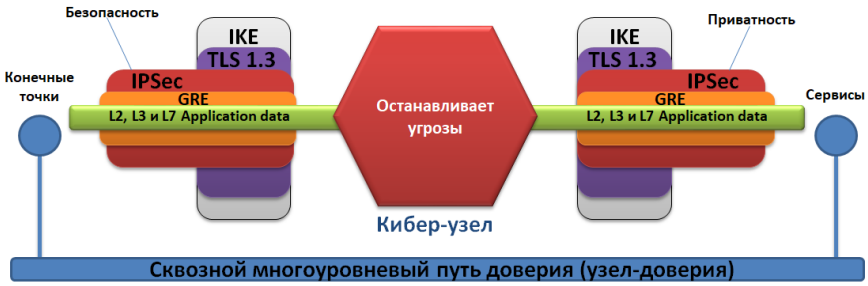


*Рис. 6. Сквозной многоуровневый путь доверия*
*Fig. 6. End-to-end multilevel trust path*

Хотя IPsec – это уже целый набор различных протоколов, которые обеспечивают прозрачную и безопасную защиту данных на сетевом уровне, но его основная сложность состоит в том, что в процессе установления соединения двум участникам защищенного канала необходимо согласовать довольно большое количество различных параметров. В частности, нужно аутентифицировать друг друга, сгенерировать и обменяться ключами, а также договориться, с помощью каких протоколов шифровать данные.

Для упрощения этой процедуры создания защищенного соединения можно использовать IKE (Internet Key Exchange)[14] с помощью которого формируется Psec SA (Security Association – ассоциация безопасности), то есть те самые политики согласования работы участников защищенного соединения. Через этот протокол участники договариваются, какой алгоритм шифрования будет применен, по какому алгоритму будет проводиться проверка целостности и как аутентифицировать друг друга. В 2018 г. был сертифицирован протокол TLS 1.3 [15] [16], предоставляющий шифрование, аутентификацию и целостность соединения.

Завершает процесс логического соединения между двумя конечными точками инкапсуляция различных протоколов туннелирования сетевых пакетов, например, с помощью протокола GRE [15]. Его основное назначение – инкапсуляция пакетов сетевого уровня сетевой модели OSI в IP-пакеты.

Теперь, когда «подняты» туннели GRE, необходимо перейти к настройке сервиса QoS – контроль качества обслуживания, чтобы трафик, предназначенный для передачи через туннели, имел приоритет по отношению к остальному трафику, идущему наружу.

[14]Internet Key Exchange. URL: https://www.techtarget.com/searchsecurity/definition/Internet-Key-Exchange (дата обращения: 14.07.2023).
[15]Why use TLS 1.3? URL: https://www.cloudflare.com/learning/ssl/why-use-tls-1.3 (дата обращения: 14.07.2023).

Это дает гарантию однозначной пересылки определённых пакетов данных незаметно для пользователя. Итак, применяя технологию QoS, пользователь избегает трудностей при скачивании данных, видеозвонках, просмотре видео, документов и так далее [15]. Такая технологическая реализация компонента узел доверия будет соответствовать глобальному стандарту мобильной связи 5G, в соответствии с которым создается целая система качества обслуживания.

## Заключение

Результаты анализа представленных выше модульных решений технологической платформы реализации концепции сети кибербезопасности корпоративной КИИ показывают принципиальную возможность перехода к стадии практического проектирования соответствующей конкретной корпоративной системы, что подтверждается также анализом рынка существующих технических решений, результаты которого выходят за рамки настоящего исследования.

Такая платформа обеспечит выполнение необходимого функционала сети кибербезопасности, в частности за счет двух сервисов: SASSE (secure private access – безопасного частного доступа) и безопасного доступа в Интернет (secure internet access).

Безопасный частный доступ означает, что удалённый объект КИИ имеет возможность защищенного использования частных или корпоративных приложений в публичном облаке, так как необходимое взаимодействие происходит через доверительный путь к ближайшему киберузлу, который, в свою очередь, создает аналогичный путь доверия по отношению к публичному облаку. Важно отметить, что всё это должно основываться на модели с нулевым доверием. Надо отметить, что пользователю нужно иметь только один узел-доверия (доверительный путь) для доступа в сеть кибербезопасности.

Второй набор сервисов сеть кибербезопасности – это безопасный доступ в Интернет, что поддерживается корпоративной SaaS службой. Сопряжение с приложениями SaaS выполняет обфускацию исходного IP-адреса. Поэтому, например, обеспечивается нужный уровень конфиденциальности используемых веб-приложений.

Кроме защиты сетевого уровня с помощью узлов доверия, сеть кибербезопасности предоставляет XDR сервис с элементами ИИ для аналитики, автоматизации и управления политиками безопасности.

Несмотря на определенную перспективность и актуальность технологической реализации концепции корпоративной сети кибербезопасности, надо отметить и соответствующие ограничения по развитию подобных систем кибербезопасности. Как уже указывалось выше, очевидным сдерживающим фактором является сложность и достаточно высокая стоимость практической реализации и эксплуатации сети кибербезопасности, то есть условий достижимости, возможных только для крупных стратегически важных цифровых «предприятий», имеющих необходимые ресурсы для снижения существенных рисков своего функционирования.

Тем не менее, изложенные выше результаты могут быть полезны в качестве методического иллюстративного материала в учебных курсах по подготовке, переподготовки и повышению квалификации специалистов сил обеспечения безопасности КИИ Российской Федерации.

СПИСОК ЛИТЕРАТУРЫ:

1. Горбатов Виктор С. и др. Кибербезопасность сетевого периметра объекта критической информационной инфраструктуры. Безопасность информационных технологий. [S.l.], т. 29, № 4, с. 12–26, 2022. ISSN2074-7136. DOI: http://dx.doi.org/10.26583/bit.2022.4.02. – EDN BHDPHL.

2. Горбатов Виктор С. и др. Функциональность сети кибербезопасности критической информационной инфраструктуры. Безопасность информационных технологий, [S.l.], т. 30, № 1, с. 27–39, 2023. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2023.1.02. – EDN PUBRZL.
3. Root of Trust Definitions and Requirements – Public Release v1.0.1. GlobalPlatform. – March 2017. URL: https://globalplatform.org/specs-library/root-of-trust-definitions-and-requirements-v1-1-gp-req_025/ (дата обращения: 14.07.2023).
4. Морозова К.Д., Сорокин А.С. Сравнительный анализ эффективности функционирования систем мобильной связи 4G и 5G.Телекоммуникации и информационные технологии. 2018, № 2, с. 25–33. – EDN YROGAH.
5. Бельский В.С., Дрынкин А.В., Давыдов С.А. Вопросы обеспечения безопасности абонентов в сетях радиодоступа пятого поколения. International Journal of Open Information Technologies. 2021, № 7, с. 32–54. – EDN RJBNP.
6. Ковтун А.В. Управление доступом к информационным ресурсам предприятий на основе концепции identity access management. Наука и инновации в современном мире. М.: Сборник научных статей. 2018, с. 158–162. – EDN QRXEIX.
7. Pedro Garcia Lopez, Alberto Montresor, Dick Epema, Anwitaman Datta, Teruo Higashino. Edge-centric Computing: Vision and Challenges. ACM SIGCOMM Computer Communication Review. 2015, vol. 45, iss. 5, p. 37–42. DOI: http://dx.doi.org/10.1145/2831347.2831354.
8. Шабаев М.Б., Матыгов М.М. Как работает VPN и обзор лучших VPN провайдеров. Тенденции развития науки и образования. 2020, № 68-1, с. 52–54. DOI: http://dx.doi.org/10.18411/lj-12-2020-41.
9. Аникин Д.В. Защита информации в корпоративной сети с использованием технологии VPN. Банковский бизнес и финансовая экономика: глобальные тренды и перспективы развития. Минск: Материалы VI Международной научно-практической конференции молодых ученых, магистрантов и аспирантов. 2021, с. 21–26. – EDN DBOZDA.
10. Tibbs R.W., & Oakes E. (2005). Firewalls and VPNs: Principles and Practices (Prentice Hall Security Series). URL: https://www.semanticscholar.org/paper/Firewalls-and-VPNs%3A-Principles-and-Practices-HallTibbs-Oakes/b7ad0008ba752d10f0f61f5a29ad3f6376141b12 (дата обращения: 14.07.2023).
11. Харламова Т.Л., Мурашева Т.В. Переход на удаленную форму работы как ответ на вызовы цифровизации. Неделя науки СПбПУ. 2019, с. 55–57. – EDN PCNMBB.
12. Ермакова А.В., Бабенко К.А., Мирошникова Н.Е. Текущее состояние и перспективы развития сети 5G. Телекоммуникации и информационные технологии. 2021, № 1, с. 21–28. – EDN IAAGUU.
13. Коптев Д.С., Шевцов А.Н., Щитов А.Н. Анализ работы протокола защиты сетевого трафика на IP-уровне (IPSec). Наука и современность. 2016, № 3, с. 133–142. – EDN WZWAMD.
14. Tibbs R, Oakes E. Firewalls and VPNs: Principles and Practices (Security). New Jersey: Prentice Hall. 2022, p. 467.
15. Рубашенков А.М., Семёнов Д.А. Протокол GRE. European Science. 2018, № 9, с. 27–29. – EDN VNJBIW.
16. Кулебякин Р.Б., Частухина Л.В., Григоренко В.А. Протоколы безопасности SET, TLS И SSL. Сравнительный анализ. Современные проблемы проектирования, применения и безопасности информационных систем. Материалы XVI Международной научной конференции. 2015, с. 68–82. – EDN GJSPKB.

REFERENCES:

[1] Gorbatov Viktor S. et al. Cybersecurity of the network perimeter of the critical information infrastructure object. IT Security (Russia), [S.l.], v. 29, no. 4, p. 12–26, 2022. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2022.4.02 (in Russian). – EDN BHDPHL.
[2] Gorbatov Viktor S. et al. Functionality of the critical information infrastructure cybersecurity network. IT Security (Russia), [S.l.], v. 30, no. 1, p. 27–39, 2023. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2023.1.02 (in Russian). – EDN PUBRZL.
[3] Root of Trust Definitions and Requirements – Public Release v1.0.1. GlobalPlatform. – March 2017. URL: https://globalplatform.org/specs-library/root-of-trust-definitions-and-requirements-v1-1-gp-req_025/ (accessed: 14.07.2023).
[4] Morozova K.D., Sorokin A.St. Comparative analysis of 4g and 5g mobile communication systems functioning efficiency. Telecommunications and information technology. 2018, no. 2, p. 25–33 (in Russian). – EDN YROGAH.
[5] Belsky V., Drynkin A., Davydov S. A subscriber’s privacy on the 5g radio interface. International Journal of Open Information Technologies. 2021, no. 7, p. 32–54 (in Russian). – EDN RJBNP.

[6] Kovtun A.V. Managing access to information resources of enterprises based on the concept of identity access management. Science and innovation in the modern world. M.: Collection of scientific articles. 2018, p. 158–162 (in Russian). – EDN QRXEIX.
[7] Pedro Garcia Lopez, Alberto Montresor, Dick Epema, Anwitaman Datta, Teruo Higashino. Edge-centric Computing: Vision and Challenges. ACM SIGCOMM Computer Communication Review. 2015, vol. 45, iss. 5, p. 37–42. DOI: http://dx.doi.org/10.1145/2831347.2831354.
[8] Khabaev M.B., Martynov M.M. How VPN works and an overview of the best VPN providers. Trends in the development of science and education. 2020, no. 68-1, p. 52–54. DOI: http://dx.doi.org/10.18411/lj-12-2020-41 (in Russian).
[9] Anikin D.V. Information protection in a corporate network using VPN technology. Banking business and financial economics: global trends and development prospects. Minsk: Materials of the VI International Scientific and Practical Conference of Young Scientists, undergraduates and postgraduates.2021, p. 21–26 (in Russian). – EDN DBOZDA.
[10] Tibbs R.W., & Oakes E. (2005). Firewalls and VPNs: Principles and Practices (Prentice Hall Security Series). URL: https://www.semanticscholar.org/paper/Firewalls-and-VPNs%3A-Principles-and-Practices-HallTibbs-Oakes/b7ad0008ba752d10f0f61f5a29ad3f6376141b12 (accessed: 14.07.2023).
[11] Kharlamova T.L., Murashova T.V. Transition to a remote form of work as a response to the challenges of digitalization. SpbSPU Science Week. 2019, p. 55–57 (in Russian). – EDN PCNMBB.
[12] Ermakova A.V., Babenko K.A., Miroshnikova N.E. The current state and prospects of development of the 5G network. Telecommunications and information technology. 2021, no. 1, p. 21–28 (in Russian). – EDN IAAGUU.
[13] Koptev D.S., Shevtsov A.N., Shields A.N. Analysis of the network traffic protection protocol at the IP level (IPsec). Science and modernity. 2016, no. 3, p. 133–142 (in Russian). – EDN WZWAMD.
[14] Tibbs R, Oakes E. Firewalls and VPNs: Principles and Practices (Security). New Jersey: Prentice Hall. 2022, p. 467.
[15] Rubashenkov A.M., Semenov D.A. GRE Protocol. European Science. 2018, no. 9, p. 27–29 (in Russian). – EDN VNJBIW.
[16] Kulebyakin R.B., Chastukhina L.V., Grigorenko V.A. Security Protocols SET, TLS And SSL. Comparative analysis. Modern problems of design, application and security of information systems. Materials of the XVI International Scientific Conference. 2015, p. 68–82 (in Russian). – EDN GJSPKB.

*Поступила в редакцию – 14 августа 2023 г. Окончательный вариант – 01 октября 2023 г.*
*Received – August 14,2023. The final version – October 01, 2023.*