Виктор С. Горбатов[1], Игорь Ю. Жуков[2], Владислав В. Кравченко[3], Дмитрий И. Правиков[4]
[1,2]Национальный исследовательский ядерный университет «МИФИ»,
Каширское шоссе, 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

ФУНКЦИОНАЛЬНОСТЬ СЕТИ КИБЕРБЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

DOI: http://dx.doi.org/10.26583/bit.2023.1.02

Аннотация. Анализ современных подходов по противодействию компьютерным атакам на критическую информационную инфраструктуру (КИИ), представленную в виде распределенных информационных ресурсов, показывает, что существует объективная необходимость в технологическом развитии данного направления. В этом аспекте наиболее перспективным решением данной проблемы представляется использование концепции «Cybersecurity Mesh» («сети кибербезопасности»), введенное фирмой Gartner без точных указаний практической реализации и возможных технологических решений. В настоящей работе приведены результаты исследования функциональных требований к системам, реализованным в соответствии с указанной выше концепцией, на основе которых в дальнейшем будет задана новая архитектура кибербезопасности КИИ. Подробно рассмотрены предложенные авторами концепции особенности ее применения, на основе которых разработаны требования к функциональной структуре возможных технологических требований, которая состоит из четырех базовых уровней, позволяющих гибко реагировать на возникающие проблемы интеграции и безопасности. К таким уровням относятся: интеллектуальная информационная безопасность и аналитика, распределённая структура идентификации, консолидированная политика и управление состоянием, консолидированная интерактивная информационная панель. Для удовлетворения заданным функциональным требованиям предложена технологическая модель построения сети кибербезопасности в виде органичного объединения трех достаточно разнородных технологий: мобильной связи стандарта 5G, пограничного сервиса безопасного доступа (SASE – Secure Access Service Edge) и расширенного обнаружения и реагирования (XDR) в консолидированную облачную платформу. Результаты исследований функциональности концепции сети кибербезопасности можно рассматривать как методологию обеспечения безопасности КИИ, подразумевающую переход от построения единого защищенного цифрового периметра вокруг всех ее устройств или узлов к точечной защите каждой удаленной точки доступа. Данная публикация может быть полезной специалистам сил обеспечения безопасности объектов КИИ, а также работникам образовательных учреждений при реализации соответствующих программ подготовки, переподготовки и повышения квалификации таких специалистов.

Ключевые слова: кибербезопасность, компьютерные атаки, критическая информационная инфраструктура, сетевые технологии, технологическое развитие, точечная защита, функциональность.

Для цитирования: 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. URL: https://bit.spels.ru/index.php/bit/article/view/1473. DOI: http://dx.doi.org/10.26583/bit.2023.1.02.

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 shosse, 31, Moscow, 115409, Russia
[2]JSC "RAMEK-VS", 5-i Verkhniy per., 1, korp. 2, lit. A., St. Petersburg, 194292, Russia
[2,3,4]National University of Oil and Gas "Gubkin University", Leninsky av. 65, bd. 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

Functionality of the critical information infrastructure cybersecurity network

DOI: http://dx.doi.org/10.26583/bit.2023.1.02

Abstract. The analysis of modern approaches to countering computer attacks on critical information infrastructure (CII), presented in the form of distributed information resources, shows that there is an objective need for technological development of this direction. In this aspect, the most promising solution to this problem seems to be the use of the concept of "Cybersecurity Mesh" (cybersecurity networks), introduced by Gartner without precise instructions on practical implementation and possible technological solutions. This paper presents the results of a study of functional requirements for systems implemented in accordance with the above concept, on the basis of which a new architecture of CII cybersecurity will be set in the future. The features of its application proposed by the authors of the concept are considered in detail, on the basis of which the requirements for the functional structure of possible technological requirements have been developed. It consists of four basic levels that allow you to respond flexibly to emerging integration and security challenges. These levels include: intelligent information security and analytics, distributed identity structure, consolidated policy and state management, consolidated interactive dashboard. To meet the specified functional requirements, a technological model for building a cybersecurity network is proposed in the form of an organic combination of three fairly heterogeneous technologies: 5G mobile communications, Secure Access Edge (SASE – Secure Access Service Edge) and advanced detection and response (XDR) into a consolidated cloud platform. The results of the studies of the functionality of the concept of a cybersecurity network can be considered as a methodology for ensuring the security of CII, implying a transition from building a single secure digital perimeter around all its devices or nodes to point protection of each remote access point. This publication can be useful for experts in the security forces of CII facilities, as well as to employees of educational institutions in the implementation of appropriate training, retraining and advanced training programs for such specialists.
Keywords: cybersecurity, computer attacks, critical information infrastructure, network technologies, technological development, point protection, functionality.
For citation: 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. URL: https://bit.spels.ru/index.php/bit/article/view/1473. DOI: http://dx.doi.org/10.26583/bit.2023.1.02.

Введение

Аналитический обзор [1] существующих подходов по противодействию компьютерным атакам на объекты критической информационной инфраструктуры (КИИ) показывает, что существующие меры противодействия угрозам разрабатывались, в первую очередь, на системы, для которых можно организовать формирование и контроль периметра безопасности (т.н. «замкнутые» системы»). Вместе с тем, одним из значимых факторов, определяющим актуальность поставленной проблемы применительно к объектам КИИ, является низкий уровень адекватной защиты в случае, например, удаленного режима работы сотрудников. В этом случае классическое понятие сетевого периметра «размывается» и требуется использование новых более гибких модульных подходов к

архитектуре безопасности, учитывающих угрозы, связанные с фактическим «размыканием» информационной системы, а также наличием удаленного доступа в условиях различного рода ограничений как технического, так и экономического характера.

В табл. 1, составленной на основании данных [2, 3], приведены проблемы, возникающие при удалённом режиме работы.

Таблица 1. Проблемы безопасности КИИ в формате удалённого режима работы

Для сотрудников (удобства)	Для компаний (проблемы)
Работа удалённо, с доступом к данным и приложениям в любое время и в любом месте.	Возросшая зависимость от сторонних поставщиков услуг и приложений для содействия переходу к удалённой рабочей среде.
Подключение через домашние маршрутизаторы / беспроводные устройства без ограничений, связанных с обеспечением безопасности.	Появление новых угроз и новых механизмов атак на системы, обрабатывающие конфиденциальную информацию.
Использование одного и того же устройства для доступа к личным учетным записям, а также для выполнения корпоративной работы.	Отсутствие возможности контроля событий информационной безопасности для части используемой инфраструктуры.

Указанные проблемы осознаются специалистами подразделений информационной безопасности и, как правило, решаются организационными и техническими мерами. Для их решения разрабатываются политики информационной безопасности (ИБ), создаются регламенты обучения и/или сотрудникам предоставляются аппаратно-программные средства, позволяющие обеспечивать приемлемый уровень безопасности данных.

Тем не менее, классическими угрозами остаются взлом и заражение сетевой инфраструктуры, источники которых проанализированы в [3, 4].

Данные табл. 2, составленной по [2, 5–7], дают общее представление оценки защищенности и мер противодействия угрозам, связанным с переходом на режим удалённой работы.

Анализ распространенных типов векторов кибератак: фишинга, внедрения вредоносного ПО, компрометация паролей, недостатки средств шифрования, неактуализированное ПО, проведен в [2, 8]. Современные информационные системы имеют тенденцию развития в сторону усложнения, с чем связана возможность применения все более изощренных методов для выявления их уязвимостей. Эффективность мер по ограничению такой возможности: внедрение политик нулевого доверия, устранение неоправданной сложности, тестирование на проникновение, сегментация сетевой инфраструктуры, обучение сотрудников рассмотрена в [9, 10]. Такие меры дают хороший эффект в случае сосредоточения бизнес-процессов вокруг корпоративного дата-центра, но не обеспечивают необходимого уровня безопасности и контроля доступа, необходимых современным цифровым средам.

Так цифровая трансформация бизнес-процессов стимулируют развитие и внедрение облачных технологий, например, предоставление по подписке ПО (SaaS). Второй фактор – это упомянутый выше формат дистанционного режима работы сотрудников, получающих удаленный доступ к корпоративным ресурсам, сосредоточенным в дата-центре или в облаке.

Один из возможных подходов по созданию безопасного соединения – технологии настройки VPN от удаленного пользователя к корпоративным приложениям имеет серьезные недостатки, проанализированные в [11–13].

Таблица 2. Оценка защищенности и рекомендации по минимизации последствий

Объект	Угроза	Уровень угрозы	Мера
Рабочее место пользователя	Заражение вирусом	Высокий	Защита антивирусом
Корпоративные данные	Нарушение конфиденциальности	Высокий	Использование DLP (data leak protection, предотвращение утечек данных)
Корпоративные данные	Перехват	Средний	Использование шифрования
Инфраструктура компании (серверы)	Заражение вредоносным ПО	Средний	Контроль трафика пользователей. Авторизованный доступ для пользователей программ. Работа через терминальный доступ
Шлюз доступа и инфраструктура	НСД	Высокий	Аутентификация с использованием двух факторов и более
Пользователь (как объект атаки)	Компрометация путем социальной инженерии	Средний	Информирование, обучение, проведение разъяснительной работы. Использование средств для защиты на уровне почты и открываемых файлов

Использование сетевых протоколов шифрования трафика в случае отсутствия необходимого механизма защиты на сетевом уровне также несет в себе серьезные риски нарушения конфиденциальности [14]. Такой же вывод следует относительно рисков безопасности DNS-серверов.

Отсутствие защиты на сетевом уровне удаленного доступа повышает риски атак типа Man-in-the-Middle [15], распределённого отказа в обслуживании серверов [16], сетевого вторжения [17, 18].

Приведенный выше, даже неполный анализ рисков безопасности при удаленном режиме работы, показывает актуальность технологического развития средств защиты сетевого виртуального периметра, что также подтверждается следующими статистическими данными [5, 19]:

1. *Уязвимости*. За последние два года количество фишинговых инцидентов увеличилось на 600%, а атаки вымогателей происходят каждые 11 с, что отображает реальный уровень рисков современных ИТ-систем.

2. *Атаки нулевого дня*, количество которых в 2021 г. достигло рекордного уровня в 66 дней, что более чем вдвое больше 2020 г.

3. *Стоимость ущерба* только от атак вымогателей оценивается в 6 трлн долл. в год, а стоимость киберпреступных атак растет примерно на 15% в год.

Как указывалось в [1], возможным ответом на проблему повышения уровня сетевой безопасности является разработка масштабной, интегрированной и автоматизированной платформы, названной авторами соответствующей концепции [20] как сеть кибербезопасности (Cybersecurity Mesh). Авторы данной концепции определяют данный механизм доверенной защиты на сетевом уровне как «современный концептуальный подход к архитектуре безопасности, который позволяет распределенному предприятию развёртывать и расширять безопасность там, где это наиболее необходимо».

Развивая указанную идею в направлении ее практической реализации, можно представить такое технологическое решение следующим образом. Невозможность доверенного контроля физической интернет-инфраструктуры не исключает создания виртуальных решений в виде интеллектуального программного слоя или программного киберуровеня, который и назван сетью кибербезопасности, обеспечивающей высокопроизводительный, распределенный и безопасный доступ в любом месте, в любое время (с любого устройства), включая поддержку устройств Интернета вещей (IoT).

В настоящей работе проанализирована требуемая функциональность такого тренда технологического развития, указанного в упомянутой выше концепции сети кибербезопасности. Приведен подробный анализ особенностей предложенного механизма доверенной защиты сетевого уровня КИИ, на основе которого обоснованы требования к функциональной структуре сети кибербезопасности. Техническое воплощение сети кибербезопасности предложено реализовать в виде органичного объединения в единую мощную облачную платформу трех достаточно разнородных технологий: *мобильной связи стандарта 5G, пограничного сервиса безопасного доступа* (SASE – Secure Access Service Edge) и *расширенного обнаружения и реагирования* (XDR – eXtended Detection and Response). Очевидно, что это потребует программной перенастройки архитектуры используемого сегмента Интернета для обеспечения корпоративного безопасного удаленного доступа в условиях невозможности изменения физической инфраструктуры.

1. Функциональные особенности сети кибербезопасности

Идея создания сети кибербезопасности состоит в переходе от традиционных методов защиты классического периметра к обеспечению защищенности всей разнообразной сетевой инфраструктуры (КИИ), охватывающей периферийные вычислительные устройства (edge computing devices), удалённые машины (remote machines) и их пользователей, а также облачные технологии и средства Internet-of-Things (IoT). По мнению авторов концепции [21] CSMA (Cybersecurity Mesh Architecture) указанная платформа должна обеспечивать взаимодействие и координацию между отдельными сервисами за счет реализации более интегрированной политики безопасности. Она должна быть ориентирована на снижение корпоративных рисков за счет увеличения уровня защищенности всех отдельных конечных точек доступа. Для достижения этой цели CSMA должна отвечать следующим функциональным требованиям [5, 21]:

1. Создавать более динамичную среду взаимодействия и интеграции отдельных сервисов сетевой безопасности.
2. По мере роста цифровизации бизнеса решения CSMA должны предлагать более масштабируемые и гибкие меры безопасности.
3. Повышать уровень реагирования на атаки и воздействия дестабилизирующих факторов, улучшать оборонительную стратегию, облегчая взаимодействие между аналитическими и интегрированными инструментами безопасности.
4. Создавать быстро разворачиваемую и удобно поддерживаемую среду, уменьшая до минимума инвестиции в конкретные решения безопасности и освобождая активы для поддержки более важных бизнес операций.

В дополнение к повышению уровня безопасности КИИ можно отметить и другие аспекты содействия платформы сети кибербезопасности основной бизнес деятельности вследствие минимизации инвестиций в безопасность: большего использования сторонних приложений и сервисов, создания новых каналов распространения продуктов и услуг, запуска новых инициатив в дополнение к существующей информационной инфраструктуре. За счет гибкости и масштабируемости CSMA ее использование в

разработке ИТ должно позволить повышение уровня централизованного управления политикой безопасности на основе модульной системы, применяемой к нескольким технологиям одновременно [21].

Новый уровень инфраструктуры кибербезопасности должен также позволить [5, 21] превентивное противодействие будущим угрозам и снижение рисков безопасности за счет выбора сервисов, облегчающих интеграцию, например, подключаемых application programming interfaces (API), который позволяет осуществлять кастомизацию и расширение, такие как extensible analytics (расширяемая аналитика), закрытия уязвимостей и применения комплексного подхода.

В [5, 21] указан и такой фактор привлекательности практического воплощения концепции сети кибербезопасности как уменьшение сложности развертывания корпоративной ИТ-инфраструктуры в условиях взрывных темпах цифровизации, когда традиционные модели безопасности становятся тяжелыми и громоздкими. Применение CSMA должно уменьшить сложность и повысить эффективность проектирования, развертывания и обслуживания ИТ-систем. Они становятся более практичными в отличие от использования сторонних облачных приложений, неконтролируемых распределённых данных и недоверенных устройств, что усложняет традиционные политики и методы безопасности цифровых активов, лежащих за пределами традиционного периметра сети.

Таким образом, ускорение цифровой трансформации и соответствующих инноваций диктует необходимость повышения уровня сетевой кибербезопасности путем унификации средств защиты, охватывающих все конечные точки доступа, и интегрированной политики безопасности применительно ко всем сегментам цифровой среды. Брандмауэры и другие средства сетевого управления сетью должны обеспечивать независимую безопасность определенного сегмента КИИ, не представляющего угрозы для всей инфраструктуры. Сервисы обеспечения кибербезопасности должны доставляться и управляться через облако из единой контрольной точки. За счет централизации управления сокращаются непроизводственные расходы на ИТ-персонал, а также на эксплуатацию рабочих станций, необходимых для управления разрозненными сервисами.

Принятие стратегии сети кибербезопасности имеет явные преимущества в части повышения масштабируемости, совместимости и интероперабельности для новых разработок, меняя подходы к проектированию и построению сетевой инфраструктуры. Для существующих сетей переход на новую стратегию, очевидно, означает дополнительные значительные корректировки инфраструктуры, но с учетом вышеприведенной статистики в случае КИИ выгода может оправдывать необходимые затраты.

2. Функциональная структура сети кибербезопасности

Исходя из описанных выше функциональных особенностей сети кибербезопасности, CSMA должна включать в себя четыре базовых уровня, позволяющих гибко и адаптируемо реагировать на современные проблемы интеграции и безопасности КИИ.

Рассмотрим подробно эти уровни на основе данных [5, 21]:

1. *Интеллектуальная информационная безопасность и аналитика.*

Функционал этого уровня отвечает за сбор, агрегирование и анализ данных об инцидентах из различных сервисов безопасности. На основе этих данных такие решения, как управление информацией и событиями безопасности (SIEM – Security Information and Event Management) и координации и автоматизации процессов реагирования на инциденты (SOAR – Security Orchestration Automation and Response), вызывают соответствующее реагирование по противодействию компьютерным атакам.

Под термином интеллектуальная информационная безопасность и аналитика (Security Intelligence and Analytics) понимается реализация противодействия изощрённым киберугрозам в режиме реального времени, невозможного без использования методов интеллектуального анализа потенциальных угроз (threat intelligence), больших данных (big data) и машинного обучения. Таким образом, и порождаются подобные решения для Security Intelligence and Analytics киберугроз (рис. 1, составленный на основе [21]), воспринимающие, анализирующие действующие против тактик, методов и процедур кибернарушителей [22].

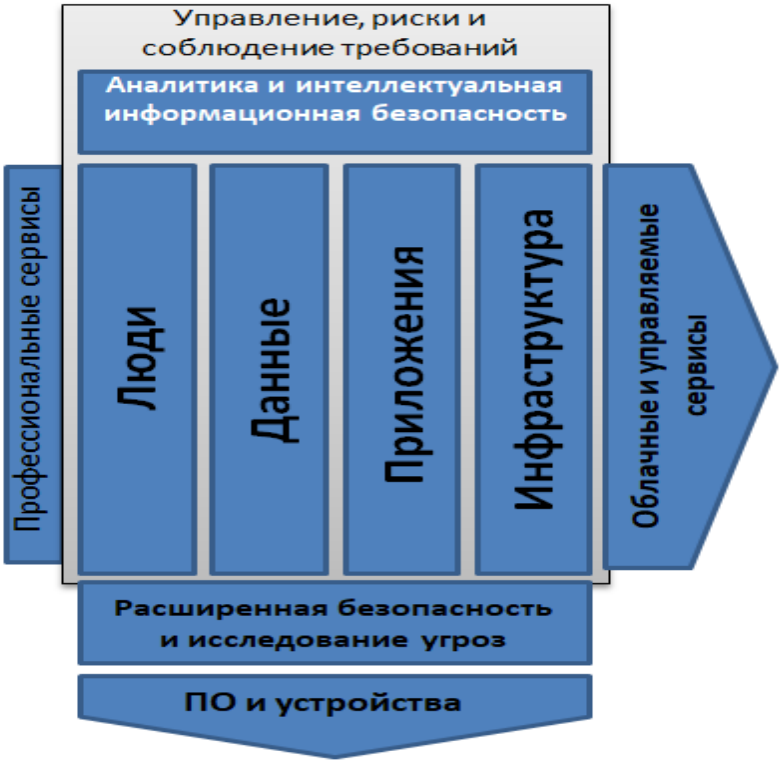

Рис. 1. Структура уровня интеллектуальной информационной безопасности и аналитики
Fig. 1. Structure of the level of intelligent information security and analytics

Таким образом, ставшая модной проблематика искусственного интеллекта органично интегрируется в область обеспечения информационной безопасности через термин «интеллект безопасности» (Security Intelligence), понимаемый как обнаружение и анализ текущих и потенциальных угроз в режиме реального времени.

Основным решением на рынке информационной безопасности в сфере Security Intelligence являются системы SIEM. Главными задачами системы SIEM [23] являются сбор, хранение и агрегация событий безопасности из различных сервисов ИТ-инфраструктуры, нормализация и корреляция данных, выявление угроз и нарушений политик безопасности и ведение отчетности. Но, появились и другие решения, входящие в упомянутые выше системы XDR, что позволяет получить более усовершенствованный уровень интеллектуальной информационной безопасности и аналитики, чем при использовании только одного решения (например, SIEM).

Вместе с тем, архитектура сети кибербезопасности значительно функциональней, чем только XDR, который появился как способ для поставщиков систем безопасности объединения своих продуктов в единую платформу. XDR служит лишь «потенциальной

основой» средств security analytics и intelligence, которые требуются для реализации CSMA с целью повышения эффективности уровня аналитики / интеллекта в сети кибербезопасности. То есть, технологии безопасного пограничного доступа (SASE) и XDR – это лишь составные части интегрированного комплекса сети кибербезопасности, обеспечивающего преимущества, масштабируемость и экономию в среднесрочной перспективе.

2. Распределённая структура идентификации.

На этом уровне фокусируется предоставление служб управления идентификацией и доступом, которые являются центральными в политике безопасности с нулевым доверием. Его функционал должен включать децентрализованное управление идентификацией, службы каталогов, проверку подлинности, управление правами и адаптивный доступ.

3. Консолидированная политика и управление состоянием.

Управление и применение согласованных политик безопасности в различных средах требует перевода политик применительно к их особенностям. Технологические решения на этом уровне преобразуют политики в правила и параметры конфигурации, необходимые для конкретной среды или сервиса, или могут предоставлять службы динамической авторизации во время выполнения. Так, CSMA обеспечивает преобразование единой политики кибербезопасности в собственную конфигурацию каждого сервиса безопасности, гарантируя, что ИТ-команды могут более эффективно выявлять риски несоответствия и проблемы неправильной конфигурации.

4. Консолидированная интерактивная информационная панель.

Массив дискретных и несвязанных традиционных сервисов безопасности усложняет выполнение необходимых операций, заставляя переключаться между несколькими информационными панелями. Этот уровень позволит обеспечивать интегрированную прозрачность всей архитектуры безопасности, позволяя более эффективно обнаруживать, исследовать и реагировать на возникающие инциденты.

Предлагаемая структура сети кибербезопасности в виде четырех базовых уровней, «обрамленных» возможными техническими решениями (подлежит дальнейшему обсуждению), приведена на рис. 2, составленными по данным [20, 21].

В сложившихся геополитических условиях наиболее актуальной проблемой является возможность реализации в России предложенной концепции с использованием программных и аппаратных средств, технологически независимых от зарубежных вендоров. Как представляется, текущий уровень импортозамещения позволяет обеспечить большинство средств, представленных на рис. 2.

Также стоит отметить, что функциональная структура сети кибербезопасности должна удовлетворять требованиям реализации архитектурной концепции нулевого доверия (ZTN – Zero Trust Network), принятой почти два десятилетия назад [10].

Основной принцип архитектуры с нулевым доверием заключается в том, что в этом случае отсутствует предположение о безопасности сетевого доступа к определенному ресурсу. То есть, сеть кибербезопасности должна расширять ZTN от закрытия периметров вокруг локализованных ресурсов до создания периметров вокруг распределенных субъектов и объектов. Адаптивное управление удаленным доступом с тщательным анализом, как субъектов, так и объектов является решающим элементом эффективности ZTN [10].

Для удовлетворения приведенных выше функциональных требований по надёжному и безопасному соединению пользователей, устройств и процессов новым и универсальным способом предлагается технологическое решение сети кибербезопасности в виде единой облачной платформы. Ее вышеприведенные функциональные возможности достигаются за

счет объединения нескольких достаточно разнородных технологий (рис. 3): мобильной связи стандарта 5G, пограничного сервиса безопасного доступа (SASE) и расширенного обнаружения и реагирования (XDR).

Рис. 2. Функциональные уровни CSMA (архитектуры сети кибербезопасности)
Fig. 2. Functional layers of CSMA (Cybersecurity Network Architectures)

Рис. 3. Технологическая основа сети кибербезопасности
Fig. 3. Technological basis of the cybersecurity network

Учитывая сложность реализации предложенной архитектуры сетевой безопасности, данная идея подлежит дальнейшему исследованию и соответствующей публикации.

Заключение

Проведенное аналитическое исследование функциональных особенностей концепции новой архитектуры защиты объектов КИИ, получившей наименование сети кибербезопасности, а также ее функциональной структуры, позволяет перейти к следующему этапу реализации соответствующих технологических решений. Основой таких решений должна стать единая мощная облачная платформа, функциональные возможности которой можно достигнуть за счет объединения нескольких достаточно разнородных технологий: мобильной связи стандарта 5G, пограничного сервиса безопасного доступа (SASE) и расширенного обнаружения и реагирования (XDR).

Изложенные результаты исследования функциональности концепции сети кибербезопасности, по сути, представляют собой методологию защиты объектов КИИ, подразумевающей переход от построения единого цифрового периметра вокруг всех устройств или узлов КИИ к точечной защите каждого объекта.

Представляется, что данная публикация будет полезна специалистам подразделений информационной безопасности территориально распределенных объектов КИИ, а также работникам образовательных учреждений при реализации соответствующих программ подготовки, переподготовки и повышения квалификации таких специалистов.

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. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2022.4.02. – EDN: BHDPHL.
2. Ерышов В.Г., Ерышов Н.В. Анализ угроз информационной безопасности в условиях перехода сотрудников организации на удаленный режим работы. Национальная безопасность России: актуальные аспекты. Сборник избранных статей Всероссийской научно-практической конференции. СПБ.: 2020, с. 17–20. DOI: http://dx.doi.org/10.37539/NB186.2020.88.96.003. – EDN: UAMVTF.
3. Бедняков Н.Д., Хахина А.М. Сетевая безопасность в повседневной жизни. Информационные технологии: прошлое, настоящее, будущее. Сборник статей по материалам межинститутской научно-практической конференции. СПБ.: ФГАОУ ВО «Санкт-Петербургский политехнический университет Петра Великого». 2021, с. 18–23. URL: https://elibrary.ru/item.asp?id=46247186 (дата обращения: 10.12.2022). – EDN: WHDXWR.
4. Вишневский А.С. Обманная система для выявления хакерских атак, основанная на анализе поведения посетителей веб-сайтов. Вопросы кибербезопасности. 2018, №3(27), с. 54–62. DOI: http://dx.doi.org/10.21681/2311-3456-2018-3-54-62.
5. Харламова Т.Л., Мурашева Т.В. Переход на удаленную форму работы как ответ на вызовы цифровизации. Неделя науки СПбПУ. 2019, с. 55–57. URL: https://elibrary.ru/download/elibrary_42437456_25451943.pdf (дата обращения: 10.12.2022). – EDN: AIOCPJ.
6. Глухов Н.И., Наседкин П.Н. Аналитика внутренних угроз информационной безопасности предприятий. Доклады томского государственного университета систем управления и радиоэлектроники. 2021, № 1, с. 33–41. DOI: http://dx.doi.org/10.21293/1818-0442-2021-24-1-33-41.
7. Брюховецкий А.А., Скатков А.В. Адаптивная модель обнаружения вторжений в компьютерных сетях на основе искусственных иммунных систем. Электротехнические и компьютерные системы. 2013, № 12(88), с. 102–111. URL: https://www.elibrary.ru/item.asp?id=21197855 (дата обращения: 10.12.2022). – EDN: RVWRTD.
8. Веревкин С.А., Миклуш В.А. Современное развитие компьютерных вирусов. Информационные технологии и системы: управление, экономика, транспорт, право. 2017, № 3, с. 96–100. URL: https://www.elibrary.ru/item.asp?id=32470433 (дата обращения: 10.12.2022). – EDN: YPMWRG.
9. Петренко С.А., Зотова А.В. Безопасные сетевые технологии нового поколения. Защита информации. Инсайд. 2014, № 2, с. 26–31. URL: https://www.elibrary.ru/item.asp?id=22954663 (дата обращения: 10.12.2022). – EDN: TIIGAN.

10. Кузнецов С.А., Куликов И.А., Фоминых А.А. Модель нулевого доверия применительно к корпоративным информационным системам. Актуальные научные исследования в современном мире. 2021, № 6-1(74), с. 59–62. URL: https://www.elibrary.ru/item.asp?id=46326395 (дата обращения: 10.12.2022). – EDN: TNNNET.
11. 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.
12. 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. URL: https://www.elibrary.ru/item.asp?id=47975667 (дата обращения: 10.12.2022). – EDN: DBOZDA.
13. Tibbs R, Oakes E. Firewalls and VPNs: Principles and Practices (Security). New Jersey: Prentice Hall. 2022, p. 467. URL: https://www.semanticscholar.org/paper/Firewalls-and-VPNs%3A-Principles-and-Practices-Hall-Tibbs-Oakes/b7ad0008ba752d10f0f61f5a29ad3f6376141b12 (дата обращения: 10.12.2022).
14. Анисимов А.В. Обеспечение безопасности DNS. IT-Технологии: развитие и приложения. СПБ.: XV ежегодная международная научно-техническая конференция «IT-Технологии: развитие и приложения». 2018, с. 97–102. URL: https://www.elibrary.ru/item.asp?id=36822147 (дата обращения: 10.12.2022). – EDN: YUQFBJ.
15. Sichkar V.N. IPSEC and SSL as solutions for the enterprise network security. Juvenis Scientia. 2018, no 1, p. 13–15. URL: https://www.elibrary.ru/item.asp?id=32621323 (дата обращения: 10.12.2022). DOI: http://dx.doi.org/10.15643/jscientia.2018.01.004. – EDN: YSMDOK.
16. Саттаров Александр Б., Милославская Наталья Г. Учебно-лабораторный комплекс по изучению атак типа «Человек посередине» и способов защиты от них. Безопасность информационных технологий, [S.l.], т. 25, № 4, с. 63–74, 2018. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2018.4.06. – EDN: YQNKOT.
17. Мамедов Р.А. Анализ применения и последствия массированных атак распределенного отказа в обслуживании на сервер со среднестатистической мощностью. Научно-технический вестник Поволжья. 2014, № 3, с. 150–157. URL: https://www.elibrary.ru/item.asp?id=21743807 (дата обращения: 10.12.2022). – EDN: SHVHYR.
18. Корнев Д.А., Лопин В.Н., Лузгин В.Г. Активные методы обнаружения SYN-flood АТАК. Ученые записки. Электронный научный журнал Курского государственного университета. 2012, № 4–2(24), с. 64–70. URL: https://www.elibrary.ru/item.asp?id=18334638 (дата обращения: 10.12.2022). – EDN: PLFQLV.
19. Зацепина А.С., Боровский А.С. Сравнительный анализ UBA, SIEM, SOAR систем информационной безопасности. Компьютерная интеграция производства и ИПИ-технологии. СПБ.: Сборник материалов IX Всероссийской конференции с международным участием. 2019, с. 206–209. URL: https://www.elibrary.ru/item.asp?id=41380743&pff=1 (дата обращения: 10.12.2022). – EDN: GEVJCM.
20. Русакова О.И., Головань С.А. Анализ кибербезопасности в контексте современных угроз. Иркутский государственный университет путей сообщения. 2022, № 10–2, с. 496–504. URL: https://www.elibrary.ru/item.asp?id=49833097 (дата обращения: 10.12.2022). DOI: https://doi.org/10.25806/uu10-22022496-504. – EDN: NANGAJ.
21. 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).
22. Paul Shread. Cybersecurity Mesh, Decentralized Identity Lead Emerging Security Technology: Gartner. URL: https://www.esecurityplanet.com/networks/cybersecurity-mesh-decentralized-identity-emerging-security-technology/ (дата обращения: 10.12.2022).
23. Милославская Наталья Г., Толстой Александр И. Information Security Intelligence - основа современного управления информационной безопасностью. Безопасность информационных технологий, [S.l.], т. 20, № 4, с. 88–96, 2013. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/307 (дата обращения: 10.12.2022). – EDN: TRMKXX.

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] Eryshov Vadim G., Eryshov Nikita V. Analysis of threats to information security in the context of the transition of employees to remote operation. National security of Russia: actual aspects. Collection of selected articles of

the All-Russian Scientific and Practical Conference. SPB.: 2020, p. 17–20. DOI: http://dx.doi.org/10.37539/NB186.2020.88.96.003 (in Russian). – EDN: UAMVTF.

[3] Bednyakov N.D., Khakhina A.M. Network security in everyday life. Information technologies: past, present, future. Collection of articles on the materials of the inter-institute scientific and practical conference. St. Petersburg: Peter the Great St. Petersburg Polytechnic University. 2021, p. 18–23. URL: https://elibrary.ru/item.asp?id=46247186 (accessed: 10.12.2022) (in Russian). – EDN: WHDXWR.

[4] Vishnevsky A.S. Content based attack detection in web-oriented honeypots. Voprosy kiberbezopasnosti. 2018, no. 3(27), p. 54–62. DOI: http://dx.doi.org/10.21681/2311-3456-2018-3-54-62 (in Russian).

[5] Kharlamova T.L., Murasheva T.V. Transition to remote work as a response to the challenges of digitalization. SPbPU Science Week. 2019, p. 55–57. URL: https://elibrary.ru/download/elibrary_42437456_25451943.pdf. (accessed: 10.12.2022) (in Russian). – EDN: AIOCPJ.

[6] Glukhov N.I., Nasedkin P.N. Analytics of internal threats to the information security of enterprises. Reports of the Tomsk State University of Control Systems and Radioelectronics. 2021, no. 1, p. 33–41. DOI: http://dx.doi.org/10.21293/1818-0442-2021-24-1-33-41 (in Russian).

[7] Bryukhovetskiy A.A., Skatkov A.V. Adaptive model of intrusion detection in computer networks based on artificial immune systems. Electrotechnical and computer systems. 2013, no. 12(88), p. 102–111. URL: https://www.elibrary.ru/item.asp?id=21197855 (accessed: 10.12.2022) (in Russian). – EDN: RVWRTD.

[8] Verevkin S.A., Miklush V.A. The modern development of computer viruses. Information technologies and systems: management, economics, transport, law. 2017, no. 3, p. 96–100. URL: https://www.elibrary.ru/item.asp?id=32470433 (accessed: 10.12.2022) (in Russian). – EDN: YPMWRG.

[9] Petrenko S.A., Zotova A.V. Secure network technologies of a new generation. Information protection. Insider. 2014, no. 2, p. 26–31. URL: https://www.elibrary.ru/item.asp?id=22954663 (accessed: 10.12.2022) (in Russian). – EDN: TIIGAN.

[10] Kuznetsov S.A., Kulikov I.A., Fominykh A.A. Zero trust model for corporate information systems. Actual scientific research in the modern world. 2021, no 6-1(74), p. 59–62. URL: https://www.elibrary.ru/item.asp?id=46326395 (accessed: 10.12.2022) (in Russian). – EDN: TNNNET.

[11] Shabaev M.B., Matygov 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).

[12] Anikin D.V. Information protection in corporate network with use of 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. URL: https://www.elibrary.ru/item.asp?id=47975667 (accessed: 10.12.2022) (in Russian). – EDN: DBOZDA.

[13] Tibbs R, Oakes E. Firewalls and VPNs: Principles and Practices (Security). New Jersey: Prentice Hall. 2022, p. 467. URL: https://www.semanticscholar.org/paper/Firewalls-and-VPNs%3A-Principles-and-Practices-Hall-Tibbs-Oakes/b7ad0008ba752d10f0f61f5a29ad3f6376141b12 (accessed: 10.12.2022).

[14] Anisimov A.V. Securing DNS. IT-Technologies: development and applications. St. Petersburg: XV Annual International Scientific and Technical Conference «IT Technologies: development and applications». 2018, p. 97–102. URL: https://www.elibrary.ru/item.asp?id=36822147 (accessed: 10.12.2022) (in Russian). – EDN: YUQFBJ.

[15] Sichkar V.N. IPSEC and SSL as solutions for the enterprise network security. Juvenis Scientia. 2018, no 1, p. 13–15. URL: https://www.elibrary.ru/item.asp?id=32621323 (accessed: 10.12.2022). DOI: http://dx.doi.org/10.15643/jscientia.2018.01.004. – EDN: YSMDOK.

[16] Sattaro Alexander B., Miloslavskaya Natalia G. Educational and Laboratory System for Studying Man-in-the-Middle Attacks and Ways to Protect against Them. IT Security (Russia), [S.l.], v. 25, no. 4, p. 63–74, 2018. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2018.4.06 (in Russian). – EDN: YQNKOT.

[17] Mammadov R.A. The analysis of applications and implications of massive distributed denial attacks of service to the server with the average power. Scientific and Technical Bulletin of the Volga region. 2014, no.3, p. 150–157. URL: https://www.elibrary.ru/item.asp?id=21743807 (accessed: 10.12.2022) (in Russian). – EDN: SHVHYR.

[18] Kornev D.A., Lopin V.N., Luzgin V.G. Active methods for detecting SYN-flood attacks. Scientific notes. Electronic scientific journal of Kursk State University. 2012, № 4–2(24), p. 64–70. URL: https://www.elibrary.ru/item.asp?id=18334638 (accessed: 10.12.2022) (in Russian). – EDN: PLFQLV.

[19] Zatsepina A.S., Borovsky A.S. Comparative analysis of UBA, SIEM, SOAR information security systems. Computer integration of production and IPI-technologies. St. Petersburg: Collection of materials of the IX All-Russian Conference with international participation. 2019, p. 206–209. URL: https://www.elibrary.ru/item.asp?id=41380743&pff=1 (accessed: 10.12.2022) (in Russian). – EDN: GEVJCM.

[20] Rusakova O.I., Golovan S.A. Analysis of cybersecurity in the context of modern threats. Irkutsk State University of Railways. 2022, no. 10–2, p. 496–504. URL: https://www.elibrary.ru/item.asp?id=49833097 (accessed: 10.12.2022). DOI: https://doi.org/10.25806/uu10-22022496-504 (in Russian). – EDN: NANGAJ.
[21] 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 (accessed: 10.12.2022).
[22] Paul Shread. Cybersecurity Mesh, Decentralized Identity Lead Emerging Security Technology: Gartner. URL: https://www.esecurityplanet.com/networks/cybersecurity-mesh-decentralized-identity-emerging-security-technology/ (accessed: 10.12.2022).
[23] Miloslavskaya, Natalia Georgievna; Tolstoy, Aleksandr Ivanovich. Information security intelligence as a basis for modern information security management. IT Security (Russia), [S.l.], v. 20, no. 4, p. 88–96, 2013. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/307 (accessed: 10.12.2022) (in Russian). – EDN: TRMKXX.

Поступила в редакцию – 14 декабря 2022 г. Окончательный вариант – 01 февраля 2023 г.
Received – December 14,2022. The final version – February 01, 2023.