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: d_pravikov@mail.ru, https://orcid.org/0000-0001-5217-4537

КИБЕРБЕЗОПАСНОСТЬ СЕТЕВОГО ПЕРИМЕТРА ОБЪЕКТА КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

DOI: http://dx.doi.org/10.26583/bit.2022.4.02

Аннотация. Целью настоящей статьи является аналитическое предпроектное исследование возможных технологических аспектов противодействия внешним компьютерным атакам на критическую сетевую инфраструктуру. Это позволит конкретизировать задачи по дальнейшему разрешению этой проблемы в аспекте разработки необходимых программно-технических средств. Практическая реализация таких задач – актуальная и достаточно нетрадиционная проблема в силу различных факторов изменения классического понятия сетевого периметра как физической границы информационной инфраструктуры, который становится виртуальным и, следовательно, требует применения новых подходов к разработке технических решений. На основании статистических данных о количестве и качестве компьютерных инцидентов в работе дано обоснование актуальности поставленной проблемы, приведен обзор широко используемых технических средств по защите классического сетевого периметра, таких как межсетевые экраны и системы обнаружения атак и вторжений. Проведен сравнительный анализ современных технологических трендов их развития, именуемых в публикациях как «Threat Detection and Response», «Extended Detection and Response». Однако, несмотря на мощный программно-аппаратный функционал указанных решений, указан их общий недостаток – отсутствие адекватного противодействия компьютерным атакам при удалённом формате работы пользователей. В связи с этим, подробно изложена новейшая концепция защиты виртуального сетевого периметра, названная авторами как «Cybersecurity Mesh» («сеть кибербезопасности»). Именно эта методология представляется наиболее перспективной с целью разработки соответствующих технологических решений обеспечения кибербезопасности периметра критической информационной инфраструктуры. Данная публикация может быть полезной специалистам сил обеспечения безопасности объектов критической информационной инфраструктуры, а также работникам образовательных учреждений при реализации соответствующих программ подготовки, переподготовки и повышения квалификации таких специалистов.

Ключевые слова: кибербезопасность, компьютерные атаки, критическая информационная инфраструктура, объект, сетевой периметр, технологические решения.
Для цитирования: 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. URL: https://bit.spels.ru/index.php/bit/article/view/1451. DOI: http://dx.doi.org/10.26583/bit.2022.4.02.

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

Cybersecurity of the network perimeter of the critical information infrastructure object

DOI: http://dx.doi.org/10.26583/bit.2022.4.02

Abstract. The purpose of this paper is an analytical pre-project study of possible technological aspects of countering external computer attacks on critical network infrastructure. This will make it possible to specify the tasks for further resolving this problem in the aspect of developing the necessary software and hardware. The practical implementation of such tasks is an urgent and rather unconventional problem due to various factors of change in the classical concept of the network perimeter as a physical boundary of the information infrastructure, which becomes virtual and, therefore, requires the use of new approaches to the development of technical solutions. Based on statistical data on the number and quality of computer incidents, the study provides a justification for the relevance of the above problem, and gives an overview of widely used technical means for protecting the classic network perimeter, such as firewalls and systems for detecting attacks and intrusions. A comparative analysis of modern technological trends in their development, referred to in publications as «Threat Detection and Response», «Extended Detection and Response», is carried out. However, despite the powerful software and hardware functionality of these solutions, their common drawback is indicated as the lack of adequate counteraction to computer attacks with a remote mode of the user work. In this regard, the latest concept of virtual network perimeter protection, referred to by the authors as «Cybersecurity Mesh» («cybersecurity network»), is detailed. It is this methodology that seems to be the most promising for the development of appropriate technological solutions to ensure the cybersecurity of the perimeter of the critical information infrastructure. The paper might be useful to specialists working on the security of critical information infrastructure facilities, as well as to employees of educational classes in the implementation of appropriate training, retraining and advanced training programs for such specialists.

Keywords: cybersecurity, computer attacks, critical information infrastructure, object, network perimeter, technological solutions.
For citation: GORBATOV, Viktor S. et al. Cybersecurity of the network perimeter of the critical information infrastructure object. IT Security (Russia), [S.l.], v. 29, n. 4, 2022. p. 12–26, 2022. ISSN 2074-7136. URL: https://bit.spels.ru/index.php/bit/article/view/1451. DOI: http://dx.doi.org/10.26583/bit.2022.4.02.

Введение

Развитие информационных технологий в соответствии с известным философским законом единства и борьбы противоположностей порождает проблему обеспечения их безопасности, меняя модельные представления о методах и способах противодействия деструктивным воздействиям. В настоящее время приоритетной государственной задачей в области информационной безопасности наряду с защитой информации, выраженной в парадигме сохранения ее доступности, целостности и конфиденциальности [1], является обеспечение устойчивости функционирования критически важных предприятий производственной и/или социальной сферы[1]. Законодательно[2] эта задача выражается как обеспечение безопасности объектов критической информационной инфраструктуры

[1] Доктрина информационной безопасности Российской Федерации, утверждена Указом Президента Российской Федерации 5 декабря 2016, № 646. – 16 с. URL: http://www.kremlin.ru/acts/bank/41460 (дата обращения: 25.08.2022).

[2] Федеральный закон от 26.07.2017, № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». URL: http://pravo.gov.ru/ (дата обращения: 25.08.2022).

(КИИ). К ним, в частности, относятся АСУ ТП топливно-энергетического комплекса [2]. В терминах настоящей статьи практическая реализация такой задачи сводится к обеспечению кибербезопасности КИИ как противодействию компьютерным атакам не только на информационные ресурсы, но и в целом на процессы управления критическими процессами жизнедеятельности [3, 4].

Об актуальности поставленной проблемы свидетельствует нижеприведенная статистика по публикациям количества и качества компьютерных инцидентов. Так, по данным[3] только за первые шесть месяцев 2021 г. количество кибератак на отечественную критическую инфраструктуру выросло на 150%, причем наибольшее число атак было зафиксировано в сферах промышленности, науки и образования, что составляет около 30% от всех зафиксированных случаев.

В других обзорах [4] сообщается, что только 40% всех атак на российскую критическую инфраструктуру были совершенны обычными «классическими» нарушителями, а 60% были совершены хакерами, поддерживаемыми проправительственными структурами, причем их целью является не финансовой шантаж, а именно нарушение устойчивости функционирования компаний и предприятий.

По известным геополитическим причинам в 2022 г., по первым оценкам компаний, ситуация только ухудшилась. Так, компания StormWall, которая занимается защитой от DDoS-атак, заявила[5], что с началом открытого военного противостояния кибератакам подверглись такие ведущие компании России топливно-энергетического и других секторов как «Лукойл», «Газпром», «Норникель». Многие компании сообщают, что атаки реализуются чаще всего из стран Евросоюза – 46,7% совершенных кибератак, а также из США – 28,9%. Постоянно публикуются списки расположенных в России компаний с призывами к дальнейшему их взлому[5].

Проблема обеспечения кибербезопасности объектов КИИ нефтегазового сектора усугубляется естественными технологическими новациями систем управления АСУ ТП, связанными, в частности, с применением систем дистанционного управления [5]. Это приводит к появлению очевидных особенностей так называемой промышленной кибербезопасности [6], основным фактором которой стало «размытие» физических границ периметра объекта защиты. Кроме того, следствием одного из ощутимых и фактически необратимых последствий «ковидных» ограничений стало применение формата удалённой работы сотрудников, в том числе промышленных компаний в нефтегазовой сфере, где кибератаки на этот сегмент превосходят другие отрасли (особенно со стороны проправительственных хакеров).

Таким образом, возникает актуальная технологическая задача скорейшей трансформации методов и подходов по защите сетевого периметра [7–12] объектов КИИ вследствие его «размытия» по технологическим и/или социальным факторам.

Настоящая работа посвящена результатам аналитического обзора возможных решений поставленной задачи с целью выбора наиболее перспективного подхода, который можно использовать для его дальнейшей практической реализации, а также в учебных целях по образовательным программам подготовки, переподготовки и повышению квалификации работников сил обеспечения безопасности объектов КИИ.

[3]Научно-технический центр ФГУП «ГРЧЦ». URL: rdc.grfc.ru (дата обращения: 06.01.2022).
[4]Group-IB. URL: www.group-ib.ru (дата обращения: 25.01.2022).
[5]StormWall. URL: www.stormwall.pro (дата обращения: 26.04.2022).

1. Технологии защиты сетевого периметра

В настоящее время выделяют четыре основных класса средств защиты сетевого периметра, использующие методы и средства распознавания атак по анализу трафика[6]:

– обнаружения атак (СОА, IDS – Intrusion Detection System) и обнаружения вторжений (СОВ, IPS – Intrusion Prevention System);

– межсетевые экраны нового поколения (NGFW – Next Generation Firewall);

– универсальный шлюз (UTM – Unified Threat Management);

– системы обнаружения и реагирования (EDR – Endpoint Detection & Response, NDR – Network Detection & Response, MDR – Managed Detection&Response, EDR – Extended Detection&Response).

В настоящее время системы СОА и СОВ практически не используют по-отдельности. Их особенности заключаются в реакции системы на инцидент: СОА только сообщает о факте обнаружения атаки, в то время как СОВ может разрывать соединение при том же обнаружении [13].

В целях решения поставленной выше задачи и для удобства сравнения в данной работе ограничимся только рассмотрением сетевых средств защиты периметра, которые также отличаются по схеме установки в информационную инфраструктуру организации. Так СОВ устанавливается на пути прохождения трафика, а СОА взаимодействует только с копией трафика, который следует через сетевое оборудование, виртуальные машины или через оптический ответвитель [13, 14].

Обычно совокупность СОА/СОВ ставят на периметре после межсетевого экрана для того, чтобы устранить внешние вторжения. СОВ раскрывают шифрованный трафик и действует по схеме «человек посередине» (man-in-the-middle) [14]. Схема отличий работы СОА и СОВ представлена на рис. 1.

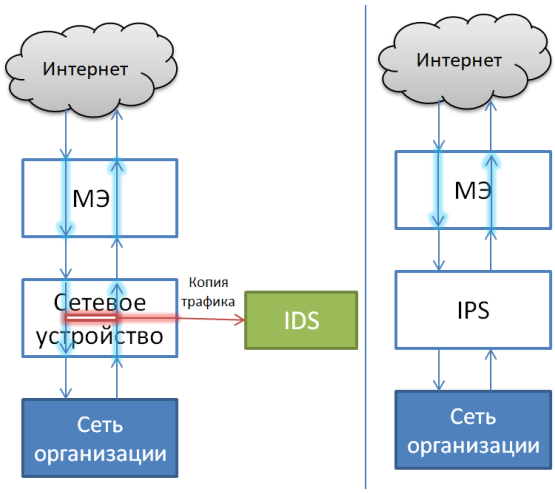

Рис. 1. Схема работы IDS и IPS
Fig. 1. Scheme of IDS and IPS

Так как на практике СОА по отдельности не используются, то системы защиты функционируют либо как IDPS-Intrusion Detection and Prevention Systems, либо как решения с открытыми движками, либо как решение для анализа сетевого трафика.

Для СОВ наиболее популярным является комплексный подход, при котором происходит его внедрение в межсетевой экран NGFW или шлюз UTM[6]. Данные решения

[6]Securitylab. URL: www.securitylab.ru (дата обращения: 06.01.2022).

очень похожи, они являются составными и включают в себя[6] следующие элементы: СОВ; межсетевой экран; антивирусное средство; VPN приложение; веб фильтрацию; антиспам; защиту от утечек (DLP-Data Leak Prevention).

Основным различием этих устройств является их внутренняя архитектура. В NGFW для всех функций предоставляется свой процессор, в то время как у UTM решения используется один единственный. Таким образом, у NGFW есть определенное преимущество в виде параллельности процессов, что повышает производительность системы[6]. Эти отличия отображены на рис. 2.

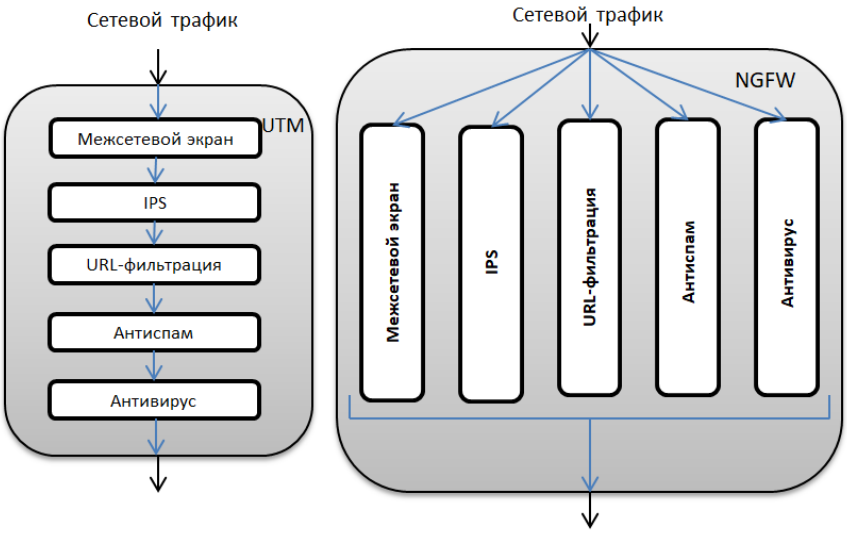

Рис. 2. Схема работы UTM и NGFW
Fig. 2. Scheme of UTM и NGFW

Необходимо отметить, что почти все современные UTM решения уже содержат NGFW. В свою очередь NGFW решения содержат функции типичные UTM. Практическое решение принимается на основе анализа требований конкретных условий эксплуатации и имеющегося бюджета[6].

Эти современные решения могут работать с большим объёмом трафика, анализировать заданный набор протоколов, в том числе, седьмого уровня модели OSI, обнаруживать атаки, используя методы сигнатурного, поведенческого анализа, а также технологии машинного обучения и обнаружения сетевых аномалий. Помимо прочего они могут защищать периметр внутренней сетевой инфраструктуры от внешних угроз и обнаруживать внутреннюю вредоносную активность.

Статистика показывает, что практически 93% атак – это реализация ситуации с возможностью проникновения и получения доступа ко всем средствам локальной вычислительной сети (ЛВС). Причем для тестирования на преодоление и получения доступа в ЛВС во многих случаях требуется не более получаса[6].

Необходимо отметить, что данный класс систем защиты не выявляет ряд вторжений по следующим причинам[6]:

– они действуют только на периметре защищаемой инфраструктуры;

– не фиксируется информация обо всём трафике, а записывается только информация о тех сигнатурах, которые сработали;

– не просматривается заново ранее обработанный трафик, что требуется для выявления неизвестных на момент реализации угроз.

Поэтому все данные решения не могут гарантированно реализовать защиту от целенаправленных квалифицированных атак, локализовать угрозу, точно выявить пораженные узлы и предоставить фактуру для проведения полноценного расследования инцидентов[6].

В качестве разрешения данной проблемы предлагается новый NDR-класс устройств обнаружения и реагирования (detection and response).

В различных публикациях сообщается, что NDR-решения позволяют выявить подозрительную активность в трафике, не отмеченную устройствами периметровой защиты[7], а также, что NDR – это одно из лучших средств обнаружения угроз, которое к тому же хорошо встраивается такое решение как Центр мониторинга информационной безопасности (SOC – Security Operations Center)[8].

Основными особенностями NDR-решений являются[6]:

– исследование внутреннего и внешнего трафика, причем необходимо отметить, что рассматриваются как «периметровые» протоколы известные как HTTP, DNS, SMTP, так и «инфраструктурные» (DCE/RPC – Distributed Computing Environment / Remote Procedure Calls или (SMB – Server Message Block, LDAP – Lightweight Directory Access Protocol);

– запись всего трафика, который уже был обработан с целью проведения расследований, восстановления цепочки атаки, выявления и локализации пораженных узлов и оценки ущерба.

В инфраструктуре организации NDR-решение выступает как единый узел анализа всего трафика или произвольного набора сетевых сегментов (рис. 3).

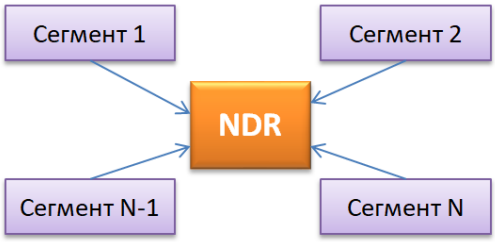

Рис. 3. Схема встраивания NDR в сетевую инфраструктуру
Fig. 3. Diagram of NDR integration into the network infrastructure

В противовес классическим средствам периметровой защиты NDR –решения действуют в режиме обнаружения, а не предотвращения вторжений. Хотя они не могут дешифровать трафик методом «man-in-the-middle», но как указано[6], это нельзя считать значимым недостатком по следующим причинам.

1. В ситуации с внешним трафиком часто используется способ перенаправления трафика непосредственно после средств IPS/UTM/NGFW, которые содержат такие решения.

2. В ситуации с внутренним трафиком 64% специалистов выбирают критерий прозрачности, а не шифрование.

3. Производители средств NDR предлагают альтернативные методы работы с шифрованным трафиком. Так, например, в решении Positive Technologies Network Attack Discovery – системе глубокого анализа сетевого трафика, реализован метод выявления

[7]Gartner. URL: www.gartner.com (дата обращения: 06.01.2022).
[8]ExtraHop Networks. URL: www.extrahop.com (дата обращения: 12.02.2022).

вредоносного поведения в шифрованном трафике без его дешифровки, на основе статистических данных запросов и ответов в рамках одного соединения[9].

В табл. 1 на основе данных[6, 10] и [14] приведены сравнительные данные современных решений защиты периметра сетевой инфраструктуры.

Таблица 1. Сравнение современных средств защиты периметра

	«Классическая» IDS	IPS (NG IPS)	UTM	NGFW (при включении всех модулей)	Detection And Response
Методы обнаружения атак	Сигнатуры	Сигнатуры, поведенческий анализ, машинное обучение и аномалии	Сигнатуры, поведенческий анализ, машинное обучение и аномалии	Сигнатуры, поведенческий анализ, машинное обучение и аномалии	Сигнатуры, поведенческий анализ, машинное обучение и аномалии и более
Блокировка атак	Нет, только выявление	Да	Да	Да	Да
Работа с шифрованным трафиком	Отсутствует	Man-in-the-middle	Man-in-the-middle	Man-in-the-middle	Альтернативные методы
Анализ сессий	Первые N байт	Первые N байт	Первые N байт	Первые N байт	Целиком
Анализ «внешних» протоколов	Да	Да	Да	Да	Да
Анализ «внутренних» протоколов	Нет	Нет	Нет	Нет	Да
Индексация обработанного трафика	Отсутствует	Частично (только о выявленных атаках)	Частично (только о выявленных атаках)	Частично (только о выявленных атаках)	Полная (хранение информации о трафике, независимо от обнаружений)
Хранение сырого трафика	Отсутствует	Отсутствует	Отсутствует	Частично (только фрагменты, относящиеся к выявленной атаке)	Полное

В течение длительного периода решения защиты периметра были единственным методом мониторинга сети. В настоящее время ландшафт сетевых угроз КИИ сильно меняется и теперь важно обеспечивать не только мониторинг периметра, но и глубоко изучать все угрозы внутренней сети. С этой точки зрения более перспективными представляются решения указанного выше класса обнаружения и реагирования (detection and response). Но, за последнее время семейство таких решений (обнаружения и реагирования) возросло, появился целый ряд предложений со своими особенностями, которые и будут рассмотрены далее.

[9]URL: https://www.ptsecurity.com/ru-ru/products/network-attack-discovery/ (дата обращения 21.09.2022).
[10]Лаборатория Касперского. URL: www.kaspersky.ru (дата обращения: 06.01.2022).

2. Сравнительный анализ решений «Threat Detection and Response»

Как указано выше решения типа «Threat Detection and Response» (обнаружение и реагирование на угрозы) в настоящее время считается незаменимым средством обеспечения безопасности корпоративных сетей. Из-за возрастания масштаба вычислительных сред и все более сложных требований по их безопасности обнаружение и предотвращение атак должно происходить в автоматизированном режиме, а в случае их реализации сетевая инфраструктура должна быть быстро и эффективно восстановлена и/или очищена.

Указанные выше аббревиатуры (EDR, MDR, NDR, XDR) могут скрывать несколько типов решений «обнаружения и реагирования», предлагаемых на рынке. Рассмотрим, что означают эти аббревиатуры, и что отличает одно решение от другого.

В EDR-решении каждое устройство, подключённое к сети, рассматривается как потенциальный вектор атаки для угроз из Интернета. В целом, решения EDR собирают данные с конечных точек, используя их для выявления возможных атак и предоставляя эффективные способы расследования и реагирования на инциденты с автоматизацией формирования последующей отчетности[11].

NDR-решение обеспечивает полное обнаружение известных и неизвестных сетевых атак. Такие решения, как правило, обеспечивают централизованный машинный анализ сетевого трафика и соответствующее реагирование, включая эффективные рабочие процессы и автоматизацию подготовки отчетности. Размещение в сети и использование машинного обучения обеспечивают полное понимание процессов и анализ сети, в частности, для выявления и устранения «боковиков» («lateral movements»)[11].

В MDR-решениях управляемого обнаружения и реагирования основное внимание уделяется не технологиям, а сервису. В рамках таких решений клиенты передают свои операции по обеспечению безопасности на аутсорсинг в целях обеспечения круглосуточной надежной безопасности. Поставщики таких услуг безопасности предлагают своим клиентам MDR доступ к своему пулу аналитиков и инженеров по безопасности, которые специализируются на мониторинге сети, анализе инцидентов и реагировании на инциденты безопасности. Эта услуга особенно востребована в области SOC (центр управления безопасностью) и SIEM (информация о безопасности и управление событиями) из-за отсутствия у заказчика специалистов нужной квалификации и/или необходимых ресурсов[11].

XDR-решение расширяет потенциал EDR-устройств за счет применения значительно более мощного пакета «искусственного интеллекта», а также реализации автоматизированного подхода. Отсюда его условное название «все в одном», так как оно включает сразу четыре компонента: UBA/UEBA, EDR, SIEM и SOAR. Как правило, это моновендорная реализация[10].

Для проведения сравнительного анализа по критериям: цель, используемые методы и возможные проблемы применения, на основе данных[11, 12, 13] для указанных выше решений можно использовать табл. 2.

На основании данных табл. 2 можно выделить основные возможности каждого метода защиты, показанные на рис. 4.

Таким образом, внедрение технологических решений XDR в комплекс безопасности объекта КИИ имеет значительное преимущество за счет улучшения возможностей защиты, обнаружения и реагирования. Например, даже при больших

[11]Nomios Group. URL: www.nomios.com (дата обращения: 12.02.2022).
[12]CISCO. URL: www.cisco.com (дата обращения: 06.01.2022).
[13]Checkpoint. URL: www.checkpoint.com (дата обращения: 6.01.2022).

инвестициях в безопасность сети время обнаружения и отклика на инциденты может быть замедлено из-за большого количества потоков анализируемых данных от различных продуктов. Инструментарий XDR позволяет централизовать все эти данные в одном хранилище, что значительно облегчает получение целостного представления о потенциальных угрозах.

Таблица 2. Сравнение решений класса обнаружения и реагирование

	EDR	NDR	MDR	XDR «всё в одном»
Область применения	Конечные точки и хосты	Сетевой трафик и трафик между устройствами	Организации	Конечные точки, хосты, Сетевой трафик и трафик между устройствами, приложения
Цель	Защита конечной точки/области доступа от проникновения, мониторинг и смягчение последствий, оценка уязвимости, оповещение и реагирование	Видимость / прозрачность сетевого трафика, обнаружение известных и неизвестных угроз и lateral movements, оповещение и реагирование	Аутсорсинг экспертных знаний в области безопасности, централизация информации о безопасности, высококачественные консультации и соблюдение требований безопасности	Видимость / прозрачность на нескольких уровнях безопасности (сеть, конечная точка, приложения), обнаружение известных и неизвестных угроз уровня lateral movements, включая все компоненты, комплексный мониторинг и смягчение последствий, оценка уязвимости, оповещение и реагирование, упрощение и консолидация событий, а также целенаправленное реагирования.
Методы	Malicious behaviour, Indicator of Attack (IoA), Indicator of Compromise (IoC), сигнатуры, машинное обучение	Indicator of Attack (IoA), обнаружение аномалий, поведение пользователей, машинное обучение	Интеграция клиентских систем через различные интерфейсы (API, ведение журнала, сбор данных и т.д.)	Машинное обучение, Indicator of Attack (IoA), обнаружение аномалий, поведение пользователя, вредоносное поведение, Indicator of Compromise
Основные проблемы	Advanced Persistent Threats (APT), ransomware, вредоносные скрипты и т. д.	Продвинутые атаки и вторжения, malware-free атаки	Нехватка навыков/ресурсов в области безопасности в организации, упрощение повседневной безопасности: сведение к минимуму предупреждений / событий	Возможность интеграции / взаимодействия производителей, частично типичные проблемы для EDR и NDR.

Поддержание сетевой безопасности в актуальном состоянии требует повышенного внимания, что может привести к «растянутости» команд безопасности с отвлечением сотрудников от выполнения важных и трудоемких бизнес-задач. Инструментарий XDR

повышает эффективность операций безопасности за счет обширных возможностей автоматизации, таких, как мониторинг аномалий, извлечение информации из соответствующих источников данных, отправка предупреждений и даже реализация мер по устранению последствий инцидентов[14].

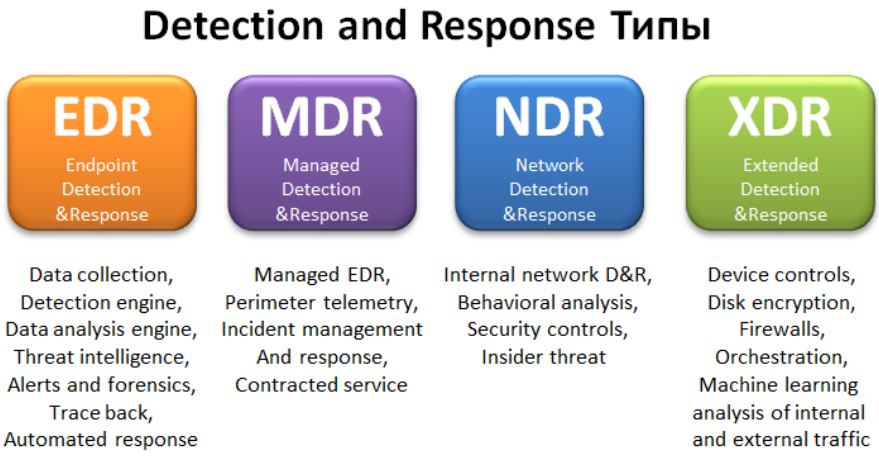

Рис. 4. Разновидности средств обнаружения и реагирования
Fig. 4. Varieties of detection and response tools

XDR – хороший вариант бюджетной экономии. Если не платить за несколько лицензий и подписок на прикладное ПО (SaaS) можно в конечном итоге увидеть более низкую общую стоимость владения и снижение накладных расходов на обеспечение безопасности.

3. Решения типа «Extended Detection and Response»

Надо отметить, что системы обнаружения и реагирования оперируют данными из журналов безопасности, логов сетевых устройств, а также получают данные от антивирусов. Для анализа этой информации создаются структурные элементы, называемые Security Operation Center (SOC). Специалисты SOC-подразделений анализируют события безопасности, выявляют и расследуют инциденты, принимают меры для предупреждения и блокировки кибератак[15].

XDR стали объединять в себе все основные инструменты для SOC: UBA/UEBA, EDR, SIEM и SOAR.

Рассмотрим работу системы XDR подробнее. За счет объединения разных инструментов она даёт возможность комплексно следить за атаками с помощью сравнительного анализа поколений актуальных и предыдущих данных на уровнях[15]: конечных точек; сети (IPS – Intrusion Detection System, сетевые сенсоры, шлюзы безопасности); сканеров уязвимостей; облачных средах и виртуализации; почтового трафика; системы управления доступом; DLP-систем и т.д.

Собранные данные идут на обработку в нескольких этапах. В первую очередь осуществляется нормализация этой информации по заранее заданным параметрам. Затем она поступает в Data Lake («озеро данных»). Проводится корреляция данных и реагирование, в том числе расследование инцидента. В этом смысле решение XDR похоже на известную SIEM технологию. Но, главной его отличительной чертой является

[14]Издание Anti-Malware.ru. URL: www.anti-malware.ru (дата обращения: 25.03.2022).
[15]Хакер.ru. URL: www.xakep.ru (дата обращения: 12.02.2022).

объединение множества событий, которые поступают из самых разных источников, в общую историю атаки[15]. В конечном итоге, появляется возможность фиксировать все этапы атаки и выяснить первоначальное действие как источник инцидента через единую консоль, что устраняет потребность в разных элементах администрирования, зачастую не связанных друг с другом. Процессы сбора и анализа событий реализованы на автоматизированных действиях системы и машинном обучении, что позволяет сократить количество администраторов безопасности и других работников, сил обеспечения безопасности[15]. На рис. 5 приведена схема работы решений XDR.

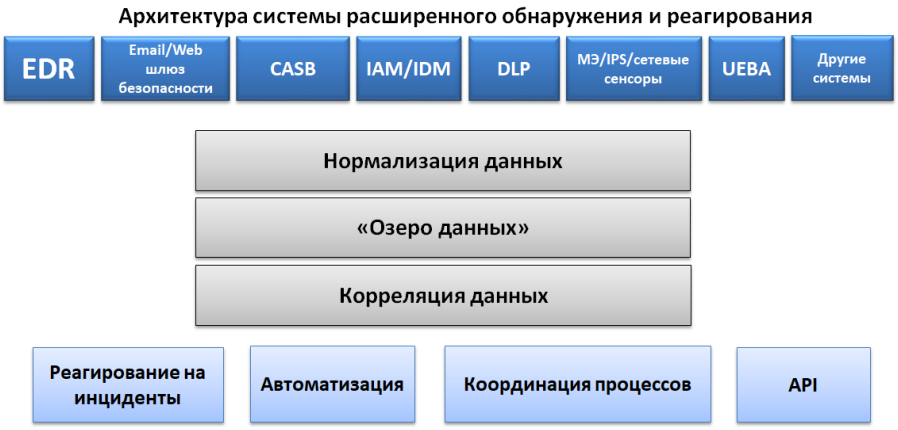

Рис. 5. Схема работы XDR-решений
Fig. 5. Scheme of XDR-solutions

Соединение решений UBA/UEBA, EDR, SIEM и SOAR в единый комплекс даёт соответствующий синергетический эффект. Комплекс содержит весь спектр сетевых устройств сетевой защиты, позволяющий активно выявлять неизвестные угрозы и реагировать на них в автоматизированном режиме, предотвращая развитие атаки.

XDR-решение может работать и на уровне конечных устройств, анализируя сетевой трафик, электронную почту и облачную инфраструктуру, включая различные системы контейнеризации. Установленные на конечных точках сенсоры собирают данные телеметрии, сведения о поведении пользователя, программ и другую информацию. Отдельный модуль анализирует сетевой трафик всех подключённых к сети устройств, в том числе «интернета вещей» (IoT/IIoT), принтеры и личные устройства сотрудников, используемые по схеме BYOD (Bring Your Own Device)[15].

Важно выделить такой компонент XDR как систему обеспечения безопасности облачных сервисов. Всё больше пользователей переносит информационную инфраструктуру в «облака», все чаще используются системы контейнеризации. Поэтому нужны и меры выявления соответствующих угроз. Собранные XDR-модулями сведения передаются в глобальную базу об угрозах и событиях, где информация обрабатывается с использованием искусственного интеллекта и специальных алгоритмов работы с большими данными. Необходимо отметить, что в отличие от SIEM-систем XDR-решение анализирует происходящее в корпоративной сети как единое целое, выдавая несколько сообщений об атаках вместо тысяч предупреждений. Используя встроенную в систему модуль визуализации, можно обеспечить операционный контроль всех устройств, задействованных в атаке, проанализировать выполненные действия, а также оценить их последствия. Все стадии атаки можно «отмотать назад» вплоть до «нулевого пациента», ставшего источником заражения.

Таким образом, XDR-решения выводят работу SOC на новый уровень. Специалисты по безопасности получают только значимые информативные оповещения, отсортированные по приоритету в зависимости от критичности инцидента, благодаря многоуровневому анализу сведений, собранных по всей инфраструктуре организации, экспертным данным об угрозах, искусственному интеллекту и анализу по методологии «больших данных» (Big Data). Сведения об угрозах из различных источников в автоматизированном режиме сопоставляют роботы, что обеспечивает глубокий анализ на ранее недоступном уровне. Богатый контекст по большему количеству векторов атаки дает возможность распознать индикаторы компрометации даже в событиях, которые по отдельности кажутся безобидными. Контекст позволяет сопоставлять факты, получить более детальную информацию для расследования. В результате сокращается время на обнаружение, сдерживание и реагирование, а масштаб последствий может снижаться до минимального уровня.

Вместе с тем у всех современных решений по обнаружению и реагированию есть один общий минус – невозможность адекватной защиты при удалённом формате работы. Так в отчете[7] за 2021 г. был сформирован список технологий, которые могут повлиять на эффективность бизнеса в ближайшие годы. На период 2022–2025 гг. сделан прогноз о развитии технологической концепции, названной «Cybersecurity Mesh» («сеть кибербезопасности». Основной особенностью этой концепции является учет такого фактора как дистанционный формат работы сотрудников, «размывается» классическое определение периметра безопасности. Очевидно, что технологическое решение этой концепции потребует более гибкой модульной архитектуры, которая должна соединять в единый комплекс все распределённые службы. То есть методология «Cybersecurity Mesh» направлена на интеграцию всей структуры безопасности, а также осуществление защиты территориально распределенных активов. По предварительным оценкам авторов подобная трансформация инфраструктуры безопасности должна сократить бизнес потери примерно на 90%.

4. Концепция «Cybersecurity Mesh»

Понятие и концепция «Cybersecurity Mesh» введено фирмой Gartner. Точного определения этой тенденции технологического развития средств сетевой безопасности пока нет, как и готовых решений. Авторы выдвинули данную концепцию без уточнения мер и конкретных технических решений[7].

В сфере технологий обеспечения информационной безопасности на уровне организации наблюдается тенденция к децентрализации контрольных точек и переносу мер защиты с внешней границы IT-систем на уровень конечных пользователей. При этом учитывается упомянутый выше фактор дистанционных форматов бизнес-процессов работы сотрудников, в результате чего многие риски могут быть реализованы на уровне пользователей.

В этом случае очевидна неэффективность обычной защиты с помощью межсетевого экрана от утечки данных сотрудника, а существующие облачные решения не позволяют контролировать безопасность используемых аппаратных средств. С этим связана так называемая концепция безопасности нулевого доверия («Zero Trust») [15], в том числе к легальным пользователям.

Концепция «Cybersecurity Mesh» показывает возможность реализации «Zero Trust»-решений как набора децентрализованных устройств, помогающих организовать защиту на уровне конечных пользователей, их компьютеров и активов во внутренней сети: приложений, баз данных и даже каналов связи[7]. Разделение доступов, внедрение

дополнительных способов аутентификации, контроля устройства, анализа поведения и других средств направлены на повышение общего уровня безопасности и предотвращение большей части вторжений и инцидентов. Акцент на децентрализацию помогает избежать точек отказа, а также осуществление проверок подлинности данных без необходимости постоянной связи. Сюда же относятся комплексные решения с использованием технологии блокчейн[7].

Таким образом, обеспечение кибербезопасности сетевой инфраструктуры по-прежнему является концептуальной стратегией, а не определенной архитектурой или стандартизированным техническим подходом. Это говорит о том, что на уровне пользователей необходимо модифицировать архитектуру кибербезопасности с целью интеграции инструментов безопасности в единую экосистему. Это позволит снизить риски проявления отдельных инцидентов безопасности. Система безопасности распределенной корпоративной сети как объекта КИИ должна использовать аналитику искусственного интеллекта в сочетании с элементами управления идентификацией, политикой, позицией и прозрачностью информации/событий.

Заключение

Приведенный аналитический обзор существующих технологических решений обеспечения кибербезопасности сетевого периметра объектов КИИ показывает, что, несмотря на их определенную эффективность по противодействию компьютерным атакам, существует объективная необходимость в технологическом развитии данного направления, основой которого, на наш взгляд, может стать концепция «Cybersecurity Mesh». По мнению авторов, ее технологическая реализация позволит обеспечить необходимую защищенность сетевого периметра распределенных объектов КИИ. Эти аспекты станут предметом дальнейших исследований и соответствующих публикаций.

СПИСОК ЛИТЕРАТУРЫ

1. Клименко И.С. Информационная безопасность и защита информации. Модели и методы управления. Монография. Инфра-М, серия Научная мысль, 2019. – 180 с. DOI: http://dx.doi.org/10.12737/monography_5d412ff13c0b88.75804464.
2. Zhukov A.N., Geraskin N.I. & Krasnoborodko A.A. (2016). Defining quantitative criteria for the physical protection system effectiveness of nuclear facilities. Defense & Security Analysis, 32, 91–96. DOI: http://dx.doi.org/10.1080/14751798.2015.1130320.
3. Наталичев Роман В. и др. Эволюция и парадоксы нормативной базы обеспечения безопасности объектов критической информационной инфраструктуры. Безопасность информационных технологий, [S.l.], т. 28, № 3, с. 6–27, 2021. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2021.3.01. – EDN JIMDXU.
4. Новопавловский Артем А., Дёмин Иван Н., Зиннуров Данил И. Использование модели компьютерных атак для предотвращения действий киберпреступников на основе модели Cyber Threat Framework. Colloquium-journal. 2019, № 16-2(40), с. 104–106. URL: https://www.elibrary.ru/item.asp?id=39242773 (дата обращения: 20.09.2022). – EDN FQGTCN.
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://www.elibrary.ru/item.asp?id=42437509&pff=1 (дата обращения: 20.09.2022). – EDN PCNMBB.
6. Касперский Е.В. В заложниках у автоматики: как защитить промышленность от кибератак. www.RBC.RU. Есть мнение. 12 сен. 2016 г. URL: https://www.rbc.ru/opinions/business/12/09/2016/57d2947d9a7947bd5adb221c?from=newsfeed (дата обращения: 20.09.2022).
7. Корниенко А.А., Слюсаренко И.М. Системы и методы обнаружения вторжений: современное состояние и направления совершенствования. CIT Forum, 2009. URL: http://citforum.ru/security/internet/ids_overview/ (дата обращения: 20.09.2022).

8. 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: 20.09.2022). – EDN DBOZDA.
9. Зацепина А.С., Боровский А.С. Сравнительный анализ UBA, SIEM, SOAR систем информационной безопасностью. 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: 20.09.2022). – EDN GEVJCM.
10. 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. URL: https://www.elibrary.ru/item.asp?id=38203954&pff=1 (дата обращения: 20.09.2022). – EDN QRXEIX.
11. 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.
12. Кусакина Н.М. Методы анализа сетевого трафика как основа проектирования системы обнаружения сетевых атак. Труды XLI Междунар. науч.-прак. конф. «International Scientific Review of the Problems and Prospects of Modern Science and Education». Boston: Problems of Science, 2018. С. 28–31. URL: https://www.elibrary.ru/item.asp?id=32639163 (дата обращения: 20.09.2022). – EDN YSVHBU.
13. Браницкий А.А., Котенко И.В. Анализ и классификация методов обнаружения сетевых атак. Труды СПИИРАН. № 2(45). СПб.: ФГБУН «СПИИРАН», 2016. С. 207–244. DOI: http://dx.doi.org/10.15622/SP.45.13.
14. Еременко В.Т., Фисун А.П., Макеев С.М., Соловьев Б.И., Маркин Д.О. Системы обнаружения компьютерных атак. Орёл: ОГУ имени И. С. Тургенева, 2018. – 135 с. URL: http://elib.oreluniver.ru/uchebniki-i-uch-posobiya/sistemy-obnaruzheniya-kompyuternyh-atak.html (дата обращения: 20.09.2022).
15. 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: 20.09.2022). – EDN TNNNET.

REFERENCES:

[1] Klimenko I.S. Information Security and Information Protection. Management models and methods. Monograph. Infra-M, Series Scientific Thought, 2019. – 180 p. DOI: http://dx.doi.org/10.12737/monography_5d412ff13c0b88.75804464 (in Russian).
[2] Zhukov A.N., Geraskin N.I. & Krasnoborodko A.A. (2016). Defining quantitative criteria for the physical protection system effectiveness of nuclear facilities. Defense & Security Analysis, 32, 91–96. DOI: http://dx.doi.org/10.1080/14751798.2015.1130320.
[3] Natalichev Roman V. et al. Evolution and paradoxes of the regulatory framework for ensuring the security of critical information infrastructure facilities. IT Security, [S.l.], v. 28, no. 3, p. 6–27, 2021. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2021.3.01 (in Russian). – EDN JIMDXU.
[4] Novopavlovskiy Artem A., Dyomin Ivan N., Zinnurov Danil I. Using the model of computer attacks to prevent the actions of cyber crimes based on the cyber Threat Framework Model. Colloquium-journal. 2019, no. 16-2(40), p. 104–106. URL: https://www.elibrary.ru/item.asp?id=39242773 (accessed: 20.09.2022) (in Russian). – EDN FQGTCN.
[5] Kharlamova T.L., Murasheva T.V. Transition to a remote form of work as a response to the challenges of digitalization. Nedelya nauki SPbPU. 2019, p. 55–57. URL: https://www.elibrary.ru/item.asp?id=42437509&pff=1 (accessed: 20.09.2022) (in Russian). – EDN PCNMBB.
[6] Kaspersky E.V. Automation hostage: how to protect the industry againts cyber attacks. URL: https://www.rbc.ru/opinions/business/12/09/2016/57d2947d9a7947bd5adb221c?from=newsfeed. (accessed: 20.09.2022) (in Russian).
[7] Kornienko A.A., Slyusarenko I.M. Systems and methods of intrusion detection: modern state and directions of improvement. CIT Forum, 2009. URL: http://citforum.ru/security/internet/ids_overview/ (accessed: 20.09.2022) (in Russian).

[8] Anikin D.V. Information Protection in the 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 Graduate Students, 2021. P. 21–26. URL: https://www.elibrary.ru/item.asp?id=47975667 (accessed: 20.09.2022) (in Russian). – EDN DBOZDA.

[9] Zatsepina A.S., Borovsky A.S. Comparative analysis of UBA, SIEM, SOAR systems of information security. Computer integration of production and IPI-technologies. SPB.: 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: 20.09.2022) (in Russian). – EDN GEVJCM.

[10] Kovtun A.V. Management of access to information resources of enterprises on the basis of the concept of identity access management. Science and innovations in the modern world. M.: Collection of scientific articles, 2018. P. 158–162. URL: https://www.elibrary.ru/item.asp?id=38203954&pff=1 (accessed: 20.09.2022) (in Russian). – EDN QRXEIX.

[11] Vishnevsky A.S. Deceptive system for the detection of hacker attacks, based on the analysis of the behavior of visitors to web sites. Voprosy kiberbezopasnosti. 2018, no. 3(27), p. 54–62. DOI: http://dx.doi.org/10.21681/2311-3456-2018-3-54-62 (in Russian).

[12] Kusakina N.M. Methods of the network traffic analysis as a basis for designing the intrusion detection system. International scientific review of the problems and prospects of modern science and education XLI International scientific and practical conference. Boston: Problems of Science, 2018. P. 28–31. URL: https://www.elibrary.ru/item.asp?id=32639163 (accessed: 20.09.2022) (in Russian). – EDN YSVHBU.

[13] Branitsky A.A., Kotenko I.V. Analysis and classification of methods for detecting network attacks. Trudy SPIIRAN. No. 2(45). SPb.: FGBUN «SPIIRAN», 2016. P. 207–244. DOI: http://dx.doi.org/10.15622/SP.45.13 (in Russian).

[14] Eremenko V.T., Fisun A.P., Makeev S.M., Solovyov BI., Markin D. O. Systems for detecting computer attacks. Oryol: OSU imeni I. S. Turgenev, 2018. – 135p. URL: http://elib.oreluniver.ru/uchebniki-i-uch-posobiya/sistemy-obnaruzheniya-kompyuternyh-atak.html (accessed: 20.09.2022) (in Russian).

[15] Kuznetsov S.A., Kulikov I.A., Fominykh A.A. Model of zero trust in relation to 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: 20.09.2022) (in Russian). – EDN TNNNET.

Поступила в редакцию – 20 августа 2022 г. Окончательный вариант – 01 октября 2022 г.
Received – August 20, 2022. The final version – October 01, 2022.