ЭКОНОМИКА И ОРГАНИЗАЦИЯ ДЕЯТЕЛЬНОСТИ ПРЕДПРИЯТИЙ, ОТРАСЛЕЙ, КОМПЛЕКСОВ

ECONOMICS AND ORGANIZATION OF ENTERPRISES, INDUSTRIES, COMPLEXES

Оригинальная статья / Original article

УДК 004.89

https://doi.org/10.21869/2223-1552-2023-13-4-111-122

Кибербезопасность объектов критической инфраструктуры

Г. В. Федотова[1,2] ✉, Ю. А. Капустина[3], А. Г. Чураев[4], З. Ю. Юлдашбаева[5]

[1] Федеральный исследовательский центр «Информатика и управление» РАН
ул. Вавилова, д. 44/2, г. Москва 119333, Российская Федерация

[2] Московская государственная академия ветеринарной медицины и биотехнологии – МВА имени К. И. Скрябина
ул. Академика Скрябина, д. 23, г. Москва 109472, Российская Федерация

[3] Уральский государственный лесотехнический университет
ул. Сибирский тракт, д. 37, г. Екатеринбург 620100, Российская Федерация

[4] СХК «Агрофирма «Согратль»
ул. Центральная, д. 23, г. Махачкала 400131, Российская Федерация

[5] Российский государственный аграрный университет – МСХА имени К. А. Тимирязева
ул. Тимирязевская, д. 49, г. Москва 127434, Российская Федерация

✉ e-mail: g_evgeeva@mail.ru

Резюме

Актуальность. *Кибербезопасность информационных систем и сервисов становится одним из важных критериев качества предоставления услуг и производства товаров в современном обществе, таким же как устойчивость и скорость передачи данных. Разработчики программных продуктов и приложений озабочены ростом количества атак на их системы, ростом объемов краж информации и активов. Конфронтация России и стран НАТО активизировало рост геополитических угроз и хакерских вторжений в информационную систему России с целью ее дестабилизации и деактивации. При этом компанией «Ростелеком-Солар» отмечено, что особенно привлекают хакеров объекты критической инфраструктуры российской экономики.*

Цель *исследования заключалась в оценке современных технологий защиты цифровых сервисов, применяемых компаниями, и определении новых подходов к усилению систем безопасности.*

Задачи. *В статье были поставлены и последовательно решены следующие задачи: оценить современные тенденции трансформации информационных систем, а также объектов критической информационной инфраструктуры в свете участившихся атак хакеров; предложить новый подход к решению проблем кибербезопасности.*

Методология. *В работе были использованы методы графического, горизонтального и логического анализа, обобщения и систематизации данных.*

Результаты. *На основе общего обзора технологий защиты критической инфраструктуры как со стороны государства, так и со стороны бизнеса был сделан вывод о необходимости формирования триады видимости уязвимостей.*

Выводы. *В статье рассмотрены направления перестройки всей кибериндустрии и формирования нового вектора развития цифрового мира в условиях меняющихся геополитических противостояний развитых держав. Сделан вывод о необходимости смены парадигмы рынка технологий в сторону перевода всех программ на российские технологии и активизацию их продвижения в страны ЕАЭС, что позволит построить новый евразийский рынок IT под наставничеством РФ.*

Ключевые слова: *кибератаки; безопасность; критическая информационная инфраструктура; цифровые системы; защита.*

Конфликт интересов: *В представленной публикации отсутствует заимствованный материал без ссылок на автора и (или) источник заимствования, нет результатов научных работ, выполненных авторами публикации лично и (или) в соавторстве, без соответствующих ссылок. Авторы декларируют отсутствие конфликта интересов, связанных с публикацией данной статьи.*

Для цитирования: Кибербезопасность объектов критической инфраструктуры / Г. В. Федотова, Ю. А. Капустина, А. Г. Чураев, З. Ю. Юлдашбаева // Известия Юго-Западного государственного университета. Серия: Экономика. Социология. Менеджмент. 2023. Т. 13, № 4. С. 111–122. https://doi.org/10.21869/2223-1552-2023-13-4-111-122.

Поступила в редакцию 10.06.2023 Принята к публикации 06.07.2023 Опубликована 30.08.2023

Cybersecurity of Critical Infrastructure Facilities

Gilian V. Fedotova[1,2] ✉, Yulia A. Kapustina[3], Abdurakhman G. Churaev[4], Zarina Yu. Yuldashbayeva[5]

[1] Federal Research Center "Computer Science and Control" RAS
44/2 Vavilova Str., Moscow 119333, Russian Federation

[2] Moscow State Academy of Veterinary Medicine and Biotechnology - MBA named after K. I. Skryabin
23 Academician Skryabina Str., Moscow 109472, Russian Federation

[3] Ural State Forestry University
37 Siberian Tract Str., Ekaterinburg 620100, Russian Federation

[4] SHK Agrofirma Sogratl
23 Centralnaya Str., Makhachkala 400131, Russian Federation

[5] Russian State Agrarian University - Moscow Agricultural Academy named after K. A. Timiryazev
49 Timiryazevskaya Str., Moscow 127434, Russian Federation

✉ e-mail: g_evgeeva@mail.ru

Abstract

Relevance*. The cybersecurity of information systems and services is becoming one of the important criteria for the quality of services and production of goods in modern society, just like the stability and speed of data transfer. Developers of software products and applications are concerned about the increase in the number of attacks on their systems, the increase in the theft of information and assets. The confrontation between Russia and NATO countries has intensified the growth of geopolitical threats and hacker intrusions into the information system of Russia with the aim of destabilizing and deactivating it. At the same time, Rostelecom-Solar noted that hackers are especially attracted to the critical infrastructure of the Russian economy.*

The purpose *of the study was to evaluate modern technologies for protecting digital services used by companies and to identify new approaches to strengthening security systems.*

Objectives*. The following tasks were set and consistently solved in the article: to assess the current trends in the transformation of information systems, as well as objects of critical information infrastructure in the light of the increasing attacks of hackers; propose a new approach to solving cybersecurity problems.*

Methodology*. The methods of graphical, horizontal and logical analysis, generalization and systematization of data were used in the work.*

Results. *Based on a general review of technologies for protecting critical infrastructure, both from the side of the state and from the side of business, it was concluded that it is necessary to form a triad of visibility of vulnerabilities.*

Conclusions. *The article considers the directions of restructuring the entire cyber industry and the formation of a new vector for the development of the digital world in the context of changing geopolitical confrontations between developed powers. It is concluded that it is necessary to change the paradigm of the technology market in the direction of transferring all programs to Russian technologies and intensifying their promotion to the EAEU countries, which will allow building a new Eurasian IT market under the guidance of the Russian Federation.*

Keywords*: cyber attacks; security; critical information infrastructure; digital systems; protection.*

***Conflict of interest**: In the presented publication there is no borrowed material without references to the author and (or) source of borrowing, there are no results of scientific works performed by the author of the publication, personally and (or) in co-authorship, without relevant links. The author declares no conflict of interest related to the publication of this article.*

For citation: Fedotova G. V., Kapustina Y. A., Churaev A. G., Yuldashbayeva Z. Yu. Cybersecurity of Critical Infrastructure Facilities. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Ekonomika. Sotsiologiya. Menedzhment = Proceedings of the Southwest State University. Series: Economics, Sociology and Management*. 2023; 13(4): 111–122. (In Russ.) https://doi.org/10.21869/2223-1552-2023-13-4-111-122.

Received 10.06.2023 Accepted 06.07.2023 Published 30.08.2023

***

Введение

С момента принятия в 2017 г. Советом Безопасности ООН резолюции 2341 о противостоянии глобальным террористическим атакам на критически важные объекты инфраструктуры и расширении превентивных мер по их защите и предотвращению новых атак были исследованы наиболее передовые и успешные практики стран по защите указанных объектов и сделан вывод о недостаточности предпринимаемых мер защиты [1]. В России с 2018 г. вступил в силу ФЗ-187 «О безопасности критической информационной инфраструктуры Российской Федерации», который определил перечень объектов и субъектов критической информационной инфраструктуры (КИИ) или критической важной инфраструктуры (КВИ) [2]. Законом установлено, что субъекты КИИ должны не только поддерживать работу системы, но и обеспечивать их защиту от внешних вторжений. Государство со своей стороны оказывает информационную и техническую поддержку субъектам КИИ.

В мировой практике нет устоявшего понятия КИИ, поэтому за основу берем законодательно определенную терминологию – информационные и информационно-коммуникационные сети и системы, АСУ, сети электросвязи, используемые для взаимодействия между компаниями, организациями с государственными структурами в ключевых сферах. Перечень отраслей определен ФЗ-187. Другие страны под объектами КИИ понимают «…системы и активы, физические или виртуальные, жизненно важные для государства…», «…физические и информационные технологические объекты, сети, услуги и активы…» [3; 4], при этом ключевым фактором выступает значимость этих объектов для национальной безопасности государства и его граждан. Можно отметить, что важность данной инфраструктуры заключается в поддержании работоспособности и функционирования основных ключевых отраслей экономики и социальной сферы в любой стране.

Материалы и методы

Постоянные и непрекращающиеся атаки формируют новый подход к выстраиванию системы информационной безопасности уже на этапе разработки и проектирования сервисов и программах продуктов. Антироссийские санкции, ужесточившиеся в 2022 г., привели к резкому дефициту технологий и средств поддержки работоспособности серверов. Сегодня отечественный рынок столкнулся с проблемой поиска новых путей и подходов к обеспечению спроса российских пользователей и субъектов хозяйствования. Назрела необходимость разработки отечественных инструментов и перевода всех пользователей на российские операционные системы, что будет расширять возможности российских производителей. Поэтому в нашем исследовании поставлена задача изучения существующих систем поддержания безопасности инфраструктурных объектов национальной экономики.

Основной базой исследования послужили нормативно-правовые акты, направленные на повышение информационной безопасности российских цифровых инфраструктурных объектов в условиях нарастающего давления кибермошенников. Был исследован принцип построения

системы ГосСОПКА, обеспечивающий поддержание защиты и работоспособности объектов, признанных критически важными для экономики страны.

Основными методами научного исследования выступили метод аналогии, систематизации, графического и статистического анализа, выводы были сформулированы с помощью методов обобщения, генерации идей и логического анализа.

Результаты и их обсуждение

Ухудшение геополитической ситуации с начала 2022 г. поставило российские организации в центр внимания хакеров, основной целью которых являлось выведение из строя объектов критической информационной инфраструктуры. Результаты статистики кибератак за 2022 г. доказали, что активность киберзлоумышленников достигла значение 911 тыс. атак, что в 2 раза превышает показатель 2021 г. При этом по наблюдениям специалистов по безопасности атаки стали носить целевой характер, число которых достигло 65%. Основными целями атак выступили объекты КИИ России, почти 54% атак в 2022 г. были направлены на них (рис. 1).

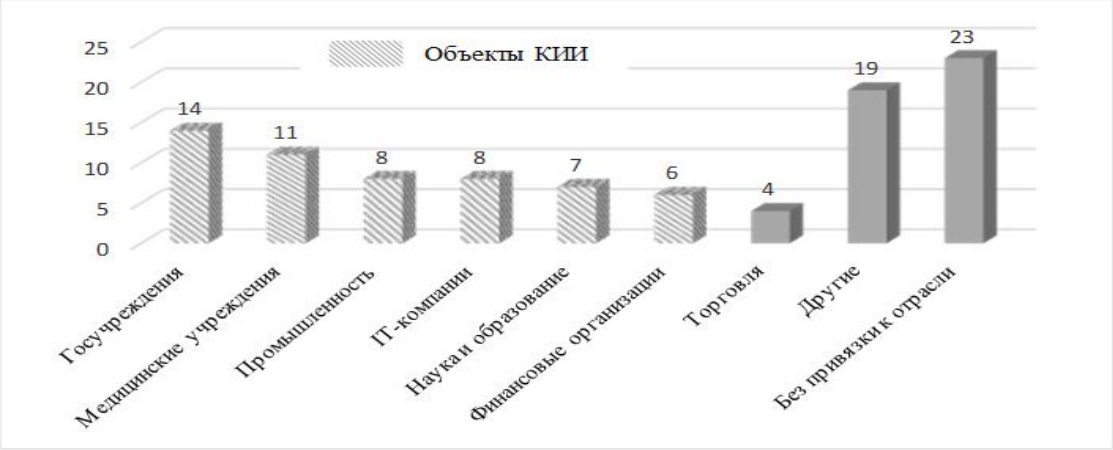

Рис. 1. Статистика кибератак на различные информационные объекты в 2022 г., % [5; 6]

Общая статистика 2022 г. констатирует не только рост общего числа атак, но и изменения самого характера атак. Атаки с середины 2022 г. стали носить целевой характер, основными объектами чаще стали выступать учреждения государственного сектора экономики. На рисунке 1 видим, что на первом месте по объему атак стоит госсектор – 14%, на втором месте медицинские учреждения – 11%, на третьем промышленность и IT-компании – по 8% всех кибератак. Все перечисленные объекты относятся к критически важной инфраструктуре страны. Очевидно, что основной целью хакеров выступает дестабилизация экономики и управление ее стратегическими информационными системами.

В 2022 г. специалистами по безопасности Positive Technologies был установлен новый антирекорд – было верифицировано около 25 тысяч новых уязвимостей, разработанных и запущенных на российские сервисы из DarkNet, или около 70 уязвимостей в день атаковали российскую инфраструктуру в 2022 г. Проблемы с идентификацией уязвимостей также были связана с тем, что иностранные вендоры ушли из России и перестали поддерживать и обновлять свои ПО. Фактически информационная инфраструктура России самостоятельно противостояла кибератакам без поддержки разработчиков приложений и программных платформ.

Видим, что кибермир выступает зеркальным отражением всех происходящих процессов в реальном мире, при этом скорость обратной связи в нем гораздо выше. Киберландшафт очень быстро меняется и спрогнозировать его будущее

состояние удается с низкой долей вероятности. Прогнозы выстраиваются, но они должны основываться на прогнозах социально-экономического развития реального сектора экономики.

Корпорации независимо от форм собственности сегодня собственными силами обеспечивают защиту своей информационной инфраструктуры от атак, но, к сожалению, усилий одной организации оказывается недостаточно для противостояния целому миру хакеров, работающих на темной стороне Интернета. Поэтому появилась идея создания единой национальной системы защиты ключевых для государства информационных объектов, которые будут обслуживаться высокопрофессиональными специалистами, готовыми в режиме 24/7 подключаться к отражению атак киберпреступников в любой точке системы. Кроме того, в такой глобальной сети аккумулируются большие массивы данных о инцидентах, проводится полный их анализ, постоянно обновляются технологии противостояния хакерам. Система функционирует как единое целое и при необходимости возникновения угроз атак весь ее потенциал будет перенаправлен на отражение текущей кибератаки. Таким образом, появилась концепция создания центров компетенций, функционирующих в единой сети подконтрольной государству.

Критически важная инфраструктура вступает базисом цифровизации государственного сектора экономики и государственного управления, поэтому ее защите уделяют внимание, прежде всего, на национальном уровне. С этой целью 15 января 2013 г. Указом Президента РФ № 31с была создана ГосСОПКА – Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ [7]. Фактически данным нормативным документом была создана сеть информационной защиты, территориально распределенная по всей стране.

ГосСОПКА имеет сложную организационно-техническую разветвленную структуру, подчиненную ФСБ России. Подразделения организованы по принципу ведомственности и территориальности. Схематично можно представить данную систему следующим образом (рис. 2).

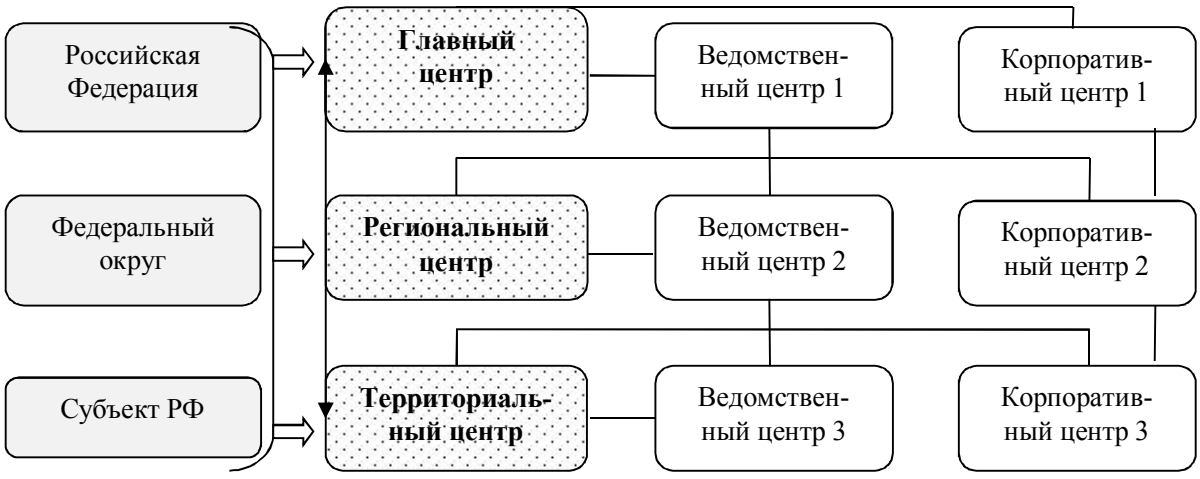

Рис. 2. Организационная структура ГосСОПКА [8]

Главный центр ГосСОПКА – Национальный координационный центр по компьютерным инцидентам (далее – НКЦКИ), образованный в 2018 г. Приказом ФСБ России [8]. Главные региональный и территориальный центры создаются и поддерживаются органами ФСБ, ведомственные центра создаются и поддерживаются органами государственной власти, корпоративные центра – организациями, осуществляющими лицензированную деятельность в области защиты

информации. Взаимосвязи внутри системы выстроены таким образом, что обмен информацией происходит не только по уровням подчиненности, но и по вертикали ведомственных и корпоративных центров [9; 10]. Основными задачами системы выступают предотвращение компьютерных атак, выстраивание систем защиты информационных ресурсов, оценка причин и последствий компьютерных атак, мониторинг степени защищенности объектов, поддержание взаимодействия между структурными подразделениями и центрами. Механизм взаимодействия регламентируется ответственными органами и поддерживается 2 способами обмена информацией: через инфраструктуру НКЦКИ, через почтовую, факсимильную или электронную связь (телефон). Субъекты КИИ должны в обязательном порядке подключиться к соответствующему ведомственному Центру ГосСОПКА, при этом субъекты частной формы собственности самостоятельно определяют порядок и формат подключения к центрам системы.

Фактически данная глобальная сеть представляет собой некий национальный SEIM, в котором функционирует множество центров мониторинга информационной безопасности, накапливаются колоссальные массивы данных о компьютерных инцидентах, и все перечисленное аккумулируется в НКЦКИ. Особенности взаимодействия объектов КИИ с государственной системой защиты ГосСОПКА определены целым рядом нормативно-правовых документов как федерального, так и ведомственного уровня.

Рассмотрим схему оперативного управления в системе ГосСОПКА (рис. 3).

В составе ГосСОПКА комплексно работают различные средства по обнаружению, защите и реагированию на компьютерные атаки. Благодаря слаженной скоординированной работе принимаются превентивные меры по предупреждению возможных атак и обеспечивается высокий уровень защиты критической инфраструктуры. По оценкам экспертов, основные потери от кибератак на российские информационные системы были связаны с утечкой конфиденциальной информации и персональных данных из наиболее популярных сервисов: «Яндекс.Еда», «Гемотест», «Вкусвилл», «СДЭК» и т. п. [11; 12]. Максимальный процент утечек персональных данных наблюдался в медицинских учреждениях (до 82% инцидентов), в научных организациях (до 67% инцидентов). При этом украденные данные становились объектами торгов в DarkNet. Общая сумма ущерба от кражи данных составила 4,35 млн долл. согласно отчету IBM [13; 14]. Структура краж представлена ниже (рис. 4).

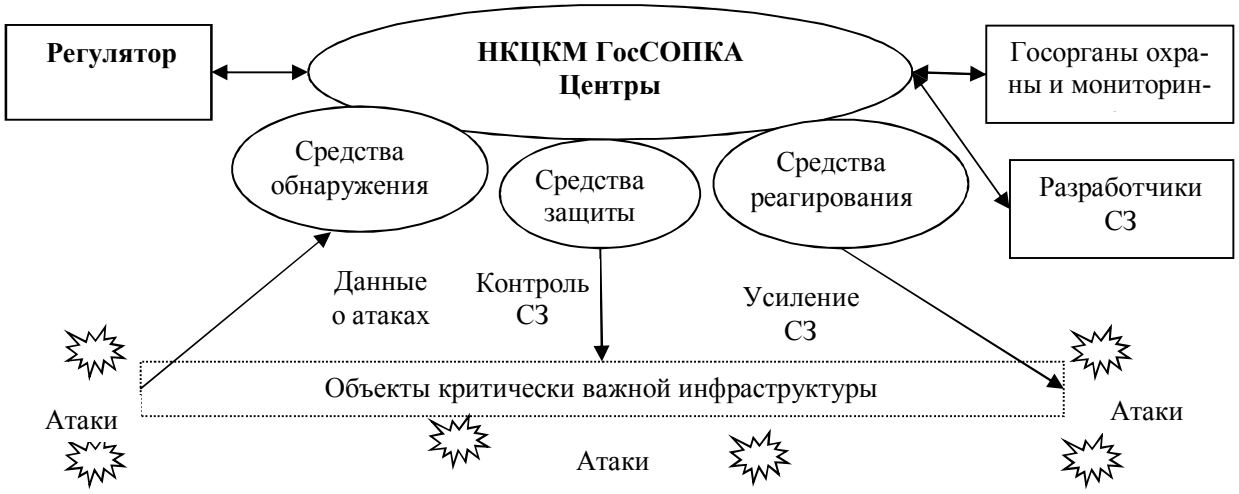

Рис. 3. Механизм информационного взаимодействия ГосСОПКА с объектами КВИ [7]

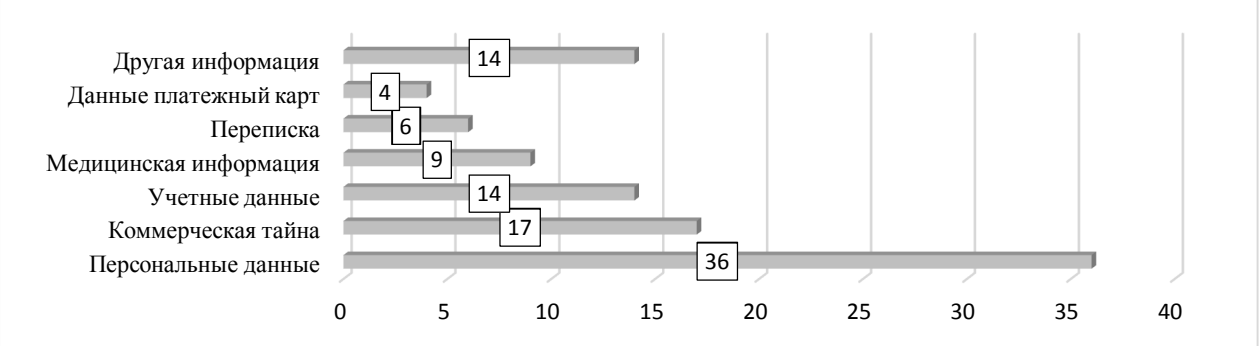

Рис. 4. Типы украденных данных по результатам успешных атак в 2022 г., % [4]

Статистика демонстрирует, что наибольшей популярностью пользовались персональные данные пользователей, кражи который достигли 36% в 2022 г. На втором месте стоит информация, относящаяся к коммерческой тайне, – до 17%, на третьем месте учетные данные – до 14%. Перечисленные информационные массивы имеют большую популярность в качестве объектов торговли в теневом Интернете, что в последующем периоде порождает волну взломов личных аккаунтов, вывода средств с личных счетов, оформление незаконных сделок по фальшивым документам и т. п. Все эти действия имеют финансовую основу, целью которой выступает мошенничество. Поэтому цифровые сервисы и организации должны не сводить информационную безопасность к формальности, а действительно гарантировать своим клиентам и контрагентам защиту данных и качество цифровых услуг.

Корпоративный уровень защиты КВИ сводится не только к необходимости подключения имеющихся объектов к системе ГосСОПКА, в которой будет оказан необходимый уровень поддержки и мониторинга состояния системы защиты. Корпорации для защиты собственных цифровых систем используют передовые технологии и средства мониторинга состояния систем [12]. В качестве примера можно рассмотреть новые принципы выстраивания системы защиты на уровне отдельной организации [13; 14].

Одним из успешных решений по борьбе с кибератаками выступают *Network Detection and Response* (далее – *NDR*) – сетевые обнаружения и реагирования, обеспечивающие оперативные ответы на подозрительные трафики как с севера на юг, так и с востока на запад через периметр предприятия [15]. Применяемые сегодня многими компаниями системы управления событиями безопасности (SEIM) и системы обнаружения вредоносной активности (EDR) недостаточны для сопротивления участившимся кибератакам, что в итоге может привести к блокировке работы системы и роста расходов на ее реабилитацию. Поэтому данные технологии необходимо укреплять новым решением NDR, которые в комбинации с уже имеющейся системой защиты позволят закрыть уязвимые точки и оперативно устранить подозрительные эксплойты уже на точке входа и блокировать их. Особенность таких решений заключается в постоянном анализе трафика и обнаружении аномалий в модели трафика, даже при зашифрованном трафике [16; 17]. Отметим, что данные решения NDR эффективнее всего применять в коллаборации с защитой SEIM&EDR. Работая в симбиозе, данные решения образуют некую *триаду видимости мониторинга уязвимостей*, т. е. наиболее правильный принцип применения данных технологий – сетевой подход к выстраиванию системы безопасности [18; 19].

Рассмотрим схему работы такой триады (рис. 5). Обоснованность сетевого под-

хода к комбинации различных технологий информационной защиты связана с необходимостью учета разнообразных факторов и новых уязвимостей, которые постоянно генерирует DarkNet (темная сторона Интернета) – сфера работы хакеров и кибермошенников [6; 20]. Только комплекс технологий (в данном случае – триада) позволит максимально усилить систему защиты информационных объектов, подвергающихся постоянным атакам из Интернета. Основной принцип работы триады – четкая скоординированность действий, применяемых системой защиты, в которой основным источником достоверности выступает только информация или сигналы, прошедшие через NDR. Часть поступающих сетевого трафика фильтруется через SEIM, при прохождении периметра и входа в него; какие-то целевые атаки нейтрализуются инструментами EDR уже в самой системе на ее конкретном участке. При этом данные сервисы не координировали свою работу, а были направлены на решение различных задач [21].

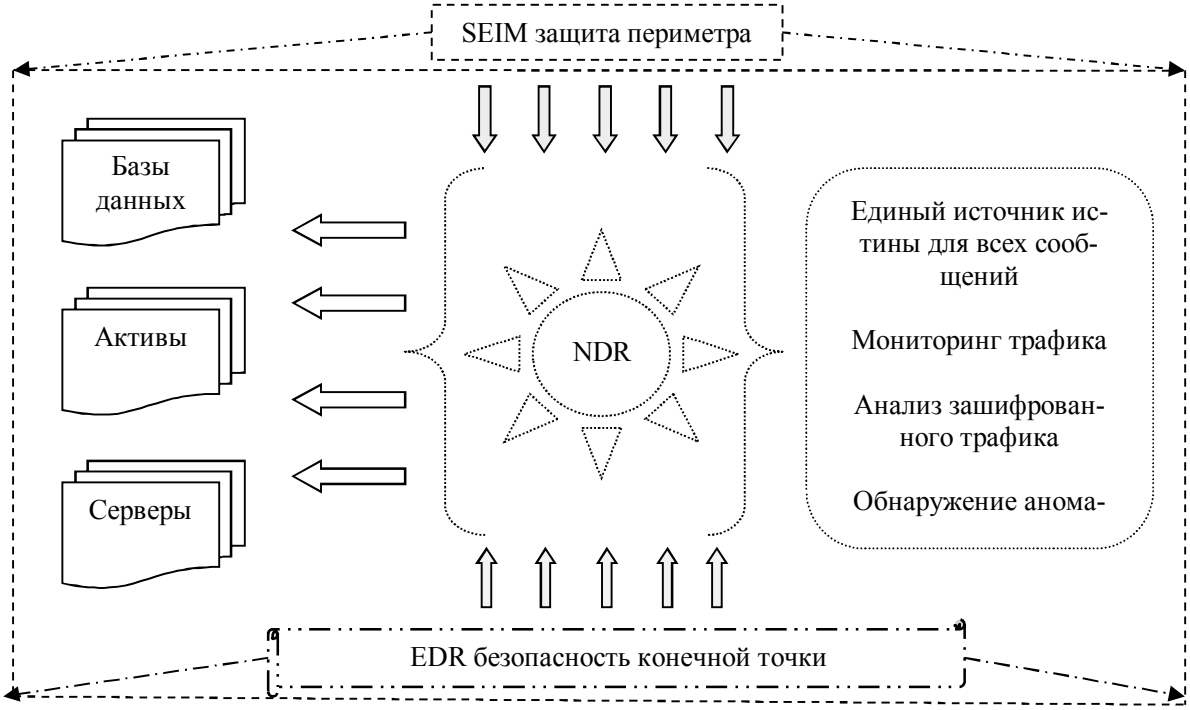

Рис. 5. Триада видимости мониторинга уязвимостей

В триаде все системы будут работать в тандеме и подчиняться NDR, которое будет анализировать весь трафик на предмет обнаружения аномалий в модели поведения. Особенность анализа, проводимого NDR-решением, является использование нетипичных технологий:

– машинное обучение – непрерывное вычисление и анализ энтропии между отдельными сегментами сети, составление статистической отчетности и выявление всплесков и отклонений;

– адаптивный базовый уровень – анализ различных хостов и сравнение их поведения, уровня активности для выявления отклонений;

– эвристика – поиск нетипичных симптомов в сети и расчет вероятности их недобросовестности;

– анализ поведения пользователя в сети – поиск нелигитимных шаблонов поведения пользователей в системе;

– данные о репутации – сформированная база и постоянно дополняющаяся, скомпрометировавших себя IP-адресов, хостов, доменов и т. п.

Комплекс представленных технологий дает возможность не просто идентифици-

ровать атаки на систему, но и распознавать зашифрованные вредоносные трафики.

В конечном итоге NDR принимает решение и проводит определенные действия на блокировку обнаруженных кибератак. Таким образом, происходит нейтрализация атак на точке входа в систему, что позволяет избежать ее дезорганизации и дополнительных расходов на ее восстановление.

Сетевой подход в формировании системы безопасности дает преимущество IT-специалистам для предупреждения новых кибератак и сохранения ценных активов и персональных данных. Хакеры постоянно повышают свою квалификацию, изобретают новые способы обхода защиты, что диктует необходимость полного анализа и моделирования ситуации в самые краткие сроки. Поэтому выстраивание триад мониторинга уязвимостей на основе нескольких технологий защиты будет укреплять сопротивляемость информационной инфраструктуры.

Современная индустрия кибербезопасности стоит на этапе переформатирования принципов и подходов выстраивания систем защиты не только в государственном секторе, но и во всех пользовательских цифровых сервисах.

Выводы

Проблемы защиты критической информационной инфраструктуры в условиях политической напряженности требуют выстраивания системы защиты национального информационного периметра, а также переход на полный технический суверенитет. Уход многих поставщиков высокотехнологичной микроэлектроники и вендоров с российского рынка и блокировка поставок импортных технологий повышают уязвимость российских систем и формируют разрыв между разработчиками и пользователями технологий. В данной ситуации остается только один путь – полный переход на российское ПО, которое необходимо развивать до уровня международного.

Постоянные атаки на государственный сектор экономики будут генерировать новые идеи и концепции для полной защиты периметра и обеспечения бесперебойности работы публичных сервисов оказания услуг населению и предприятиям. В таких условиях масштабный перевод всех пользователей на отечественные технологии позволит максимально сфокусировать усилия на адаптации технологий к условиям трансформирующегося рынка.

В будущем будут формироваться региональные локальные рынки ПО и технологий защиты информации, выстраиваться новые логистические цепи поставок оборудования, осуществляться расширение новых экосистем в отдельных регионах.

В данной ситуации Россия должна использовать свои технологические возможности для выстраивания нового киберландшафта в Евразийском регионе.

Список литературы

1. О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации: Указ Президента Российской Федерации от 30.03.2022 г. № 166. URL: http://publication.pravo.gov.ru/Document/View/0001202203300001 (дата обращения: 11.05.2023).

2. О безопасности критической информационной инфраструктуры: Федеральный закон №187-ФЗ от 26.07.2017 г. URL: https://rtmtech.ru/articles/kriticheskaya-informatsionnaya-infrastruktura-2019/ (дата обращения: 08.05.2023).

3. Карасёв П. А., Стефанович Д. В. Кибербезопасность критически важной инфраструктуры: новые вызовы // Россия в глобальной политике. 2022. № 20(6). С. 147-164.

4. Отчет «Кибератаки на российские компании в 2022 году». URL: https://rt-solar.ru/upload/iblock/4a4/ghus61x9rd8cv5vczms5ig1svts4tlep/Otchet-o-kiberatakakh-na-rossiyskie-kompanii-v-2022-godu.pdf (дата обращения: 08.05.2023).

5. Политика государства в сфере международной кибербезопасности. URL: https://www.tadviser.ru/index.php/Статья:Киберпреступность_и_киберконфликты_:_Россия (дата обращения: 08.05.2023).

6. Аналитические отчеты об угрозах и уязвимостях АСУ ТП на портале Kaspersky Threat Intelligence. URL: https://ics-cert.kaspersky.ru/services/ (дата обращения: 11.05.2023).

7. О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации: Указ Президента Российской Федерации от 15.01.2013 г. № 31с. URL: http://www.kremlin.ru/acts/bank/36691 (дата обращения: 08.05.2023).

8. О Национальном координационном центре по компьютерным инцидентам: Приказ Федеральной службы безопасности Российской Федерации от 24.07.2018 г. № 366. URL: http://publication.pravo.gov.ru/Document/View/0001201809100001 (дата обращения: 08.05.2023).

9. Безопасность объектов критической информационной инфраструктуры организации. URL: http://aciso.ru/files/docs/metodichka_2.0.pdf. Accessed 29 March 2023 (дата обращения: 08.05.2023).

10. Царев Е. О. Критическая информационная инфраструктура 2022 год. URL: https://rtmtech.ru/articles/kriticheskaya-informatsionnaya-infrastruktura-2019/ (дата обращения: 08.05.2023).

11. КиберНЕустойчивость и как с ней бороться. URL: https://www.itsec.ru/articles/ kiberneustojchivost-i-kak-s-nej-borotsya (дата обращения: 08.05.2023).

12. Кибербезопасность 2022-2023. Тренды и прогнозы. URL: https://www.ptsecurity.com/ru-ru/research/analytics/ogo-kakaya-ib/#id9 (дата обращения: 08.05.2023).

13. Федотова Г. В., Орлова Е. Р., Бочарова И. Е. Вопросы кибербезопасности цифровых финансовых сервисов // Информационные технологии и вычислительные системы. 2022. № 2. С. 37-45.

14. Об одном подходе к обеспечению безопасности данных в информационной системе средствами ОС и СУБД / Г. П. Акимова [и др.] // Информационные технологии и вычислительные системы. 2022. № 1. С. 33-39.

15. Защита критически важных объектов инфраструктуры от террористических атак: сборник передового опыта. URL: https://unrcca.unmissions.org/sites/default/files/rus_compendium_on_ critical_infrastructure_0.pdf (дата обращения: 11.05.2023).

16. Актуальные киберугрозы: итоги 2022 года. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022/ (дата обращения: 11.05.2023).

17. Мишустин заявил, что России нужно догонять зарубежные страны в области микроэлектроники. URL: https://tass.ru/ekonomika/9025357 (дата обращения: 11.05.2023).

18. Li Y. The Semiconductor Industry: A Strategic Look at China's Supply Chain. The New Chinese Dream. Cham: Palgrave Macmillan, 2021. P. 121-136.

19. Капустина Ю. А., Ильясов Р. Х., Цицигэ. Экономика хактивизма – новый вектор развития теневого бизнеса // Известия Юго-Западного государственного университета. Серия: Экономика. Социология. Менеджмент. 2022. № 2(5). С. 56-67.

20. Тренды digital-трансформации банков 2021–2024. URL: https://vc.ru/future/338072-trendy-digital-transformacii-bankov-2021-2024 (дата обращения: 11.05.2023).

21. Burbach D. T., Watts C. Messing with the Enemy: Surviving in a Social Media World of Hackers, Terrorists, Russians, and Fake News // Naval War College Review. 2020. Vol. 73, No. 1. P. 17.

References

1. O merakh po obespecheniyu tekhnologicheskoi nezavisimosti i bezopasnosti kriticheskoi informatsionnoi infrastruktury Rossiiskoi Federatsii [On measures to ensure the technological independence and security of the critical information infrastructure of the Russian Federation]. Decree of the President of the Russian Federation of March 30, 2022 № 166. Available at: http://publication.pravo.gov.ru/Document/View/0001202203300001. (accessed 11.05.2023)

2. O bezopasnosti kriticheskoi informatsionnoi infrastruktury [On the Security of Critical Information Infrastructure]. Federal Law of July 26, 2017 № 187-FZ. Available at: https://rtmtech.ru/articles/kriticheskaya-informatsionnaya-infrastruktura-2019/. (accessed 11.05.2023)

3. Karasev P. A., Stefanovich D. V. Kiberbezopasnost' kriticheski vazhnoĭ infrastruktury: novye vyzovy [Cybersecurity of Critical Infrastructure: New Challenges]. *Rossiya v global'noi politike = Russia in Global Affairs*, 2022, no. 20(6), pp. 147-164.

4. Otchet "Kiberataki na rossiiskie kompanii v 2022 godu" [Report "Cyber attacks on Russian companies in 2022"]. Available at: https://rt-solar.ru/upload/iblock/4a4/ghus61x9rd8cv5vczms5ig1svts4tlep/Otchet-o-kiberatakakh-na-rossiyskie-kompanii-v-2022-godu.pdf. (accessed 08.05.2023)

5. Politika gosudarstva v sfere mezhdunarodnoi kiberbezopasnosti [State policy in the field of international cybersecurity]. Available at: https://www.tadviser.ru/index.php/Article:Cybercrime_and_ cyberconflicts : Russia. (accessed 08.05.2023)

6. Analiticheskie otchety ob ugrozakh i uyazvimostyakh ASU TP na portale Kaspersky Threat Intelligence [Analytical reports on ICS threats and vulnerabilities on the Kaspersky Threat Intelligence portal]. Available at: https://ics-cert.kaspersky.com/services/. (accessed 11.05.2023)

7. O sozdanii gosudarstvennoi sistemy obnaruzheniya, preduprezhdeniya i likvidatsii po-sledstvii komp'yuternykh atak na informatsionnye resursy Rossiiskoi Federatsii [On the creation of a state system for detecting, preventing and eliminating the consequences of computer attacks on information resources of the Russian Federation]. Decree of the President of the Russian Federation of January 15, 2013 № 31s. Available at: http://www.kremlin.ru/acts/bank/36691. (accessed 08.05.2023)

8. O Natsional'nom koordinatsionnom tsentre po komp'yuternym intsidentam [On the National Coordination Center for Computer Incidents]. Order of the Federal Security Service of the Russian Federation dated July 24, 2018 № 366. Available at: http://publication.pravo.gov.ru/Document/View/0001201809100001. (accessed 08.05.2023)

9. Bezopasnost' ob"ektov kriticheskoi informatsionnoi infrastruktury organizatsii [Security of objects of critical information infrastructure of the organization]. Available at: http://aciso.ru/files/docs/metodichka 2.0.pdf. Accessed 29 March 2023. (accessed 08.05.2023)

10. Tsarev E. O. Kriticheskaya informatsionnaya infrastruktura 2022 god [Critical Information Infrastructure 2022]. Available at: https://rtmtech.ru/articles/kriticheskaya-informatsionnaya-infrastruktura-2019/. (accessed 08.05.2023)

11. KiberNEustoichivost' i kak s nei borot'sya [Cyber instability and how to deal with it]. Available at: https://www.itsec.ru/articles/kiberneustojchivost-i-kak-s-nej-borotsya. (accessed 08.05.2023)

12. Kiberbezopasnost' 2022-2023. Trendy i prognozy [Cybersecurity 2022-2023. Trends and forecasts]. Available at: https://www.ptsecurity.com/en-us/research/analytics/ogo-kakaya-ib/#id9. (accessed 08.05.2023)

13. Fedotova G. V., Orlova E. R., Bocharova I. E. Voprosy kiberbezopasnosti tsifrovykh finansovykh servisov [Issues of cybersecurity of digital financial services]. *Informatsionnye tekhnologii i vychislitel'nye sistemy = Information technologies and computing systems*, 2022, no. 2, pp. 37-45.

14. Akimova G. P., eds. Ob odnom podkhode k obespecheniyu bezopasnosti dannykh v informatsionnoi sisteme sredstvami OS i SUBD [On one approach to ensuring data security in an information system using OS and DBMS]. *Informatsionnye tekhnologii i vychislitel'nye sistemy = Information Technologies and Computing Systems*, 2022, no. 1, pp. 33-39.

15. Zashchita kriticheski vazhnykh ob"ektov infrastruktury ot terroristicheskikh atak. Sbornik peredovogo opyta [Protecting Critical Infrastructure from Terrorist Attacks. A Compilation of Best Practices]. Available at: https://unrcca.unmissions.org/sites/default/files/eng_compendium_on_critical_infrastructure 0.pdf. (accessed 11.05.2023)

16. Aktual'nye kiberugrozy: itogi 2022 goda [Actual cyber threats: results of 2022]. Available at: https://www.ptsecurity.com/en-us/research/analytics/cybersecurity-threatscape-2022/. (accessed 11.05.2023)

17. Mishustin zayavil, chto Rossii nuzhno dogonyat' zarubezhnye strany v oblasti mikroelektroniki [Mishustin said that Russia needs to catch up with foreign countries in the field of microelectronics]. Available at: https://tass.ru/ekonomika/9025357. (accessed 11.05.2023)

18. Li Y. The Semiconductor Industry: A Strategic Look at China's Supply Chain. The New Chinese Dream. Cham, Palgrave Macmillan Publ., 2021, pp. 121-136.

19. Kapustina Yu. A., Ilyasov R. Kh., Tsitsige. Ekonomika khaktivizma – novyi vektor razvitiya tenevogo biznesa [The economy of hacktivism is a new vector for the development of shadow business]. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Ekonomika. Sotsiologiya.*

Menedzhment = Proceedings of the Southwest State University. Series: Economics, Sociology and Management, 2022, no. 2(5), pp. 56-67.

20. Trendy digital-transformatsii bankov 2021–2024 [Trends in digital transformation of banks 2021–2024]. Available at: https://vc.ru/future/338072-trendy-digital-transformacii-bankov-2021-2024. (accessed 11.05.2023)

21. Burbach D. T., Watts C. Messing with the Enemy: Surviving in a Social Media World of Hackers, Terrorists, Russians, and Fake News. *Naval War College Review*, 2020, vol. 73, no. 1, p. 17.

Информация об авторах / Information about the Authors

Федотова Гилян Васильевна, доктор экономических наук, ведущий научный сотрудник, Федеральный исследовательский центр «Информатика и управление» РАН; профессор кафедры экономики и цифровых технологий в АПК, Московская государственная академия ветеринарной медицины и биотехнологии – MBA имени К. И. Скрябина, г. Москва, Российская Федерация,
e-mail: g_evgeeva@mail.ru,
Researcer ID: N-8708-2015,
ORCID: 0000-0002-2066-8628

Gilian V. Fedotova, Dr. of Sci. (Economics), Leading Researcher, Federal Research Center "Computer Science and Control" of the Russian Academy of Sciences; Professor of the Department of Economics and Digital Technologies in the Agroindustrial Complex, Moscow State Academy of Veterinary Medicine and Biotechnology – MBA named after K. I. Skryabin, Moscow, Russian Federation,
e-mail: g_evgeeva@mail.ru,
Researcer ID: N-8708-2015,
ORCID: 0000-0002-2066-8628

Капустина Юлия Александровна, кандидат экономических наук, доцент, директор социально-экономического института, Уральский государственный лесотехнический университет, г. Екатеринбург, Российская Федерация,
e-mail: kapustina_bu@mail.ru,
ORCID: 0000-0002-6828-4332

Yulia A. Kapustina, Cand. of Sci. (Economics), Associate Professor, Director of the Socio-Economic Institute, Ural State Forestry University, Yekaterinburg, Russian Federation,
e-mail: kapustina_bu@mail.ru,
ORCID: 0000-0002-6828-4332

Чураев Абдурахман Гарунович, директор, СХК «Агрофирма «Согратль», г. Махачкала, Российская Федерация,
e-mail: zoo@rgau-msha.ru,
Researcer ID: ISB-2210-2023,
ORCID: 0009-0005-5051-0361

Abdurakhman G. Churaev, Director of Agricultural Company "Agrofirma "Sogratl", Makhachkala, Russian Federation,
e-mail: zoo@rgau-msha.ru,
Researcer ID: ISB-2210-2023,
ORCID: 0009-0005-5051-0361

Юлдашбаева Зарина Юсупжановна, студент, Российский государственный аграрный университет – МСХА имени К. А. Тимирязева, г. Москва, Российская Федерация,
e-mail: zoo@rgau-msha.ru,
Researcer ID: ISB-1911-2023,
ORCID: 0009-0007-5045-0949

Zarina Yu. Yuldashbayeva, Student, Russian State Agrarian University – Moscow Agricultural Academy named after K. A. Timiryazev, Moscow, Russian Federation,
e-mail: zoo@rgau-msha.ru,
Researcer ID: ISB-1911-2023,
ORCID: 0009-0007-5045-0949