Якоб Я. Месенгисер[1], Марк А. Малахов[2], Наталья Г. Милославская[3]
Национальный исследовательский ядерный университет «МИФИ»,
Каширское ш., 31, Москва, 115409, Россия
[1]e-mail: myy001@campus.mephi.ru, http://orcid.org/0000-0002-6674-4374
[2]e-mail: mma034@campus.mephi.ru, http://orcid.org/0000-0001-8599-1920
[3]e-mail: NGMiloslavskaya@mephi.ru, http://orcid.org/0000-0002-1231-1805

ЦЕНТРЫ УПРАВЛЕНИЯ СЕТЕВОЙ БЕЗОПАСНОСТЬЮ КАК СИЛЫ ГОССОПКА

DOI: http://dx.doi.org/10.26583/bit.2022.1.09

Аннотация. В статье рассматривается необходимость создания центра управления сетевой безопасностью (ЦУСБ), а также определяются функции ЦУСБ и требования к инфраструктуре на основании требований по обеспечению безопасности, предъявляемых к субъектам критической информационной инфраструктуры Российской Федерации (КИИ РФ). Целью настоящей работы является описание ЦУСБ как сил Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак, направленных на информационные ресурсы Российской Федерации (ГосСОПКА). В рамках работы решаются следующие задачи: определяется перечень контролирующих органов, регламентирующих процессы и меры обеспечения безопасности, предъявляемых к субъектам КИИ РФ для обеспечения безопасности объектов КИИ РФ, а также сами эти процессы и меры; описываются центры мониторинга безопасности и ЦУСБ как силы ГосСОПКА. Результаты настоящей работы можно использовать в рамках организации процессов взаимодействия с ГосСОПКА и создания ЦУСБ, занимающегося вопросами противодействия компьютерным атакам, обнаружения и реагирования на инциденты круглосуточно, и учебного курса, посвященного вопросам обеспечения безопасности объектов КИИ.

Ключевые слова: центр управления сетевой безопасностью, ГосСОПКА, КИИ РФ, компьютерная атака, информационная безопасность.
Для цитирования: МЕСЕНГИСЕР, Якоб Я.; МАЛАХОВ, Марк А.; МИЛОСЛАВСКАЯ, Наталья Г. ЦЕНТРЫ УПРАВЛЕНИЯ СЕТЕВОЙ БЕЗОПАСНОСТЬЮ КАК СИЛЫ ГОССОПКА. Безопасность информационных технологий, [S.l.], т. 29, № 1, с. 94–107, 2022. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1404. DOI: http://dx.doi.org/10.26583/bit.2022.1.09.

Yakob Y. Mesengiser[1], Mark A. Malakhov[2], Natalia G. Miloslavskaya[3]
National Research Nuclear University MEPhI (Moscow Engineering Physics Institute),
Kashirskoe shosse, 31 Moscow, 115409, Russia
[1]e-mail: myy001@campus.mephi.ru, http://orcid.org/0000-0002-6674-4374
[2]e-mail: mma034@campus.mephi.ru, http://orcid.org/0000-0001-8599-1920
[3]e-mail: NGMiloslavskaya@mephi.ru, http://orcid.org/0000-0002-1231-1805

Network Security Centers as the GosSOPKA Forses

DOI: http://dx.doi.org/10.26583/bit.2022.1.09

Abstract. The paper addresses the need to create a Network Security Center (NSC), and the functions of the NSC and infrastructure requirements on the basis of security requirements imposed by the subjects of the critical information infrastructure (CII) of the Russian Federation (RF) to ensure the safety of CII objects of the RF. The current work describes the NSC as the forces of the State System for Detecting, Preventing and Eliminating the Consequences of Computer Attacks Aimed at the Information Resources of the RF (GosSOPKA). As part of the work, the following tasks are solved: a list of regulatory bodies regulating the processes and security measures presented to the subjects of the CII of the RF to ensure security of objects of the CII of the Russian Federation as well as these processes and measures themselves are determined; Security Operations Centers (SOCs) and NSCs as the GosSOPKA forces are described. It is possible to use the results obtained in the framework of the processes of organizing

cooperation with GosSOPKA, and the creation of a NSC dealing with computer attacks, detecting and responding to incidents around the clock; and a training course dedicated to the CII security.
Keywords: network security centers, GosSOPKA, critical information infrastructure of Russian Federation, computer attack, information security.
For citation: MESENGISER, Yakob Y.; MALAKHOV, Mark A.; MILOSLAVSKAYA, Natalia G. Network Security Centers as the GosSOPKA Forses. IT Security (Russia), [S.l.], v. 29, n. 1, p. 94–107, 2022. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/1404. DOI: http://dx.doi.org/10.26583/bit.2022.1.09.

Введение

В настоящее время все сложнее становится противодействовать компьютерным атакам (КА). Так, за период с января по сентябрь 2019 г., удельный вес киберпреступлений, по данным МВД России, составил 13,5% [1]. В период с января по май 2021 г. удельный вес киберпреступлений вырос почти что до 27%[1] [2].

Угроза реализации КА актуальна и для органов власти, и для бизнеса, но для организаций, признанных субъектом критической информационной инфраструктуры Российской Федерации (КИИ РФ), КА представляют особую опасность для общества. Самостоятельно защищаться от таких атак способны далеко не все. 1 января 2018 г. вступил в силу Федеральный закон №187-ФЗ от 26.07.2017, который регулирует отношения в области обеспечения безопасности КИИ РФ в целях ее устойчивого функционирования при проведении в отношении ее КА[1]. Организациям, признанным субъектами КИИ РФ, необходимо обеспечить непрерывное и продуктивное взаимодействие с Государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак, направленных на информационные ресурсы Российской Федерации (ГосСОПКА)[2]. В рамках ГосСОПКА обеспечивается концентрация компетенций, необходимых для предотвращения КА и реагирования на них. При этом государство в лице Национального координационного центра по компьютерным инцидентам (НКЦКИ) выступает гарантом добросовестности центров ГосСОПКА, устанавливая требования к их деятельности, осуществляя надзор за этой деятельностью и даже непосредственно участвуя в реагировании на некоторые КА [3, 4].

Различные аспекты организации системы защиты объектов КИИ РФ рассматривались в публикациях [5–10]. В источнике [5] представлен исчерпывающий перечень документов, необходимых для разработки субъектами КИИ для создания и функционирования систем безопасности значимых объектов КИИ РФ. В [6] авторы предлагают фрагменты рекомендательной методики формирования требований к структурным подразделениям, необходимой для практического использования руководителями структурных подразделений ответственных за обеспечение безопасности значимых объектов КИИ РФ. В основе методики авторами была принята образовательная инициатива NICE, которая представляет собой сотрудничество правительства, научных кругов и частного сектора экономики, возглавляемое Национальным институтом стандартов и технологий Министерства торговли США [6]. В [7] авторами был представлен исчерпывающий состав мер по обеспечению безопасности объектов КИИ РФ третьей категории значимости. В [8] автор описывает способы взаимодействия объектов топливно-энергетического комплекса с ГосСОПКА. Так, сообщение об инциденте может быть передано через интернет-портал НКЦКИ, письмом по электронной почте,

[1]МВД России публикует данные о состоянии преступности по итогам пяти месяцев 2021 года. URL: https://мвд.рф/news/item/24738876 (дата обращения: 01.01.2022).

[2]Федеральный закон от 26 июля 2017 г. №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». URL: https://docs.cntd.ru/document/436752114/ (дата обращения: 01.01.2022).

телефонным звонком или официальным письмом. Также возможна передача сведений об инциденте с помощью специальных средств взаимодействия, напрямую подключающихся к инфраструктуре НКЦКИ. Возможна и следующая схема взаимодействия: субъект КИИ, обслуживаемый центром ГосСОПКА, может сообщить об инциденте в этот центр ГосСОПКА, и оно будет передано в НКЦКИ [8]. При организации системы защиты объектов КИИ РФ следует уделять должное внимание курсам повышения квалификации сотрудников. Так, в [9] автором рассматривается программа повышения квалификации, позволяющая слушателям курса получить знания и навыки в области обеспечения безопасности объектов КИИ РФ. Программа разъясняет действия государственных органов, учреждений и других организаций при реализации требований Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». В [10] авторами был представлен сравнительный анализ подходов к категорированию объектов КИИ в РФ и США. В работе рассматриваются основные законы, регулирующие вопросы обеспечения безопасности объектов КИИ в РФ и США, области КИИ в РФ и США. Приводится сравнение областей КИИ. Также рассматриваются основные методы по категорированию критической инфраструктуры в РФ и США. На основании проведенного исследования авторами делается вывод о схожести в выделении областей КИИ в РФ и США и принципиальных различиях в методиках соблюдения безопасности КИИ.

Таким образом, проведенный выше небольшой обзор научных статей показывает, что организация эффективного и результативного противодействия КА является актуальной темой: авторы работ раскрывают различные аспекты защиты объектов КИИ РФ. В рамках настоящей работы авторы предлагают описание подразделения – центра управления сетевой безопасностью (ЦУСБ), способного обеспечить эффективность и результативность противодействия КА. ЦУСБ также ответственен за информирование и взаимодействие с центром ГосСОПКА. Первоочередной целью развертывания ЦУСБ [11] является предоставление организации возможностей по организации непрерывных процессов предотвращения, выявления и оперативного реагирования на события и инциденты, происходящие в реальном времени, а также по прогнозированию и предупреждению КА на защищаемые объекты КИИ РФ на всех стадиях их жизненного цикла на основе своевременного анализа данных об этих событиях и инцидентах.

Таким образом, являясь частью субъекта КИИ РФ, ЦУСБ может выступать в роли силы ГосСОПКА. Целью данной статьи является определение функций ЦУСБ и требований к инфраструктуре на основании требований по обеспечению безопасности, предъявляемых к субъектам КИИ РФ.

1. Перечень контролирующих органов, регламентирующих правила, процессы и меры обеспечения безопасности для объектовКИИ РФ

Одним из важнейших этапов в области обеспечения безопасности КИИ РФ, согласно Федеральному закону №187-ФЗ, является создание ГосСОПКА.

ГосСОПКА включает в себя силы и средства. Федеральный закон №187-ФЗ относит к силам ГосСОПКА следующие субъекты:

1) подразделения и должностные лица федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования ГосСОПКА на информационные ресурсы РФ. В соответствии с указом Президента РФ от 15.01.2013

№31с этим органом является Федеральная Служба Безопасности Российской Федерации (ФСБ России)[3]. Функции ФСБ России определены в федеральном законе №187-ФЗ[1].

2) организация, создаваемая федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования ГосСОПКА на информационные ресурсы РФ, для обеспечения координации деятельности субъектов КИИ РФ по вопросам обнаружения, предупреждения и ликвидации последствий КА и реагирования на компьютерные инциденты – НКЦКИ[1]. Важно отметить, что согласно Федеральному закону №187-ФЗ, НКЦКИ осуществляет свою деятельность в соответствии с положением, утверждаемым ФСБ России[1]. Содержание положения ФСБ России о деятельности НКЦКИ представлено в приказе ФСБ России от 24 июля 2018 г. №366[4];

3) подразделения и должностные лица субъектов КИИ РФ, которые принимают участие в обнаружении, предупреждении и ликвидации последствий КА и в реагировании на компьютерные инциденты[1].

Также следует отметить указ Президента РФ от 25.11.2017 №569[4], в котором Федеральная служба по техническому и экспортному контролю (ФСТЭК России) является органом исполнительной власти, уполномоченным в области обеспечения безопасности КИИ, противодействия техническим разведкам и технической защиты информации, а также специально уполномоченный орган в области экспортного контроля.

2. Процессы и меры обеспечения безопасности объектов КИИ РФ

Для определения процессов и мер обеспечения безопасности объектов КИИ РФ необходимо определить категорию значимости рассматриваемых объектов КИИ РФ. Определять категорию значимости объектов КИИ РФ следует согласно постановлению Правительства РФ от 8 февраля 2018 г. №127[5]. После определения категории значимости объектов КИИ РФ возможно переходить к выбору процессов и мер обеспечения безопасности объектов КИИ РФ, руководствуясь приказом ФСТЭК России от 25 декабря 2017 г. №239[6]. В этом документе определены следующие группы мер обеспечения безопасности объектов КИИ РФ в соответствии с категорией значимости этих объектов:

- идентификация и аутентификация;
- управление доступом;
- ограничение программной среды;
- защита машинных носителей информации;
- аудит безопасности;
- антивирусная защита;
- предотвращение вторжений (компьютерных атак);
- обеспечение целостности;

[3]Указ Президента РФ от 15.01.2013 №31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации». URL: https://docs.cntd.ru/document/902392496 (дата обращения: 01.01.2022).

[4]Приказ ФСБ России от 24 июля 2018 г. №366 «О Национальном координационном центре по компьютерным инцидентам». URL: https://publication.pravo.gov.ru/Document/View/0001201809100001 (дата обращения: 01.01.2022).

[5]Постановление Правительства РФ от 8 февраля 2018 г. №127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений». URL: https://docs.cntd.ru/document/556499040 (дата обращения: 01.01.2022).

[6]Приказ ФСТЭК России от 25 декабря 2017 г. №239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации». URL: http://publication.pravo.gov.ru/Document/View/0001201803270041 (дата обращения: 01.01.2022).

- обеспечение доступности;
- защита технических средств и систем;
- защита информационной (автоматизированной) системы и ее компонентов;
- реагирование на компьютерные инциденты;
- управление конфигурацией;
- управление обновлениями программного обеспечения;
- планирование мероприятий по обеспечению безопасности;
- обеспечение действий в нештатных ситуациях;
- информирование и обучение персонала.

В приказе ФСБ России от 6 мая 2019 г. №196 представлены требования к средствам ГосСОПКА, средствам обнаружения, предупреждения и ликвидации последствий, средствам технические, программные, программно-аппаратные и иные средства поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов КИИ, средствам обмена и криптографическим средствам защиты информации, необходимой субъектам КИИ РФ в части реализации функций безопасности, визуализации, построения сводных отчетов и хранения информации[7].

Схематическое представление связи терминов и определений, представленных в нормативных правовых документах[2-7], приведено на рис. 1.

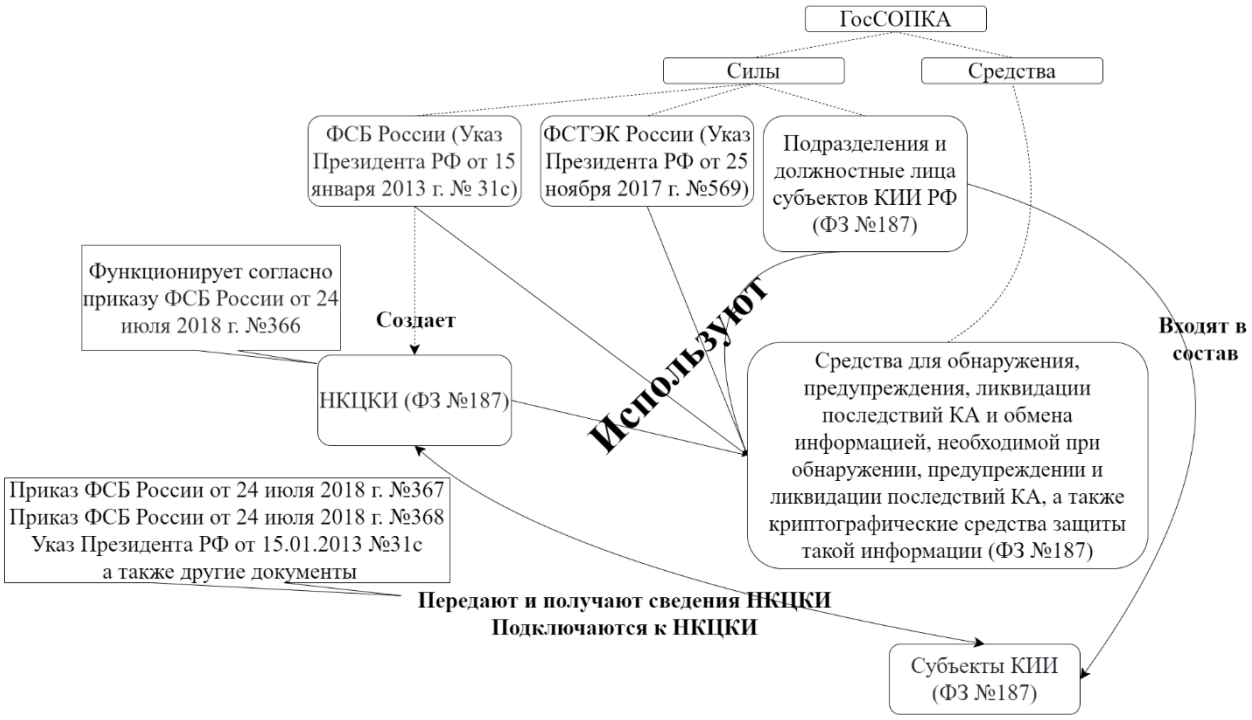

Рис. 1. Схематическое представление связи терминов и определений, представленных в нормативных правовых документах[2-7]
Fig. 1. Visual representation of the connection between terms and definitions presented in the regulatory legal documents[2-7]

[7]Приказ ФСБ России от 6 мая 2019 г. №196 «Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты». URL: https://docs.cntd.ru/document/554691438 (дата обращения: 01.01.2022).

3. ЦМБ как силы ГосСОПКА, их функции и требования к инфраструктуре

Задача автоматизации работ по обработке информации и событий информационной безопасности (ИБ) заключается в создании организацией собственного специализированного подразделения – центра мониторинга безопасности (ЦМБ) [12].

С организационной точки зрения ЦМБ – это централизованное подразделение, которое занимается вопросами мониторинга ИБ на организационном уровне, а также плюс созданная для обнаружения, анализа, подготовки отчетности и реагирования на инциденты ИБ группа, состоящая в основном из операторов, работающих с текущими данными, и аналитиков безопасности, которые выполняют углубленный анализ собранных данных[8]. Аналитики безопасности осуществляют анализ ранее не происходивших и неизвестных событий ИБ и новых уязвимостей, опираясь на различные источники и исторические данные самой организации (в случае ЦМБ срок давности таких данных обычно составляет от нескольких дней до месяца). У них должно быть четкое понимание локальной, региональной и глобальной среды и событий, которые могут повлиять на безопасность функционирования информационно-телекоммуникационных сетей (ИТКС) субъектов КИИ РФ и, как следствие, деятельности организации в целом. Штат ЦМБ зависит от сложности ИТКС организации.

С технической точки зрения – это детально разработанные процессы мониторинга ИБ ИТКС с предопределенными процедурами реагирования в конкретных ситуациях и взаимодействия с различными подразделениями внутри самой организации и другими структурами (в случае необходимости), а также арсенал специализированных средств для автоматизации такой деятельности

ЦМБ исключает потребность вручную искать, собирать, оценивать, классифицировать, анализировать и, в конечном счете, дифференцировать и связывать с ИБ данные, полученные из многочисленных гетерогенных источников в ИТКС организации[9]. Он непрерывно контролирует безопасность сетей, анализирует локально и дистанционно эксплуатируемые злоумышленниками уязвимости элементов ИТКС и может рассматриваться как ядро обеспечения сетевой безопасности в рамках ИТКС на операционном уровне управления сетью. ЦМБ как основа для осуществления дальнейшей деятельности по реагированию на инциденты ИБ централизованно собирает данные с сотен средств защиты информации (СЗИ) и обобщает их в единую картину состояния сетевой безопасности ИТКС, помогая персоналу ЦМБ быстро разобраться в текущей ситуации. Чтобы обеспечивать эти качества, ЦМБ в ИТКС должен работать в круглосуточном режиме и выполнять следующие типовые функции [13]:

- эксплуатационная поддержка функционирования ЦМБ с командной консолью, используемой для выполнения различных команд расширенного администрирования (повседневной эксплуатации и управления), поиска неисправностей и решения возникающих проблем силами самого субъекта КИИ РФ;
- отслеживания состояния активов ИТКС для их последующего восстановления после инцидентов ИБ;
- идентификация на основе результатов сканирования уязвимостей для последующего управления установкой обновлений для устранения найденных уязвимостей;

[8]Security Operations Center. 2015. URL: http://resources.infosecinstitute.com/security-operations-center/ (дата обращения: 30.12.2021).

[9]Security Operations Center: Building, Operating, and Maintaining your SOC. Cisco Press, 2015. URL:https://supportforums.cisco.com/sites/default/files/security_operations_center_9780134052014_ch_1_final__0.pdf (дата обращения: 30.12.2021).

● анализ сетевого трафика и информации о потоках данных для поиска любых сведений, которые могут быть полезны для выявления неисправностей и отклонений от штатного функционирования всех элементов ИТКС и, в конечном счете, обнаружения событий ИБ;

● мониторинг устройств и связь с системами управления их конфигурированием и централизованного управления СЗИ, предназначенными для автоматизации и полного контроля их жизненного цикла, включая единое управление процессами конфигурирования, настройки политик, оценки статуса, генерации отчетов о функционировании и т.д.;

● управление информацией о безопасности на основе сбора журналов регистрации событий (ЖРС), их хранения, архивирования и подготовки соответствующей отчетности, используемой далее для управления рисками ИБ и их ранжирования на основе анализа воздействия на бизнес, включая пассивную оценку и активную обработку рисков ИБ;

● обработка данных о событиях/инцидентах ИБ с непрерывной обратной связью и, при необходимости, эскалацией проблем на высшие уровни в организации;

● осуществление действий по сбору свидетельств компьютерных преступлений для реконструкции инцидента ИБ в ИТКС в признаваемом при судебном расследовании порядке, включая идентификацию, сбор, сохранение, восстановление, анализ и представление фактов.

Средства, которые должны использоваться для обеспечения работы ЦМБ (а, значит, и ЦУСБ) в достаточной мере описаны в Приказе Федеральной службы безопасности Российской Федерации от 06.05.2019 № 196[7].

Традиционные ЦМБ, работающие на основе правил, хорошо справлялись с задачей защиты от традиционных атак несколько лет назад. В настоящее время ИТКС как единое целое часто не является конечной целью злоумышленников; наоборот, их интересуют конечные устройства, поскольку ценные данные часто находятся именно там. Атаки характеризуются большей целенаправленностью, продуманностью, подготовленностью, использованием скрытых технологий взлома (например, APT-атаки и атаки на стороне клиента). Можно сделать вывод, что первые ЦМБ не были рассчитаны на растущие объемы данных, относящихся к ИБ современных гетерогенных ИТКС, и им не удавалось сохранять полный контроль над сложной сетевой ситуацией и поддерживать требуемый уровень ИБ ИТКС должным образом.

На основе анализа первоисточников, описывающих практический опыт внедрения и использования ЦМБ, были выявлены следующие серьезные ограничения их функциональных возможностей [14]:

● невозможность работы в крупномасштабных, гетерогенных, распределенных и сложно связанных ИТКС с подключением пользователей из любого места в любое время;

● ручная интеграция различных технологий защиты в едином ЦМБ;

● недостаточная гибкость и производительность ЦМБ для обработки больших объемов ранее накопленных (исторических), только что собранных и аналитически выведенных на их основе данных, известных как «технологии больших данных»;

● невозможность обеспечить высокую степень надежности/устойчивости при сборе, передаче и обработке данных о событиях ИБ, что делает их уязвимыми к атакам на SIEM-систему и сам ЦМБ;

● зависимость от централизованных правил корреляции, обрабатываемых на одном узле, что затрудняет масштабируемость, создает уязвимости и единую точку отказа;

● ограниченные возможности анализа, оценки и визуализации уровня ИБ, поскольку ЦМБ осуществляет мониторинг событий на сетевом уровне и поиск неисправностей во внутренних элементах ИТКС, а также обеспечивает не очень сложную корреляцию;

● невозможность интерпретации данных более высоких уровней, таких как данные об услугах или деятельности;

● отсутствие реакции на выявленные атаки в режиме реального времени; в дополнение к автоматизированным операциям аналитики ЦМБ должны оценивать в режиме реального времени большие объемы данных, что практически не осуществимо, и далее вручную реагировать на них.

На основе этих недостатков можно сформулировать требования к более функциональным, чем ЦМБ, ЦУСБ ИТКС организации, среди которых ключевыми являются следующие [11]:

● максимальная автоматизация рутинных операций не только по мониторингу ИБ, но и полноценному управлению инцидентами ИБ в ИТКС, приближающая реагирование на инциденты ИБ к режиму реального времени и по возможности предотвращающая их возникновение;

● создание полной видимости происходящего в ИТКС;

● анализ не только состояния, но и поведения всех элементов ИТКС и ее пользователей в определенном контексте для немедленного выявление отклонений по сравнению с нормальным поведением или функционированием, а не просто обнаружение на основе сигнатур, которые требуется постоянно обновлять и пополнять;

● поддержание требуемого организацией уровня ИБ в ИТКС в течение длительного времени без необходимости обращения к экспертам.

4. ЦУСБ как силы ГосСОПКА, их функции и требования к инфраструктуре

Центр управления сетевой безопасностью (ЦУСБ) является естественной эволюцией традиционного ЦМБ. Он решает проблемы ЦМБ путем объединения ЦМБ и концепции – интеллектуальной безопасности. Концепция интеллектуальной безопасности нашла свое воплощение в центре полноценного управления (а не просто мониторинга) ИБ ИТКС организации второго поколения – центре интеллектуальной безопасности (ЦИБ). Он имеет интегрированную архитектуру защиты от КА и объединяет полную прозрачность и контекстно-управляемый интеллект с действенным и всеобъемлющим пониманием и управлением знаниями в области ИБ[10], что позволяет постоянно контролировать ИБ ИТКС и связанных с ней элементов единого информационного пространства (ЕИП) организации. Внедряя ЦИБ, организация получает целостный и глубокий детальный взгляд на «здоровье» своей ИТКС и возможность не только обнаруживать и реагировать на атаки, но и результативно бороться с новыми угрозами ИБ, прежде чем они причинят вред, а также предотвращать инциденты ИБ, постоянно собирая и обобщая знания о сетевых атаках и уязвимостях в контексте конкретной ИТКС [9]. В России ЦИБ, использующий искусственный интеллект, был создан, например, в ПАО «Сбербанк России», в 2016 г., в результате чего количество рассматриваемых в день подозрительных событий в работе систем увеличилось до нескольких миллионов (до создания ЦИБ банку удавалось проанализировать лишь 100–200 инцидентов в день) [11].

[10]SOC vs. SIC: The Difference of an Intelligence Driven Defense® Solution. A White Paper. ITSECURITYNEWS. – Lockheed Martin Corporation, 2015. URL: https://www.itsecuritynews.info/soc-vs-sic-the-difference-of-an-intelligence-driven-defense-solution/ (дата обращения: 30.12.2021).

Как комплексное решение, ЦИБ с ИБ-аналитикой применительно к ИТКС организации в полном объеме сочетает в себе ряд интегрированных в единое целое технологий, а именно [14]:

- управление знаниями в области ИБ и содействие применению комплексного подхода к выявлению, сбору, оценке, поиску и обмену этими знаниями;
- обработка больших относящихся к ИБ данных в определенном контексте – с точки зрения любой возможной атаки для нахождения ее источника, установления ее типа, оценки последствий, визуализации направленности, выявления всех затронутых систем, приоритезации мер обеспечения ИБ и выработки предложений по нейтрализации последствий атаки;
- идентификация, отслеживание и восстановление всех элементов ИТКС после воздействия на них различных инцидентов ИБ;
- сбор данных из гетерогенных источников и управление ЖРС и учетными записями с учетом соблюдения соответствия определенным требованиям;
- централизация и агрегирование данных из разрозненных хранилищ с последующей нормализацией, корреляцией, категоризацией и анализом с применением SIEM-систем;
- визуализация уровня ИБ ИТКС и усовершенствованное (без использования статически заданных правил) обнаружение вторжений для выявления аномалий в поведении сети;
- управление рисками ИБ, сокращающее число инцидентов ИБ и обеспечивающее выполнение требований по обеспечению ИБ;
- весь цикл обработки инцидентов ИБ, заключающийся в обнаружении, оповещении, предоставлении отчетности, реагировании (включая антикризисные действия) и управлении эскалацией проблем на высшие уровни для принятия решений;
- сканирование уязвимостей с последующей реконфигурацией устройств и управлением изменениями и обновлениями;
- анализ сетевого трафика и приложений, поддерживаемый межсетевыми экранами следующего поколения (NGFW) и инструментами для расследования инцидентов ИБ.

Со своим ЦИБ организация может реализовать персонифицированное (индивидуальное) в контексте ее деятельности управление инцидентами ИБ для ИТКС. Образно говоря, если ЦМБ – это «глаза мониторинга инцидентов ИБ», то ЦИБ – это «мозг управления инцидентами ИБ с широко открытыми глазами» [15], поскольку при осуществлении управления инцидентами ИБ собранные данные о реальном уровне ИБ всей ИТКС и ее отдельных элементов и принятые обоснованные решения по корректировке этого уровня должны использоваться для реагирования на инциденты ИБ.

Учитывая все ранее выявленные возможности и ограничения ЦМБ и ЦИБ, можно определить основные характеристики ЦУСБ, который:

- функционирует на основе сценариев инцидентов ИБ и моделирования процесса «охоты за угрозами»;
- способен обнаруживать не только типовые и целенаправленные атаки, но и усложненные угрозы ИБ и атаки «нулевого дня»;
- производит обнаружение на основе разработки сценариев, исторических данных, машинного обучения и «охоты за угрозами», а также агрегированных внутренних и внешних потоков;

- реагирует упреждающее, в основном автоматизированное реагирование за счет автоматизации выполнения критически важных задач на основе специальных программных модулей (скриптов);
- сопровождает инциденты ИБ на протяжении всего заранее смоделированного периода его развития с постоянной коррекцией и настройкой поиска связанных с инцидентом данных в зависимости от получаемых результатов его расследования;
- устанавливает время реагирования на инциденты ИБ в документах и в реальности зависящее от его последствий, включая время, требуемое на коррекцию поиска связанных с инцидентом данных;
- состоит из специализированных лабораторий для разработки сценариев инцидентов и выполнения тестирования защищенности;
- орудует средствами расширенного поиска, агрегирования данных от всех источников и управления ими;
- дополнительно имеет в распоряжении специализированные средства для обнаружения угроз ИБ, поиска данных и реализации сценариев детального целенаправленного исследования угроз ИБ (Threat Hunting);
- работает постоянно в режиме реального/близкого к реальному времени обнаружения и реагирования;
- состоит из персонала, обладающего навыками моделирования и глубокого анализа корреляций всех собираемых данных и коррекций поиска новых данных;
- осуществляет визуализацию в режиме «жесткого» реального времени.

Следовательно, для того, чтобы соответствовать данным характеристикам, деятельность ЦУСБ должна определяться, но не ограничиваться следующими общими требованиями:

1. Вся деятельность ЦУСБ организации должна быть выстроена и реализована согласно требованиям, изложенным в применимых нормативных, правовых, отраслевых и других документах.
2. ЦУСБ должен представлять собой комплекс систем (подсистем), технических и программных средств, технологически и организационно объединенных каналами передачи информации различной физической природы, позволяющих обеспечить автоматизацию процесса управления инцидентами информационной безопасности (ПУИИБ) организации, включая реагирование на инциденты ИБ, за счет централизованной обработки связанной с ИБ ИТКС информации, а также предоставляющий услуги и средства связи для персонала, вовлеченного в ПУИИБ.
3. Единство и скоординированность функционирования ЦУСБ с ИТКС организации.
4. ЦУСБ должен быть системообразующим элементом системы обеспечения ИБ организации на основе жесткой связи с ней, влиять на ее развитие и совершенствование.
5. Наличие необходимой организационной структуры и органа управления ЦУСБ, основными задачами которого является администрирование управления, управление ходом функциональных процессов, оперативный контроль состояния, оперативный контроль над устранением сбоев в функционировании и информационно-аналитическое обеспечение управления совершенствованием и развитием ЦУСБ.
6. Интеграция информационных и телекоммуникационных сетей, ресурсов и услуг ЦУСБ в единую систему.
7. Применение современных средств технического, программного, информационного, аналитического, организационного и документального обеспечения, функционально объединенных в ЦУСБ.

Вышеуказанные требования являются отправной точкой для развития ЦУСБ, однако для совершенствования его функционирования предлагается использовать также и специальные требования:

1. Создание и непрерывное развитие ЦУСБ как единой экосистемы (сложной динамической системы взаимосвязанных элементов в ЕИП организации, а не просто единой платформы) для обмена информацией об ИБ ИТКС и совместных скоординированных действий по обнаружению, расследованию и предотвращению инцидентов ИБ, а также упреждающего управления сетевой безопасностью ИТКС и обучения на полученном опыте как различных подразделений организации, так и ее бизнес-партнеров, регуляторов, аудиторов и т.п.

2. Управляемость ЦУСБ с централизованной архитектурой и распределенной/ децентрализованной работой отдельных процессов при совмещении масштабируемости и эластичности сбора, хранения, первичной обработки и корреляции данных для его функционирования в изменяющейся среде осуществления деятельности организации и при появлении новых угроз ИБ в ЕИП для ее ИТКС.

3. Согласованность процессов, поддерживающих функционирование ЦУСБ, со всеми передовыми практиками и применимыми к ИТКС организации требованиями по обеспечению ИБ, определенными в международных и российских законах и подзаконных нормативных правовых актах, а также региональными и ведомственными документами.

4. Расширенная ИБ-аналитика и использование для нее как можно большего количества типов данных, поскольку по-прежнему недостаточно навыков и методов обработки неструктурированных данных в состоянии покоя, например данных из ОЗУ конечных устройств, данных от мобильных устройств, виртуальных и облачных сред.

5. Адаптивное управление событиями ИБ в ИТКС, поддерживаемое за счет применения предсказательного определения возможных тенденций в области обеспечения ИБ в ЕИП организации и типовых модульных и конфигурируемых СЗИ, сетевых устройств, протоколов, процессов и мер обеспечения сетевой безопасности, что должно обеспечить повторяемость (тиражируемость) всех процессов управления сетевой безопасностью при их использовании в различных ЦУСБ.

6. Функциональная устойчивость ЦУСБ в штатном режиме, в условиях направленных на него КА, при сбоях повышенной степени серьезности и в условиях чрезвычайных ситуаций (способность регулировать функционирование с целью поддержания выполнения операций при ожидаемых условиях и при ужесточении требований, нарушениях и непредвиденных обстоятельствах, например, способность адаптироваться к изменяющимся шаблонам компьютерных атак или условиям осуществления деятельности на основе ИТКС при внедрении новых ИКТ [16]) для обеспечения долгосрочной постоянной доступности и других важных свойств ИБ для ИТКС и всех ее элементов, аппаратного (АО) и программного обеспечения, предоставляемых ИТ-услуг, информационных потоков, знаний и баз данных и т.д., что исключит единую точку отказа.

7. Масштабируемость ЦУСБ (мера способности ИТКС к увеличению/уменьшению производительности и затрат в ответ на изменения в его потребностях в АО, приложениях, системах обработки данных и т.п.[11]) для сбора и обработки огромного количества событий из различных гетерогенных внутренних и внешних (типа Threat Intelligence) по отношению к ИТКС источников, что все вместе определяет необходимость

[11]IT Glossary. GARTNER. URL: https://blogs.gartner.com/it-glossary/operational-resilience/ (дата обращения: 30.12.2021).

применения ИТ больших данных и использования продвинутых технологий для их хранения.

8. Эластичность (способность системы с течением времени увеличивать нагрузку на свои текущие и дополнительные динамически и автоматически добавляемые по требованию вычислительные ресурсы[12]) для распределенных и реализуемых в режиме реального/близкого к реальному времени агрегирования, пакетной и потоковой обработки и передачи гибридных относящихся к ИБ больших данных.

9. Гибкость при использовании необходимых методов и инструментов ИБ-аналитики таким образом, чтобы персонал ЦУСБ мог использовать при обработке все доступные в тот момент данные (включая исторические за длительный период времени) и получать результаты, учитывающие разные точки зрения.

10. Собственная защищенность и надежность ЦУСБ, включая защищенность его инфраструктуры и процессов обработки данных, а также безопасность всех обрабатываемых в нем связанных с ИБ больших данных и хранимых входные и выходные данных процессов, а также надежность управления, поступающими в ЦУСБ из надежных источников.

11. Прозрачность для руководства организации всей деятельности ЦУСБ для принятия своевременных управленческих решений.

Заключение

В данной работе ЦУСБ описаны как силы ГосСОПКА, определены функции ЦУСБ и требования к его инфраструктуре в соответствии с требованиями, предъявляемыми субъектам КИИ РФ для обеспечения безопасности объектов КИИ РФ.

Полученные результаты позволят не только наладить взаимодействия с центром ГосСОПКА в соответствии с требованиями законодательства РФ, но и помогут специалистам информационной безопасности в построении организационного объекта, который может заниматься вопросами противодействия компьютерным атакам, обнаружении и реагировании на инциденты круглосуточно в единой централизованной системе с возможностью непрерывного развития как самого ЦУСБ, так и его интегрированности в процессы и инфраструктуру организации.

Кроме того, с применением указанных основных и дополнительных требований, имеется возможность проведения дальнейших исследований для определения структуры ЦУСБ, его программно-аппаратного обеспечения

Предложенные требования являются начальными и могут быть дополнены при их внедрении для обеспечения безопасности объектов КИИ РФ на достаточном с точки зрения нормативных документов РФ по данному вопросу.

СПИСОК ЛИТЕРАТУРЫ:

1. Лобач Д.В., Смирнова Е.А. Состояние кибербезопасности в России на современном этапе цифровой трансформации общества и становление национальной системы противодействия киберугрозам. Территория новых возможностей. Вестник Владивостокского Государственного Университета Экономики и Сервиса. Т. 11, № 4, с. 23–32, 2019. DOI: http://dx.doi.org/10.24866/VVSU/2073-3984/2019-4/023-032.
2. Швыряев П.С. Киберпреступность в России: новый вызов для общества и государства. Государственное управление. Электронный вестник. № 89, с. 184–196, 2021. DOI: http://dx.doi.org/10.24412/2070-1381-2021-89-184-196.

[12]Cyber Security: Security Operations Center (SOC) vs. Network Operations Center (NOC). INTELLECTUALPOINT. 2016. URL: https://www.intellectualpoint.com/blog/cyber-security-security-operations-center-soc-vs-network-operations-center-noc/ (дата обращения: 30.12.2021).

3. Ванцева И.О., Зырянова Т.Ю., Медведева О.О. Влияние федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» на владельцев критических информационных инфраструктур. Вестник УРФО. Безопасность в информационной сфере. № 4, с. 71–76, 2018. ISSN 2225-5435. URL: http://info-secur.ru/is_1_2018.pdf. (дата обращения: 01.01.2022).
4. Деева Т.В. Создание единой системы противодействия кибератакам: ответ на большие вызовы и угрозы налоговой безопасности страны. Проблемы рыночной экономики. № 4, с. 100–112, 2020. ISSN 2500-2325. URL: https://www.elibrary.ru/item.asp?id=44682826 (дата обращения: 08.01.2022).
5. Заворина Л.Д., Селифанов В.В. Разработка системы защиты информации значимого объекта критической инфраструктуры Российской Федерации. Сборник научных трудов Новосибирского Государственного Технического Университета. № 1, с. 123–131, 2018. ISSN 2307-6879. URL: https://www.elibrary.ru/item.asp?id=39157958. (дата обращения: 08.01.2022).
6. Гавдан Григорий П., Иваненко Виталий Г., Салкуцан Алексей А. Обеспечение безопасности значимых объектов КИИ. Безопасность информационных технологий, [S.l.], т. 26, № 4, с. 69–82, 2019. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2019.4.05.
7. Зырянова Т.Ю. Анализ требований третьей категории значимости объектов КИИ в инфраструктуре предприятия. Вестник УРФО. Безопасность в информационной сфере. № 3, с. 69–72, 2019. ISSN 2225-5435. URL: https://www.elibrary.ru/item.asp?id=41151823 (дата обращения: 08.01.2022).
8. Козьминых С.И. Взаимодействие объектов топливно-энергетического комплекса с ГосСОПКА. Информационные ресурсы России. № 1, с. 2–7, 2020. ISSN 0204-3653. URL: https://www.elibrary.ru/item.asp?id=42512104 (дата обращения: 08.01.2022).
9. Каннер Татьяна М. Особенности повышения квалификации специалистов по обеспечению безопасности значимых объектов критической информационной инфраструктуры. Безопасность информационных технологий, [S.l.], т. 26, № 3, с. 22–31, 2019. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2019.3.02 (дата обращения: 01.01.2022).
10. Кузнецов С.А., Куликов И.А., Фоминых А.А. Сравнение КИИ и методов категорирования КИИ в РФ и США. Актуальные научные исследования в современном мире. № 6–1, с. 63–68, 2021. ISSN 2524-0986. URL: https://www.elibrary.ru/item.asp?id=46326396 (дата обращения: 08.01.2022).
11. Милославская Н.Г. Построение центров управления сетевой безопасностью в информационно-телекоммуникационных сетях. М.: Горячая линия-Телком. 2020. – 461 с.
12. Bidou Renaud. Security Operation Center Concepts & Implementation. 2005. URL: http://iv2-technologies.com/~rbidou/SOCConceptAndImplementation.pdf (дата обращения: 30.12.2021).
13. Наташова Кристина В. и др. К вопросу о категорировании объектов критической информационной инфраструктуры морских портов. Безопасность информационных технологий, [S.l.], т. 27, № 2, с. 35–46, 2020. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2020.2.03.
14. Miloslavskaya Natalia G. Information Security Management in SOCs and SICs. Journal of Intelligent & Fussy Systems. Vol. 35, no. 3, p. 2637–2647, 2016. ISBN 1875-8967. URL: https://www.elibrary.ru/item.asp?id=38633644 (дата обращения: 09.01.2022).
15. Милославская Наталья Г. Центры управления информационной безопасностью. Безопасность информационных технологий, [S.l.], т. 23, № 4, с. 38–51, 2016. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/257 (дата обращения: 09.01.2022).
16. Лебедев Павел. Сбербанк обезопасит себя с помощью искусственного интеллекта. 2016. URL: https://banks.cnews.ru/news/top/2016-06-10_sberbank_obezopasit_sebya_s_pomoshchyu_iskusstvennogo (дата обращения: 30.12.2021).

REFERENCES:

[1] Lobach D.V., Smirnova E.A. The state of cybersecurity in Russia at the present stage of the digital transformation of society and the formation of a national system for countering cyber threats. A territory of new opportunities. Vladivostok State University of Economics and Service Bulletin. Vol. 11, no. 4, p. 23–32, 2019. DOI: http://dx.doi.org/10.24866/VVSU/2073-3984/2019-4/023-032 (in Russian).
[2] Shvyryaev P.S. Cybercrime in Russia: a new challenge for society and the state. State Administration. Electronic Bulletin. No. 89, p. 184–196, 2021. DOI: http://dx.doi.org/10.24412/2070-1381-2021-89-184-196 (in Russian).
[3] Vantseva I.O., Zyryanova T.Y., Medvedeva O.O. The impact of the federal law «On the security of the critical information infrastructure of the Russian Federation» on the owners of critical information infrastructures.

Bulletin of the Ural Federal District. Information security. No. 4, p. 71–76, 2018. ISSN 2225-5435. URL: http://info-secur.ru/is_1_2018.pdf (accessed: 01.01.2022) (in Russian).

[4] Deeva T.V. Creation of a unified system of countering cyberattacks: a response to major challenges and threats to the country's tax security. Market economy problems. No. 4, p. 100–112, 2020. ISSN 2500-2325. URL: https://www.elibrary.ru/item.asp?id=44682826 (accessed: 08.01.2022) (in Russian).

[5] Zavorina L.D., Selifanov V.V. Development of an information protection system for a significant object of the critical infrastructure of the Russian Federation. Collection of scientific papers of the Novosibirsk State Technical University. No. 1, p. 123–131, 2018. ISSN 2307-6879. URL: https://www.elibrary.ru/item.asp?id=39157958 (accessed: 08.01.2022) (in Russian).

[6] Gavdan Grigory P., Ivanenko Vitaly G., Salkutsan Aleksey A. Ensuring the safety of significant objects of the KII. Information Technology Security, [S.l.], vol. 26, no. 4, p. 69–82, 2019. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2019.4.05 (in Russian).

[7] Zyryanova T.Y. Analysis of the requirements of the third category of importance of CII objects in the enterprise infrastructure. Bulletin of the Ural Federal District. Information security. No. 3, p. 69–72, 2019. ISSN 2225-5435. URL: https://www.elibrary.ru/item.asp?id=41151823 (accessed: 08.01.2022) (in Russian).

[8] Kozmins S.I. Interaction of objects of the fuel and energy complex with GosSOPKA. Information resources of Russia. No. 1, p. 2–7, 2020. ISSN 0204-3653. URL: https://www.elibrary.ru/item.asp?id=42512104 (accessed: 08.01.2022) (in Russian).

[9] Kanner Tatyana M. Peculiarities of advanced training of specialists in ensuring the security of significant objects of critical information infrastructure. Information Technology Security, [S.l.], vol. 26, no. 3, p. 22–31, 2019. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2019.3.02 (in Russian).

[10] Kuznetsov S.A., Kulikov I.A., Fominykh A.A. Comparison of CII and CII categorization methods in the Russian Federation and the USA. Actual scientific research in the modern world. No. 6-1, p. 63–68, 2021. ISSN 2524-0986. URL: https://www.elibrary.ru/item.asp?id=46326396 (accessed: 08.01.2022) (in Russian).

[11] Miloslavskaya N.G. Designing Network Security Centers in Information and Telecommunication Networks. M.: Hotline-Telcom. 2020. – 461 p. (in Russian).

[12] Bidou Renaud. Security Operation Center Concepts & Implementation. 2005. URL: http://iv2-technologies.com/~rbidou/SOCConceptAndImplementation.pdf (accessed: 30.12.2021).

[13] Natashova Kristina V. et all. On the issue of categorization of objects of critical information infrastructure of seaports. Information Technology Security, [S.l.], vol. 27, no. 2, p. 35–46, 2020. ISSN 2074-7136. DOI: http://dx.doi.org/10.26583/bit.2020.2.03 (in Russian).

[14] Miloslavskaya N.G. Information Security Management in SOCs and SICs. Journal of Intelligent & Fussy Systems. Vol. 35, no. 3, p. 2637–2647, 2016. ISBN 1875-8967. URL: https://www.elibrary.ru/item.asp?id=38633644.

[15] Miloslavskaya Natalia G. Information Security Operations Centers. IT Security (Russia), [S.l.], vol. 23, no. 4, p. 38–51, 2016. ISSN 2074-7136. URL: https://bit.mephi.ru/index.php/bit/article/view/257 (accessed: 09.01. 2022) (in Russian).

[16] Lebedev Pavel. Sberbank Will Protect Itself with the Help of Artificial Intelligence. 2016. URL:https://banks.cnews.ru/news/top/2016-06-10_sberbank_obezopasit_sebya_s_pomoshchyu_iskusstvennogo (accessed: 30.12.2021) (in Russian).

Поступила в редакцию – 05 января 2022 г. Окончательный вариант – 17 февраля 2022 г.
Received – January 05, 2022. The final version – February 17, 2022.