МНОГОЛИКОСТЬ МОНИТОРИНГА В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Метельков А.Н.[1]

Ключевые слова*: наблюдение, контроль, информация, информационные ресурсы, безопасность, защищенность.*

Аннотация

Целью статьи *является исследование категории «мониторинг» в различных аспектах её использования применительно к сфере информации и информационной безопасности.*

Метод исследования*: в работе автором использован системно-структурный подход к анализу содержания понятия «мониторинг», метод сравнения множеств, объединяющих объекты мониторинга.*

Результат: *в работе исследованы различные виды объектов мониторинга и подходы к содержательному наполнению мониторинга.*

Проанализирован опыт развитых зарубежных стран в применении непрерывного мониторинга безопасности информационных систем. Предложена модель соотношения различных видов мониторинга. В результате с применением графического изображения множеств с помощью диаграмм Эйлера — Венна разработана модель взаимодействия мониторинга информационной безопасности, мониторинга информации, мониторинга защищенности информационных ресурсов и мониторинга безопасности информации.

Практическая ценность: *представленная модель соотношения различных видов мониторинга в зависимости от его объекта является оригинальным результатом, дополняющим существующие представления о предмете мониторинга в информационной среде. Разграничение мониторинга по объекту мониторинга позволяет на практике дифференцированно подходить к реализации мер во исполнение требований государственных регуляторов в сфере обеспечения информационной и функциональной безопасности.*

DOI: 10.24412/1994-1404-2025-4-69-78

Введение и постановка задачи

В современных условиях объект защиты принимает более сложный вид и отхватывает данные и «системы их передачи, обработки и хранения; системы управления; средства защиты; а также их динамически изменяющиеся взаимосвязи» [1, с. 4]. Одними из таких объектов являются киберфизические системы, которые объединят взаимодействующие сложносоставные киберфизические объекты, включающие набор взаимосвязанных физических, информационных компонент и коммуникационную среду [2]. В действующем законодательстве особое внимание уделяется обеспечению защищенности информационных ресурсов (ИР), включающих информационные системы, информационно-телекоммуникационные сети (ИТКС) и автоматизированные системы управления (АСУ). Мониторинг защищенности ИР служит важным средством обеспечения информационной безопасности (ИБ) и включает в себя постановку и решение задач, связанных с устойчивостью функционирования систем и сетей. В стандартах ГОСТ Р 59390-2021, ГОСТ Р МЭК 61513—2020 и ИСО/МЭК 12207:2008 защищенность, ИБ, кибербезопасность рассматриваются синонимично и узко таргетировано. Вследствие этого они вступают в противоречие с современными представлениями о защищённости ИР. Согласно научно обоснованным и установленным стандартам (ГОСТ Р 59709—2022, п. 3.2.7; ГОСТ Р ИСО/МЭК 27001-2006, п.3.6; ГОСТ Р ИСО/МЭК ТО 18044-2007, п.3.6) отказы технических средств признаются инцидентами ИБ, то есть являются предметом мониторинга ИБ. Одновременно, что особенно характерно для киберфизических систем, такие отказы оборудования охватываются функциональной безопасностью. Член-корреспондент РАН Д.П. Зегжда обоснованно полагает, что формальное описание процесса оценки безопасности состояния системы в динамике связано с единовременным мониторингом «информационной и функциональной безопасности» [3, с. 107].

[1] ***Метельков Александр Николаевич,*** *кандидат юридических наук, доцент, доцент кафедры прикладной математики и безопасности информационных технологий Санкт-Петербургского университета ГПС МЧС России, Санкт-Петербург, Россия. ORCID: 0000-0002-6113-8981.*

E-mail: metelkov5178@mail.ru

В рамках работы решаются задачи сравнительного анализа отдельных видов мониторинга в сфере обеспечения ИБ, систематизации отношения понятий «мониторинг информации», «мониторинг ИБ», «мониторинг безопасности информации» и «мониторинг защищённости ИР» и построения аналитической модели их взаимодействия, а также определения с помощью качественного анализа содержания мониторинга информации и его места среди других выделенных видов мониторинга.

Виды мониторинга в обеспечении ИБ

Содержание мониторинга во многом определяется его объектом, который может включать информацию, ИР и их защищенность, ИБ, в том числе информационных (автоматизированных) систем (ИС (АС)). В отдельных аспектах такие виды мониторинга могут частично совпадать, потому что информация пронизывает все объекты мониторинга. В любой современной автоматизированной системе присутствуют ключевые средства защиты, позволяющие реализовать различные задачи обеспечения ИБ путем защиты ИР[2]. Мониторинг превращает обеспечение ИБ систем и сетей в управляемый процесс с наблюдаемостью, измеримыми метриками и предсказуемым реагированием. Системы мониторинга ИБ развиваются от средств оценки соответствия до части системы управления средствами контроля и безопасности в направлении разработки интеллектуальных систем безопасности, в функции которых кроме сбора данных о текущих событиях и инцидентах ИБ входит «анализ состояния объекта защиты, принятие оперативных мер, сигнализация о действиях, включая аварийные» [4, с. 15].

В целях управления безопасностью информационной инфраструктуры в организации создается специальное подразделение — Центр управления безопасностью (SOC), который в литературе называют центром мониторинга ИБ (ЦМИБ, Security Operation Center). Некоторые авторы [4, с. 50] под ЦМИБ понимают совокупность инструментов SIEM и SOC. В работе [5, с. 83] отмечено, что в качестве базовой платформы для организации SOC, как правило, выступает система мониторинга событий ИБ (SIEM — Security Information and Event Management). Организационно-технические процедуры ЦМИБ направлены на обнаружение и предотвращение киберугроз с учетом ключевых принципов проактивной защиты как сочетания тактической и стратегической аналитики на основе инженерии знаний и интеллектуальной обработки гетерогенных слабоструктурированных данных, получаемых из внутренних и внешних источников [6]. SOC решает ряд задач, включая непрерывный мониторинг систем, устройств и сетей касательно существования признаков нарушения безопасности или иных угроз. Для сбора и анализа данных SOC использует продукты SIEM, системы обнаружения вторжений и журналы межсетевых экранов. В числе основных задач SOC называют выстраивание процессов мониторинга, обнаружения, реагирования на инциденты ИБ. Например, в США Министерство юстиции назначено федеральным поставщиком услуг для центров безопасности (SOC), поддерживающим общеправительственные инициативы по консолидации и совместному использованию услуг. ИТ-услуги предоставляют полный набор комплексных услуг кибербезопасности, которые защищают объекты информатизации от угроз и укрепляют их киберзащиту. Услуги основаны на передовых технологиях, используемых специалистами по кибербезопасности, что обеспечивает интеграцию информации об угрозах. Все услуги подкреплены службой поддержки клиентов. SOC предоставляет услуги по предотвращению и обнаружению инсайдерских угроз (ITPD), управлению уязвимостями, тестированию на проникновение, оценке киберугроз, поддержке программы борьбы с фишингом, доверенному интернет-соединению (JCOTS), поддержке политики кибербезопасности, управлению рисками цепочки поставок (SCRM), оценке и управлению кибербезопасностью (CSAM). Центры предлагают технические услуги по кибербезопасности, услуги специалиста по безопасности информационных систем (ISSO), дают независимые оценки контроля безопасности, а также оказывают услуги по управлению, рискам и обеспечению соответствия. В распределенных СОА/СОВ (Intrusion Detection System, IDS) — программная или аппаратно-программная система сетевой безопасности, предназначенная для обнаружения сетевых атак и различных аномалий, непрерывного мониторинга сетевой активности в пределах клиентской информационной инфраструктуры реализуется подсистемой (IK) сбора и предобработки данных сетевых сессий [7, с. 121].

Мониторинг служит связующим звеном между превентивными мерами и реагированием, обеспечивающим прозрачность реально происходящих событий в ИТ-ландшафте, обеспечивает раннее обнаружение событий ИБ до их перехода в состояние инцидента, приоритизацию событий, доказательственную основу, создание предпосылок для улучшения защищенности ИР путем корректировки политик, процессов, мер и средств защиты. К наполнению содержания мониторинга существует несколько подходов, три из которых представлены на рисунке 1.

Анализ является значимой составляющей содержания мониторинга, который представляет собой фиксацию фактов, зеркальное отражение происходящих процессов, аналитику и оценку, позволяющих «формировать выводы и предложения, выстраивать прогнозы, планы, сценарии развития»[3]. Взгляд, в котором

[2] Кульба В.В., Шелков А.Б., Гладков Ю.М., Павельев С.В. Мониторинг и аудит информационной безопасности автоматизированных систем. М. : Ин-т проблем управления им. В.А. Трапезникова РАН, 2009. 94 с. С.66.

[3] Масленникова Н.Ю., Слинкова О.К. Понятие и сущность мониторинга с позиции системного подхода // Science Time. 2014. № 6. С. 113.

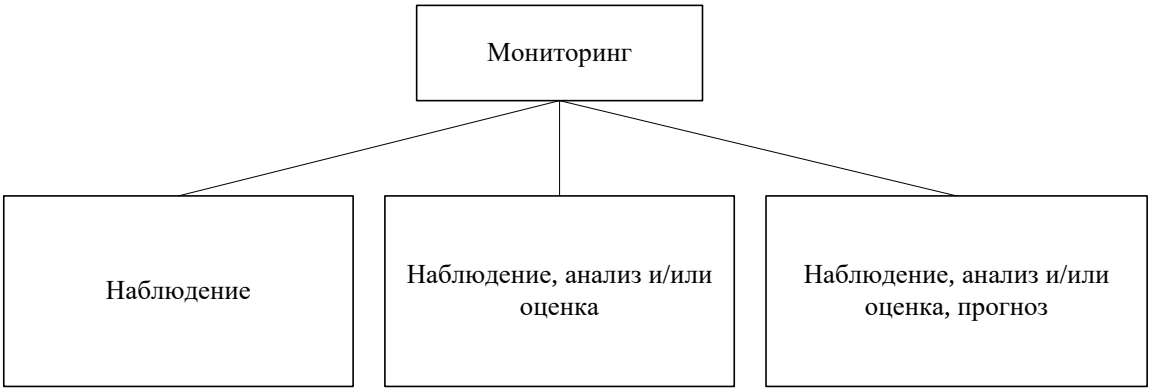

Рис. 1. Подходы к составу мониторинга

прогностический компонент включается в мониторинг, слабо обоснован, так как прогнозирование является начальным этапом планирования, имеющего самостоятельное значение. В законодательстве[4] под термином «мониторинг» понимается режим государственного контроля, предусматривающий целенаправленное, постоянное (систематическое, регулярное, непрерывное), опосредованное получение и анализ «информации о деятельности граждан и организаций, об объектах контроля с использованием систем (методов) дистанционного контроля, … в целях предотвращения причинения вреда (ущерба) охраняемым законом ценностям».

Для задач мониторинга используются различные способы (программно-аппаратный, неавтоматизированный, смешанный) и средства. Источниками данных мониторинга ИБ выступают средства защиты информации, программное обеспечение, программно-технические средства, информационные сервисы, среда функционирования ИС (АС), персонал оператора ИС (АС) [8, с. 17]. Однако само понятие ИБ (InfoSec) специалистами интерпретируется по-разному. Например, штатными писателями компании IBM Think трактуется в узком смысле как защита важной информации от несанкционированного доступа, раскрытия, использования, изменения или нарушения работы [9].

Мохаммед Абу Ламдди в статье [10] обоснованно констатирует, что стремительное внедрение технологий в различные сферы жизни сделало их доступными и привело к более широкому распространению в обществе. По мере развития технологий почти все системы подключаются к сети, включая инфраструктуру, автомобили, самолёты, предприятия химической отрасли, электростанции и другие критически важные системы. Поэтому из-за сильной зависимости от технологий в большинстве, если не во всех сферах жизни, сбой системы считается серьёзной проблемой, которая может нанести вред окружающей среде, поставить под угрозу жизнь людей и прекращение выполнение каких-либо функций. Концептуальная основа интеграции безопасности и защищённости, реализованная в модели предметной области SaS (безопасность и защищённость), позволяет осуществлять мониторинг как безопасности, так и защищенности ИС, АСУ и ИТКС.

Основные компоненты систем мониторинга ИБ включают такие классы решений, как: SIEM-системы (Security Information and Event Management), осуществляющие централизованный сбор, нормализацию и корреляцию событий из различных источников; IDS/IPS — системы обнаружения и предотвращения вторжений, фиксирующие подозрительный трафик и блокирующие его «на лету» по сигнатурам и правилам; EDR (Endpoint Detection and Response) технологии, предназначенные для мониторинга, обнаружения и реагирования на угрозы на конечных устройствах, наблюдения за поведением на рабочих станциях/серверах; XDR (Extended Detection and Response) технологии расширенного обнаружения и реагирования, защищающие ИТ-инфраструктуру и нацеленные на противодействие сложным кибератакам; класс решений NDR (Network Detection and Response), обеспечивающие анализ сетевых угроз в режиме реального времени и дополняющие сигнатурные методы; DLP (Data Loss Prevention) технологии, предоставляющие возможность наблюдения за перемещением чувствительных данных, контроль политик по безопасности служебной информации ограниченного распространения, персональных данных, коммерческой тайны; класс программных решений SOAR (Security Orchestration, Automation and Response), оркестрирующий системы безопасности, координации и управления ими, обеспечивающие автоматизацию рутинных операций при реагировании (изоляция хоста, блокировка учётной записи и т. п.); сканеры уязвимостей, осуществляющие инвентаризацию активов и оценку уязвимостей, приоритизацию исправлений; журналы событий реализующие процедуры сбора, хранения и доступа к логам (включая облака и SaaS); UBA/UEBA — системы поведенческого анализа, моделирующие правила для пользователей (объектов,

[4] Федеральный закон от 31.07.2020 N 248-ФЗ (ред. от 24.06.2025) «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации» // Собрание законодательства Российской Федерации. 2020. № 31. Ч. I. Ст. 5007.

сервисов); TIP (Threat Intelligence Platform) — платформы, агрегирующие индикаторы компрометации, обогащающие алерты и выполняющие автоматическую трансляцию сигналов в средства защиты.

Фактором, снижающим эффективность мониторинга защищенности ИР, является неопределённость и размытость понимания ИР [11,12], которое в российском законодательстве о безопасности критической информационной инфраструктуры трактуется широко. В федеральном законодательстве США (44 U.S.C., раздел 3502), наоборот, дискретный набор ИР включен как составляющий компонент в определение ИС.

Нечеткое отражение ИР, соединясь с представлениями о разнообразных видах мониторинга в информационной сфере, становится препятствием на пути решения насущных задач в обеспечении ИБ, являющейся согласно Стратегии национальной безопасности Российской Федерации (п.26) стратегическим национальным приоритетом.

Многоликость мониторинга в сфере обеспечения ИБ заключается в том, что его объектом могут быть различные явления: информация, ИБ, ИБ в ИС, безопасность информации, защищённость ИР и т. п. Федеральным законом от 5 декабря 2022 г. № 478-ФЗ введена статья 16.2, в которой содержится норма права, направленная на регулирование мониторинга ИТКС. Оригинальное правое решение реализовано в Положении о мониторинге информации и контроле потенциальных каналов утечки данных в МЧС России (Положение), утвержденном приказом МЧС России от 20.02.2025 г. № 725. В нем, в частности, термин «мониторинг информации …» по содержанию во многом совпадает с термином «мониторинг ИБ», установленным в стандартах ГОСТ Р 59547—2021 и ГОСТ Р 59709—2022. Сравнительнй анализ показывает, что вместо широкого по объему понятия «событие безопасности» в Положении используется более узкий термин «Событие ИБ», а в содержание «мониторинга информации…» не введена задача выявления уязвимостей. Включение в предмет наблюдения и анализа «других» данных размывает определённость рассматриваемого термина в Положении. В «мониторинге информации…» содержание термина мыслится как наблюдение и анализ результатов «регистрации Событий ИБ», что резко сужает по объему объект наблюдения: от информации до результатов регистрации Событий ИБ. Существенным недостатком, на наш взгляд, является изменение объекта мониторинга. Вместо «ИБ» или компонентов, ее составляющих, в качестве объекта мониторинга предлагается предельно широкая, многозначная и многоаспектная категория «информация». Под информацией, как писал академик РАН СССР В.Г. Афанасьев, обычно понимаются сведения «об окружающем мире, о внутреннем состоянии системы и внешних условиях, которые управляющая система использует в осуществлении управленческих процессов» [13, с. 26]. Добавление к мониторингу термина «информация» подчеркивает, что входом в мониторинговую систему наряду с инструментальными данными являются сведения, получаемые в результате обмена информацией, неструктурированные и иные данные. В ГОСТ Р 59547—2021 мониторинг ИБ также рассматривается как процесс постоянного наблюдения и анализа результатов регистрации событий безопасности с целью выявления нарушений безопасности информации, угроз безопасности информации и уязвимостей.

В современных исследованиях внимание уделяется мониторингу «сетей промышленного Интернета вещей» [14, с. 5], «состояния объектов» [14, с. 6], целостности данных [15, с. 8], ИБ, «событий ИБ» [16], событий сетевой активности [17], безопасности системы защиты информации [18], состояния ИБ, ИБ автоматизированных систем, компьютерных сетей, безопасности системы защиты КИИ и т. п. Многообразие видов мониторинга размывает границы между мониторингом ИБ и мониторингом защищенности ИР.

В основу классификации видов мониторинга можно положить его объект. Наиболее распространенными в доктрине являются мониторинг ИБ, мониторинг информации, мониторинг безопасности информации, мониторинг защищенности ИР. Следует подчеркнуть, что в разных нормативных документах, особенно в подзаконных правовых актах эти виды имеют одинаковое название, но несовпадающее содержание.

В актуальной среде, где многие, если не все, критически важные функции организации зависят от информационных технологий, способности управлять такими технологиями и обеспечивать конфиденциальность, целостность и доступность информации, особую важность приобретает защищенность ИР. В условиях возрастания опасности компьютерных атак пристальное внимание уделяется оценке и анализу эффективности мер безопасности и состояния ИБ организации в соответствии с требованиями государственных регуляторов и допустимым уровнем риска. Эффективность мер безопасности измеряется правильностью реализации и адекватностью согласования реализованных мер безопасности с потребностями организации в соответствии с текущим уровнем риска (т. е. полнотой реализации мер безопасности в соответствии с планом обеспечения безопасности для устранения угроз и адекватностью плана существующим рискам). ИБ ИР — это состояние защищённости информационных ресурсов и одновременно динамический процесс поддержания исходного состояния или перехода в другие допустимые благоприятные состояния. Процессом изменения состояний необходимо эффективно и проактивно управлять, чтобы организация могла выявлять и реагировать на новые уязвимости, развивающиеся угрозы в условиях постоянно меняющиеся архитектуры вычислительных систем и операционной среды.

Непрерывный мониторинг ИБ определяется как поддержание осведомленности об ИБ, уязвимостях и угрозах для поддержки принятия решений по управлению организационными рисками. Кроме того, общая архитектура безопасности организации и соответству-

ющая программа безопасности контролируются, чтобы гарантировать, что деятельность организации остается в пределах приемлемого уровня риска, в условиях происходящих изменений. Своевременная, актуальная и точная информация особенно важна с учетом ограниченности ресурсов и необходимости приоритизации деятельности.

Любые усилия, направленные на поддержку мониторинга ИБ в организации, начинаются с определения руководством комплексной стратегии мониторинга ИБ, охватывающей технологии, процессы, процедуры, операционную среду и персонал. Такая стратегия как свидетельствует зарубежный опыт:

- основана на точном понимании допустимого уровня риска и помогает должностным лицам устанавливать приоритеты и последовательность управления рисками;
- включает метрики, предоставляющие значимые показатели состояния безопасности на всех организационных уровнях;
- обеспечивает эффективность средств контроля безопасности;
- проверяет соответствие требованиям регулирующих органов к обеспечению ИБ, вытекающим из функций организации, федерального законодательства, директив, нормативных актов, политик и стандартов/руководств;
- содержит информацию обо всех ИТ-активах организации и помогает поддерживать прозрачность их безопасности;
- обеспечивает знание и контроль изменений в организационных системах и средах работы;
- поддерживает осведомленность об угрозах и уязвимостях.

Мониторинг способствует оценке ИБ, состояния защищенности ИР, систем, процессов, действий для обоснования выбора мер по обеспечению их безопасности.

Стратегии и программы мониторинга не статичны. Оценки мер безопасности, метрики состояния безопасности, а также частота мониторинга меняются в соответствии с потребностями конкретной организации с учетом требований регуляторов. Стратегия мониторинга пересматривается. Данная мера позволяет убедиться в поддержании в достаточной степени устойчивости деятельности организации в границах допустимого уровня терпимости к риску, в актуальности и полноте метрик и данных. Стратегия определяет способы идентификации состояния безопасности, эффективной поддержки принятия обоснованных решений по управлению рисками, повышения организации реагирования на известные и возникающие угрозы.

Организация устанавливает процедуру для пересмотра и изменения всех аспектов интегрированной стратегии управления, включая актуальность общей стратегии, точность отражения толерантности к риску организации, корректность измерений и применимость метрик, требования к отчетности, а также периодичность мониторинга и оценки. Если для отчетности собранные данные не требуются или оказываются бесполезными для поддержания или повышения уровня безопасности, организация рассматривает возможность прекращения их сбора**.** Факторы, способствующие изменению стратегии мониторинга, могут включать, помимо прочего:

- изменения основных задач или технологии управленческих процессов;
- значительные перемены в архитектуре организации, включая добавление или удаление систем;
- изменения в толерантности к рискам организации;
- изменения в информации об угрозах и уязвимостях;
- изменения в ИС, включая изменения в категоризации/уровне воздействия;
- проблемы, связанные с конкретными средствами контроля [12, с. 35].

Общий мониторинг не может быть эффективно реализован только с помощью одних ручных или автоматизированных процессов. Ручные процессы воспроизводимы и проверяемы, что обеспечивает их последовательное внедрение. Автоматизированные процессы, включая использование автоматизированных инструментов поддержки (например, инструментов сканирования уязвимостей и устройств сетевого сканирования), могут сделать процесс непрерывного мониторинга более экономичным, последовательным и эффективным.

Мониторинг ИБ — это непрерывный процесс сбора, корреляции и анализа событий, влияющих на конфиденциальность, целостность и доступность ИС(АС), данных, ИТКС, необходимость проведения которого продиктована потребностью в раннем обнаружении угроз безопасности функционирования систем и сетей, а также в организации и проведении управляемого реагирования на события и инциденты ИБ. Целостность эволюционной активности и иерархическую связанность выделяют в качестве общих принципов адаптивного мониторинга ИБ киберфизических систем [2, с. 41] как объекта системного анализа и уровня его изучения в общей теории систем.

Мониторинг ИБ является связующим звеном между превентивными мерами и реагированием, обеспечивает наблюдаемость реальных состояний всех компонентов постоянно расширяющегося ИТ-ландшафта. Сущность раннего обнаружения признаков инцидента ИБ заключается в оповещении пользователей о необычном поведении составляющих компонентов инфраструктуры и различных ресурсов до момента трансформации события ИБ в инцидент ИБ, а также приоритизацию таких событий с точки зрения оценки их потенциальной опасности для систем и сетей. Кроме того, мониторинг ИБ способствует формированию доказательственной базы компьютерных преступлений, включающей результаты анализа логов, контента для проведения расследований, аудита и выявления нарушений политик безопасности и требований регу-

лирующих органов по безопасности. Мониторинг ИБ служит основой для принятия мер по совершенствованию систем обеспечения ИБ и защиты информации, совершенствования политик безопасности, процессов и средств защиты.

Отсутствие мониторинга ИБ может привести к запоздалому обнаружению компьютерных атак и негативным последствиям, связанным с нанесением оператору и пользователям системы непоправимого ущерба. Инциденты, обнаруживаемые по сигналам, поступающим от третьей стороны (государственных регуляторов, вышестоящих уровней в структуре управления), способствуют обнаружению угроз ИБ, но увеличивают время нахождения нарушителя внутри периметра и, соответственно, могут привести к увеличению масштабов неблагоприятных последствий. Дефицит мониторинга влечет пропуск угроз, рефлексивное реагирование на компьютерные инциденты (КИ), например, когда наступает неприемлемое для организации событие, и приходиться расплачиваться за ошибки или дефицит внимания к обеспечению ИБ.

Деятельность по обнаружению и регистрации КИ основывается на результатах мониторинга, в рамках которого осуществляется сбор информации о событиях ИБ и других данных, поступающих из различных источников. При этом данные мониторинга включают не только информацию о состоянии объектов мониторинга ИБ, но также сведения, получаемые из среды функционирования объекта мониторинга и внешних сервисов, которые могут использоваться для выявления уязвимостей и угроз безопасности информации[5]. К данным мониторинга могут относиться следующие сведения: информация о событиях ИБ, выявленных уязвимостях, результатах контроля соответствия конфигурационных настроек, действиях пользователей, результатах контроля потоков информации, работоспособности программных, технических и программно-технических средств, включая средства защиты информации, а также различные справочные сведения. В деятельности по управлению КИ данные мониторинга могут использоваться для анализа возможности эксплуатации нарушителями уязвимостей ИР и угроз в случае реализации компьютерных атак, своевременного выявления и регистрации КИ.

Мониторинг позволяет определить результаты оценки состояния защищенности системы, процесса, действия для обоснования управленческих решений по обеспечению их ИБ. Перечень систем, процессов и действий, которые могут подвергаться мониторингу, охватывает, но при этом не ограничивается следующими аспектами: реализацией процессов системы мониторинга ИБ; менеджментом (инцидентов, уязвимостей, конфигураций); осведомленностью о безопасности и обучением; регистрацией событий контроля доступа, межсетевых экранов и других средств защиты; аудитом; процессами оценки степени риска и его обработки; сторонним менеджментом рисков; управлением непрерывностью различных аспектов деятельности организации; управлением физической и экологической безопасностью; мониторингом системы.

При построении понятийного аппарата следует учитывать положительную практику развитых зарубежных государства. Например, в США Концепция мониторинга безопасности ИС давно признана надежной практикой управления. В циркуляре А-130 административно-бюджетного управления (1997) и Федеральном законе об управлении ИБ (The Federal Information Security Management Act of 2002, FISMA) подчеркнута важность постоянного мониторинга безопасности ИС. На агентства возложены обязанности проводить оценку средств контроля безопасности с частотой, соответствующей риску, но не реже раз в год. Установлены требования по пересмотру агентствами средств контроля безопасности своих ИС и гарантий, подтверждающих, что изменения в системе не оказывают существенного влияния на безопасность, при этом планы обеспечения безопасности остаются эффективными, а средства контроля безопасности функционируют должным образом. В меморандуме М-11-33 «Инструкция по отчетности за 2011 финансовый год для Федерального закона об управлении информационной безопасностью и Управления конфиденциальностью агентств» административно-бюджетного управления США отмечена обязанность агентств проводить постоянную авторизацию ИС посредством внедрения программ непрерывного мониторинга. Инструменты, поддерживающие автоматизированный мониторинг некоторых аспектов ИС, стали эффективными средствами для сбора и анализа данных. В США непрерывный мониторинг ИБ (information security continuous monitoring, ISCM) федеральных информационных систем и организаций, как определено в Специальной публикации (SP) 800-137 Национального института стандартов и технологий (NIST), представляет собой постоянное поддержание осведомленности об ИБ, уязвимостях и угрозах для поддержки принятия решений по управлению организационными рисками. Термины «непрерывный» в данном контексте означают, что для адекватной защиты информации организации средства контроля безопасности и организационные риски оцениваются и анализируются с частотой, достаточной для принятия решений по безопасности, основанных на оценке рисков. Согласно NIST SP 800-137, программа ISCM создается для сбора информации в соответствии с заранее установленными метриками с использованием доступных средствам контроля безопасности данных. Архитектура безопасности организаций, оперативные возможности обеспечения безопасности и процессы мониторинга должны совершенствоваться в целях адекватного реагирования на динамично развивающийся ландшафт угроз и уязвимостей. Стратегия и программа ISCM организации должна регулярно проверяются на актуальность и пересматриваются по мере необходимости для повышения прозрачности активов и осведомленности об уязвимостях. Это дополнитель-

[5] ГОСТ Р 59547—2021, пункт 3.2.

но обеспечивает контроль безопасности информационной инфраструктуры на основе данных и повышает ее устойчивость. Программа ISCM-стратегии и постоянной авторизации (OA) администрации общих служб (GSA), разработанная в соответствии с NIST SP 800-137, способствует переходу от управления рисками, основанного на соблюдении требований, к управлению рисками, основанному на данных. Такой переход предоставляет GSA сведения о состоянии безопасности и постоянное понимание эффективности мер безопасности, необходимые для принятия решений по реагированию на риски.

В нормативном правовом регулировании, включая техническое регулирование, применяются следующие понятия: мониторинг информации, мониторинг ИБ, мониторинг ИБ в ИС, мониторинг безопасности информации, мониторинг защищенности ИР. Все эти понятия имеют некоторое общее содержание. Однако они существенно отличаются по объекту мониторинга, которым выступает информация, ИБ, ИБ в ИС, безопасность информации, защищённость ИР.

Сравним эти понятия. Модель взаимодействия различных видов мониторинга представлена на рисунке 2.

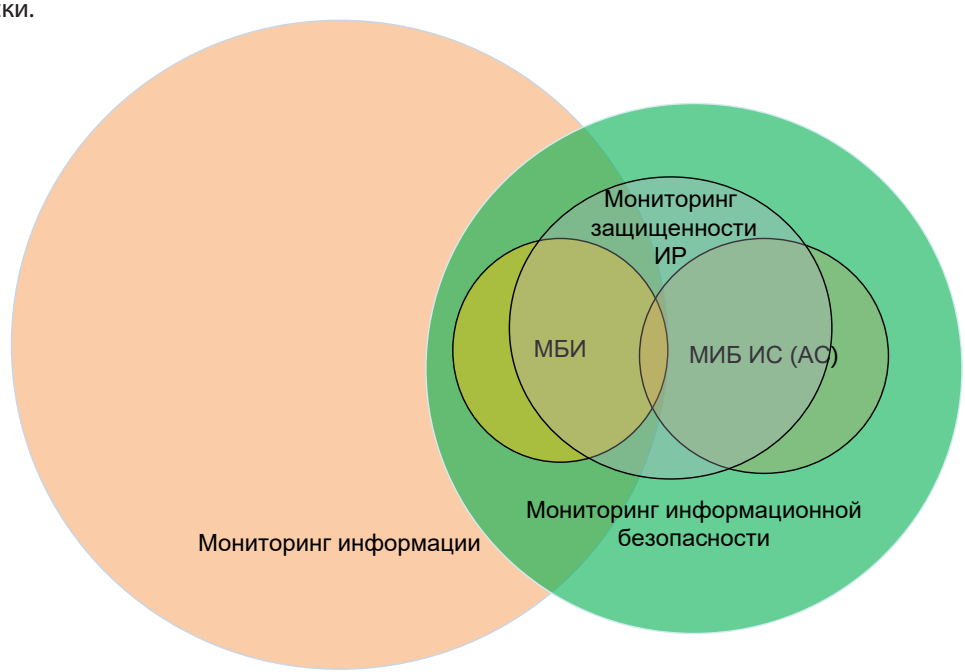

Рис.2. Схема взаимодействия различных видов мониторинга: МБИ — мониторинг безопасности информации; МИБ ИС (АС) — мониторинг информационной безопасности информационных (автоматизированных) систем

Мониторинг информации или, как нередко пишут в технической литературе, информационный мониторинг представляет собой процесс систематического отслеживания, сбора и анализа информации с целью выявления тенденций, проблем и принятия обоснованных решений. Мониторинг различных типов данных, таких как производительность ИТ-систем, финансовые данные или активность в социальных сетях, предназначен для обеспечения правильной работы систем и сетей, понимания их поведения и порядка реагирования на события, а также планирования предупредительных и иных мер. Для немедленного реагирования наблюдение может выполняться в режиме реального времени, а для выявления тенденций — в течение длительного периода.

Мониторинг ИБ в ИС(АС) представляет собой процесс постоянного наблюдения и анализа результатов регистрации событий безопасности и иных данных с целью выявления уязвимостей, нарушений и угроз безопасности информации. Процесс мониторинга ИБ может охватывать все или часть ИС(АС), составляющих информационную инфраструктуру обладателя информации и (или) оператора, в том числе функционирующих на базе информационно-телекоммуникационной инфраструктуры центра обработки данных или облачной инфраструктуры. В процессе мониторинга ИБ в рамках анализа результатов регистрации событий безопасности и иных данных мониторинга осуществляются: анализ событий безопасности и иных данных мониторинга; контроль (анализ) защищенности информации; анализ и оценка функционирования систем защиты ИС(АС); периодический анализ изменения угроз безопасности информации в ИС(АС), возникающих в ходе эксплуатации. В стандартах определены: а) требования к уровням мониторинга ИБ: — к источникам данных мониторинга, — к сбору таких данных, — их хранению, агрегированию и обработке, — представлению данных о результатах мониторинга; б) порядок осуществления мониторинга ИБ при реализации мер ЗИ; в) требования к защите данных мониторинга. Мониторинг ИБ можно

осуществлять в рамках системы менеджмента ИБ операторов ИС(АС). При осуществлении мониторинга ИБ могут быть использованы соответствующие автоматизированные средства (дополнительные программные и программно-технические средства).

В результате сравнительного анализа терминов «мониторинг безопасности информации» и «мониторинг ИБ» выявлены общие элементы в конструкции дефиниций и различия в объёме понятий. Общим является то, что это процесс или процедура наблюдения. В случае мониторинга безопасности информации эта процедура осуществляется «за процессом обеспечения безопасности информации при применении информационных технологий», а случае мониторинга ИБ это не только наблюдение регистрации событий безопасности и иных данных, но и анализ результатов этого наблюдения, который нацелен на выявление нарушений безопасности информации, угроз безопасности информации и уязвимостей. Использование при определении словосочетания «иные данные» позволяет наполнить рассматриваемое понятие смыслом, различным по объему и содержанию.

Организация может решить объединить все свои действия по мониторингу, оценке защищенности, анализу и оцениванию в одну программу оценки. Однако следует отметить, что ИСО/МЭК 27001 не требует от организаций наличия такой программы.

Организация (с учетом требований подразделов 9.1 и 5.3 ИСО/МЭК 27001) определяет субъекта мониторинга, оценки защищенности, анализа и оценивания с указанием конкретных лиц и ролей. Мониторинг, оценка защищенности, анализ и оценивание могут выполняться вручную или с помощью средств автоматизации с распределением ролей и обязанностей: потребители и планировщики оценки защищенности, рецензент оценки, владелец информации, сборщик информации, информационный аналитик, информационный коммуникатор. Указанные роли могут совмещаться в одном лице.

В аспекте ИБ мониторинг и оценка защищенности осуществляется для определения значения, состояния или тенденции в результативности или эффективности деятельности по обеспечению ИБ. Целью такой деятельности является не только обнаружение новых уязвимостей в системах, но идентификация возможных потребностей в улучшении таких систем для их актуализации и приведения в соответствие с характером появившихся угроз ИБ, уровнем развития новых технологий и текущих инфраструктурных изменений. В системе мониторинга ИБ могут быть оценены различные процессы, действия, средства контроля и управления и их группы. Например, в п. c) подраздела 7.2 ИСО/МЭК 27001 рассматриваются требования о приобретении необходимого уровня компетентности. Организация может определить, все ли лица, которым требуется обучение, прошли его, и было ли обучение проведено в соответствии с планом. Результатом оценки защищенности в таком случае может явиться число обученных людей, степень обладания такими лицами необходимыми знаниями и навыками. Компетентность персонала может быть оценена с использованием машинных программ анкетирования по завершении процесса обучения.

Заключение

В результате исследования содержания понятий в той или иной мере, коррелирующих с термином «мониторинг», можно утверждать, что особенности конкретного вида мониторинга во многом определяются объектом: информаций, ИБ, защищенностью ИР и др. В связи этим существует настоятельная необходимость выработки законодательных положений, в которых определяются основные понятия.

В правильно организованной структуре ИБ мониторинг защищенности ИР, охватывающих ИС, ИТКС и АСУ, представляет собой систему процессов, адаптируемых под меняющийся ландшафт угроз, с целью выявления возможных признаков обнаружения инцидентов ИБ на самых ранних этапах их зарождения и развития с целью предотвращения и минимизации возможных негативных и недопустимых последствий для защищаемых информации, систем и сетей.

Благодарности

Статья подготовлена в рамках выполнения в 2025 г. прикладных научных исследований Санкт-Петербургского университета ГПС МЧС России по заказу МЧС России НИР «Кибермониторинг».

Литература

1. Зегжда Д.П., Васильев Ю.С., Полтавцева М.А., Кефели И.Ф., Боровков А.И. Кибербезопасность прогрессивных производственных технологий в эпоху цифровой трансформации // Вопросы кибербезопасности. 2018. № 26. С. 2-15.
2. Васильев Ю.С. Проблемы безопасности цифрового производства и его устойчивость к киберугрозам // Ю.С. Васильев, Д.П. Зегжда, М.А. Полтавцева. Проблемы информационной безопасности. Компьютерные системы. 2017. № 4. С. 47-63.
3. Зегжда Д.П. Технические основы киберустойчивости и практика прогностической защиты от кибератак: монография. СПб. : Политех Пресс, 2022. 490 с.

4. Полтавцева М.А. Адаптивный мониторинг информационной безопасности: монография. Санкт-Петербург: Политех-пресс Санкт-Петербургский политехнический ун-т Петра Великого, 2021. 165 с.
5. Минаев В.А., Бондарь К.М., Дунин В.С. Возможности имитационного моделирования деятельности центра оперативного управления и мониторинга информационной безопасности в условиях кибератак различного масштаба // Вестник Воронежского института МВД России. 2021. № 3. С. 49-59.
6. Стрельников Р.В. SOC. Неэффективность внедрения // Вестник Балтийского федерального университета им. И. Канта. Серия: физико-математические и технические науки. 2019. № 4. С. 81-85.
7. Васильев В.И., Вульфин А.М., Картак В.М., Башмаков Н.М., Кириллова А.Д. Распределенная система обнаружения сетевых атак на основе федеративного трансферного обучения // Вопросы кибербезопасности. 2024. № 6. С. 117-129.
8. Сизов В.А. Мониторинг информационной безопасности / В.А. Сизов, А.Д. Киров. Москва: РЭУ им. Г.В. Плеханова, 2022. 88 с.
9. Holdsworth J., Kosinski M. What is information security? URL: https://www.ibm.com/think/topics/information-security (дата обращения 01.11.2025).
10. Abu Lamddi M. Developing Dependability Requirements Engineering for Secure and Safe Information Systems with Knowledge Acquisition for Automated Specification. Journal of Software Engineering and Applications. Vol. 10. No. 2, February 28, 2017.
11. Метельков А.Н. Информационные ресурсы: стремление к порядку порождает беспорядок // Правовая информатика. 2025. № 3. С. 69-78.
12. Метельков А.Н. Онтология информационных ресурсов в МЧС России// Научно-аналитический журнал «Вестник СПб университета Государственной противопожарной службы МЧС России». 2025. № 2. С. 113-127.
13. Афанасьев В.Г. Научное управление обществом (Опыт системного исследования). М., Политиздат, 1968. 384 с.
14. Шамсудинов Р.Р. Интеллектуальная система мониторинга информационной безопасности промышленного интернета вещей с использованием механизмов искусственных иммунных систем: автореф. дис. …канд. технич. наук: спец. 2.3.6. Уфа, 2023. 19 с.
15. Вульфин А.М. Модели и методы комплексной оценки рисков безопасности объектов критической информационной инфраструктуры на основе интеллектуального анализа данных: автореф. дис. … д-ра технич. наук: 2.3.6. Уфа, 2022. 36 с.
16. Дорофеев А.В., Марков А.С. Мониторинг событий информационной безопасности: технологии и методы контроля эффективности // Вестник Военного инновационного технополиса "Эра". 2022. Т. 3. № 4. С. 392-400.
17. Ерохин С.Д., Петухов А.Н., Пилюгин П.Л. Эффективность активного мониторинга событий сетевой безопасности // Электросвязь. 2020. № 2. С. 46-51.
18. Цибизова Т.Ю., Панилов П.А., Кочешков М.А. Мониторинг безопасности системы защиты информации критической информационной инфраструктуры на основе когнитивного моделирования // Известия Тульского государственного университета. Технические науки. 2023. № 6. С. 33-41.

SECTION:
INFORMATION PROTECTION METHODS AND SYSTEMS

DIVERSITY OF MONITORING IN ENSURING INFORMATION SECURITY

***Metelkov A.N.*[6]**

Keywords*: surveillance, control, information, information resources, safety, security.*

Abstract

The purpose of *the article is to study the category of "monitoring" in various aspects of its use in relation to the field of information and information security.*

Research method*: the author uses a system-structural approach to the analysis of the content of the concept of "monitoring", the method of comparing sets that unite the objects of monitoring.*

Result: *various types of monitoring objects and approaches to the content of monitoring are studied in the work.*

[6] ***Alexander N. Metelkov,*** *Ph.D. in Law, Associate Professor, Associate Professor of the Department of Applied Mathematics and Information Technology Security, St. Petersburg University of the State Fire Service of the Ministry of Emergency Situations of Russia, St. Petersburg, Russia. ORCID: 0000-0002-6113-8981.*

E-mail: metelkov5178@mail.ru

The experience of developed foreign countries in the application of continuous monitoring of the security of information systems is analyzed. A model of correlation between different types of monitoring is proposed. As a result, using a graphical representation of sets using Euler Venn diagrams, a model of interaction between information security monitoring, information monitoring, information security monitoring and information security monitoring was developed.

***Practical value:** the presented model of the correlation of various types of monitoring depending on its object is an original result that complements the existing ideas about the subject of monitoring in the information environment. Differentiation of monitoring by the object of monitoring allows in practice a differentiated approach to the implementation of measures to meet the requirements of state regulators in the field of information and functional security.*

References

1. Zegzhda D.P., Vasil'ev Ju.S., Poltavceva M.A., Kefeli I.F., Borovkov A.I. Kiberbezopasnost' progressivnyh proizvodstvennyh tehnologij v jepohu cifrovoj transformacii // Voprosy kiberbezopasnosti. 2018. № 26. S.2-15.
2. Vasil'ev Ju.S. Problemy bezopasnosti cifrovogo proizvodstva i ego ustojchivost' k kiberugrozam // Ju.S. Vasil'ev, D.P. Zegzhda, M.A. Poltavceva. Problemy informacionnoj bezopasnosti. Komp'juternye sistemy. 2017. № 4. S. 47-63.
3. Zegzhda D.P. Tehnicheskie osnovy kiberustojchivosti i praktika prognosticheskoj zashhity ot kiberatak: monografija. SPb. : Politeh Press, 2022. 490 s.
4. Poltavceva M.A. Adaptivnyj monitoring informacionnoj bezopasnosti: monografija. Sankt-Peterburg: Politeh-press Sankt-Peterburgskij politehnicheskij un-t Petra Velikogo, 2021. 165 s.
5. Minaev V.A., Bondar' K.M., Dunin V.S. Vozmozhnosti imitacionnogo modelirovanija dejatel'nosti centra operativnogo upravlenija i monitoringa informacionnoj bezopasnosti v uslovijah kiberatak razlichnogo masshtaba // Vestnik Voronezhskogo instituta MVD Rossii. 2021. № 3. S. 49-59.
6. Strel'nikov R.V. SOC. Nejeffektivnost' vnedrenija // Vestnik Baltijskogo federal'nogo universiteta im. I. Kanta. Serija: fiziko-matematicheskie i tehnicheskie nauki. 2019. № 4. S. 81-85.
7. Vasil'ev V.I., Vul'fin A.M., Kartak V.M., Bashmakov N.M., Kirillova A.D. Raspredelennaja sistema obnaruzhenija setevyh atak na osnove federativnogo transfernogo obuchenija // Voprosy kiberbezopasnosti. 2024. № 6. S.117-129.
8. Sizov V.A. Monitoring informacionnoj bezopasnosti / V.A. Sizov, A.D. Kirov. Moskva: RJeU im. G.V. Plehanova, 2022. 88 s.
9. Holdsworth J., Kosinski M. What is information security? URL: https://www.ibm.com/think/topics/information-security (data obrashhenija 01.11.2025).
10. Abu Lamddi M. Developing Dependability Requirements Engineering for Secure and Safe Information Systems with Knowledge Acquisition for Automated Specification. Journal of Software Engineering and Applications. Vol. 10. No. 2 February 28, 2017.
11. Metel'kov A.N. Informacionnye resursy: stremlenie k porjadku porozhdaet besporjadok // Pravovaja informatika. 2025. № 3. S. 69-78.
12. Metel'kov A.N. Ontologija informacionnyh resursov v MChS Rossii// Nauchno-analiticheskij zhurnal «Vestnik SPb universiteta Gosudarstvennoj protivopozharnoj sluzhby MChS Rossii». 2025. № 2. S. 113-127.
13. Afanas'ev V.G. Nauchnoe upravlenie obshhestvom (Opyt sistemnogo issledovanija). M., Politizdat, 1968. 384 s.
14. Shamsudinov R.R. Intellektual'naja sistema monitoringa informacionnoj bezopasnosti promyshlennogo interneta veshhej s ispol'zovaniem mehanizmov iskusstvennyh immunnyh sistem: avtoref. dis. …kand. tehnich. nauk: spec. 2.3.6. Ufa, 2023. 19 s.
15. Vul'fin A.M. Modeli i metody kompleksnoj ocenki riskov bezopasnosti ob#ektov kriticheskoj informacionnoj infrastruktury na osnove intellektual'nogo analiza dannyh: avtoref. dis. … d-ra tehnich. nauk: 2.3.6. Ufa, 2022. 36 s.
16. Dorofeev A.V., Markov A.S. Monitoring sobytij informacionnoj bezopasnosti: tehnologii i metody kontrolja jeffektivnosti // Vestnik Voennogo innovacionnogo tehnopolisa "Jera". 2022. T. 3. № 4. S. 392-400.
17. Erohin S.D., Petuhov A.N., Piljugin P.L. Jeffektivnost' aktivnogo monitoringa sobytij setevoj bezopasnosti // Jelektrosvjaz'. 2020. № 2. S. 46-51.
18. Cibizova T.Ju., Panilov P.A., Kocheshkov M.A. Monitoring bezopasnosti sistemy zashhity informacii kriticheskoj informacionnoj infrastruktury na osnove kognitivnogo modelirovanija // Izvestija Tul'skogo gosudarstvennogo universiteta. Tehnicheskie nauki. 2023. № 6. S. 33-41.