УДК 004

АНАЛИТИЧЕСКИЙ ОБЗОР СПОСОБОВ МОНИТОРИНГА И РЕАГИРОВАНИЯ НА ВОЗМОЖНЫЕ ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ЦИФРОВОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЕ МЧС РОССИИ И УРОВЕНЬ ИХ ТЕХНИЧЕСКОЙ РЕАЛИЗАЦИИ

Аннотация

Аналитический обзор разработан с целью выявления текущей ситуации по обеспечению организации функционирования систем мониторинга и реагирования на возможные инциденты информационной безопасности критической информационной инфраструктуры Российской Федерации применительно к цифровой информационной инфраструктуре, а также возможным направлениям развития нормативных правовых актов, регламентирующих порядок взаимодействия элементов специально созданной ведомственной организационной структуры, уполномоченной для решения задач системы обеспечения информационной безопасности МЧС России.

Аналитический обзор предназначен для специалистов в области информационной безопасности и защиты информации.

Аналитический обзор разработан в рамках прикладных научных исследований Санкт-Петербургского университета ГПС МЧС России в 2025 году.

Ключевые слова: инциденты информационной безопасности, критическая информационная инфраструктура, средство защиты информации, мониторинг, реагирование.

ANALYTICAL REVIEW OF METHODS FOR MONITORING AND RESPONDING TO POSSIBLE INFORMATION SECURITY INCIDENTS IN THE DIGITAL INFORMATION INFRASTRUCTURE OF THE RUSSIAN EMERGENCIES MINISTRY AND THE LEVEL OF THEIR TECHNICAL IMPLEMENTATION

Abstract

The analytical review was developed to identify the current situation in ensuring the organization of the functioning of monitoring systems and responding to possible incidents of information security of the critical information infrastructure of the Russian Federation in relation to the digital information infrastructure, as well as possible areas of development of regulatory legal acts governing the procedure for the interaction of elements of a specially created departmental organizational structure authorized to solve the problems of the information security system of the Ministry of Emergency Situations of Russia.

The analytical review is intended for specialists in the field of information security and information protection.

The analytical review was developed as part of the applied scientific research of the St. Petersburg University of the State Fire Service of the Ministry of Emergency Situations of Russia in 2025.

Keywords: information security incidents, critical information infrastructure, information security tool, monitoring, response.

Список сокращений

АРМ	–	автоматизированное рабочее место
АСУ ТП	–	автоматизированная система управления технологическим процессом
БД	–	база данных

ГОСТ – государственный стандарт
ГК – Гражданский кодекс
ИБ – информационная безопасность
ИС – информационная система
ИТ – информационная технология
КД – конструкторская документация (рабочая конструкторская документация)
КИИ – критическая информационная инфраструктура
ЛВС – локальная вычислительная сеть
МКПО – международная классификация промышленных образцов
МКТУ – международная классификация товаров и услуг
МПК (СПК) – международная патентная классификация (совместная патентная классификация)
НИОКР – научно-исследовательские, опытно-конструкторские и технологические работы
НИР – научно-исследовательская работа
НПП – научно-производственное предприятие
НСД – несанкционированный доступ
НТИ – научно-техническая информация
ОИС – объект интеллектуальной собственности
ОКБ – опытно-конструкторское бюро
ООО – общество с ограниченной ответственностью
ОТС – организационно-техническая система
ПДн – персональные данные
ПО – программное обеспечение
ПИ – патентные исследования
РИД – результат интеллектуальной деятельности
РФ – Российская Федерация
СВТ – средство вычислительной техники
СЗИ – средство защиты информации
СОИБ – система обеспечения информационной безопасности
ТЗ – техническое задание
ТУ – технические условия
УДК – универсальная десятичная классификация
ФЗ – федеральный закон
ФИПС – федеральный институт промышленной собственности
ФСТЭК – федеральная служба по техническому и экспортному контролю
ЭВМ – электронно-вычислительная машина

Введение

Аналитический обзор способов мониторинга и реагирования на возможные инциденты информационной безопасности (далее – ИБ) в цифровой информационной инфраструктуре МЧС России (далее – ЦИИ) и уровень их технической реализации разработан отделом информационного обеспечения населения и технологий информационной поддержки РСЧС и пожарной безопасности, кафедрой прикладной математики и безопасных информационных технологий, центром информационных и коммуникационных технологий Санкт-Петербургского университета ГПС МЧС России в НИР «Кибермониторинг», в составе авторского коллектива Буйневич М.В., Грызунов В.В., Метельков А.Н., Матвеев А.В., Максимов А.В., Папырина Е.В., Рассказов М.С., Синещук М.Ю., Тукмачева М.А., Уткин О.В., Шестаков А.В.

Актуальность обзора обусловлена ростом инцидентов (Рисунок 1) на государственную информационную инфраструктуру и промышленность, в том числе опасные производственные объекты (Рисунок 4).

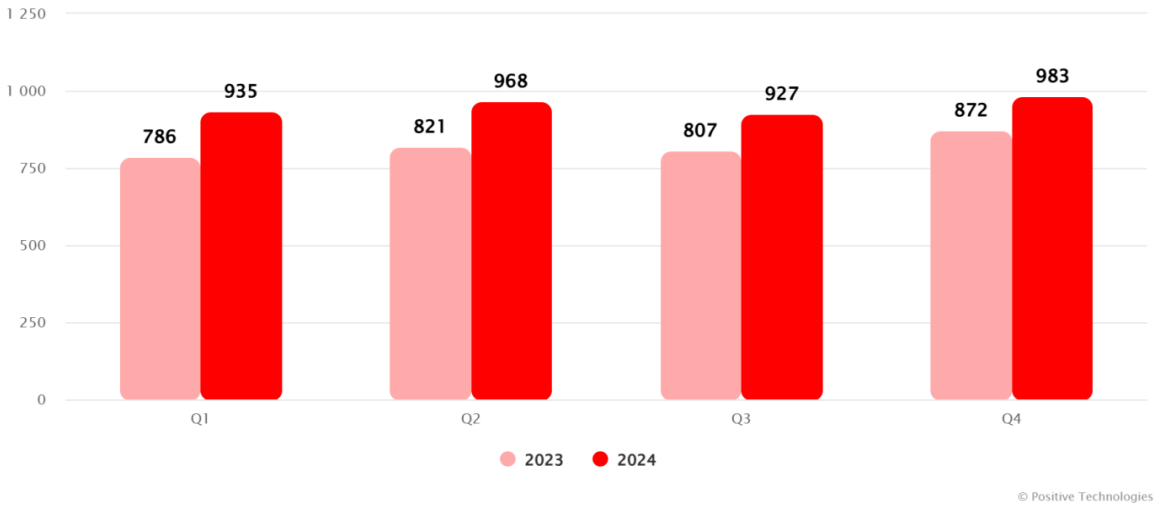


Рисунок 1 – Количество инцидентов в 2023 и 2024 годах [14]

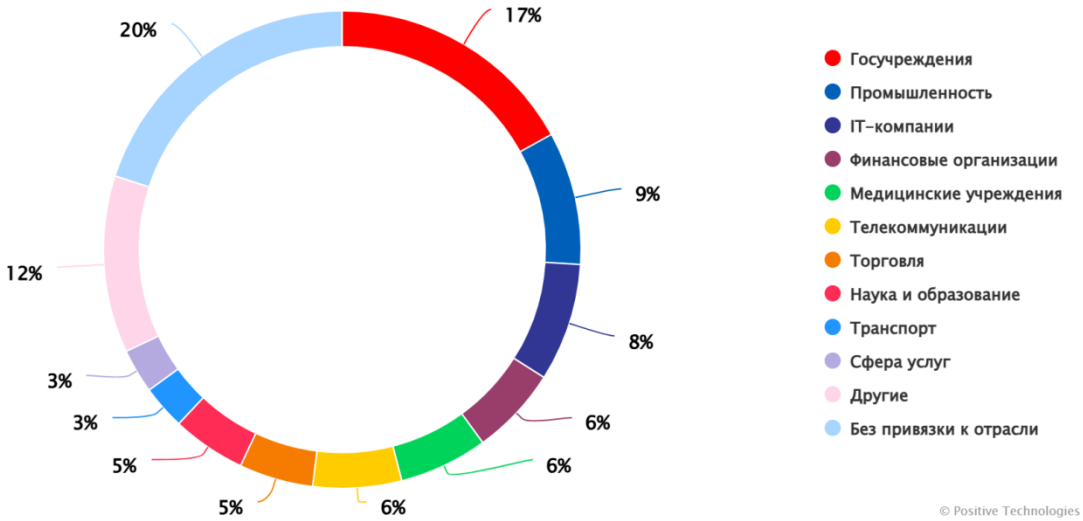


Рисунок 2 – Инциденты в организациях в 4 кв.2024 года [14]

Изменения отмечаются в реализуемых методах компьютерных атак (КА) (Рисунок 3) и их последствиях (Рисунок 4).

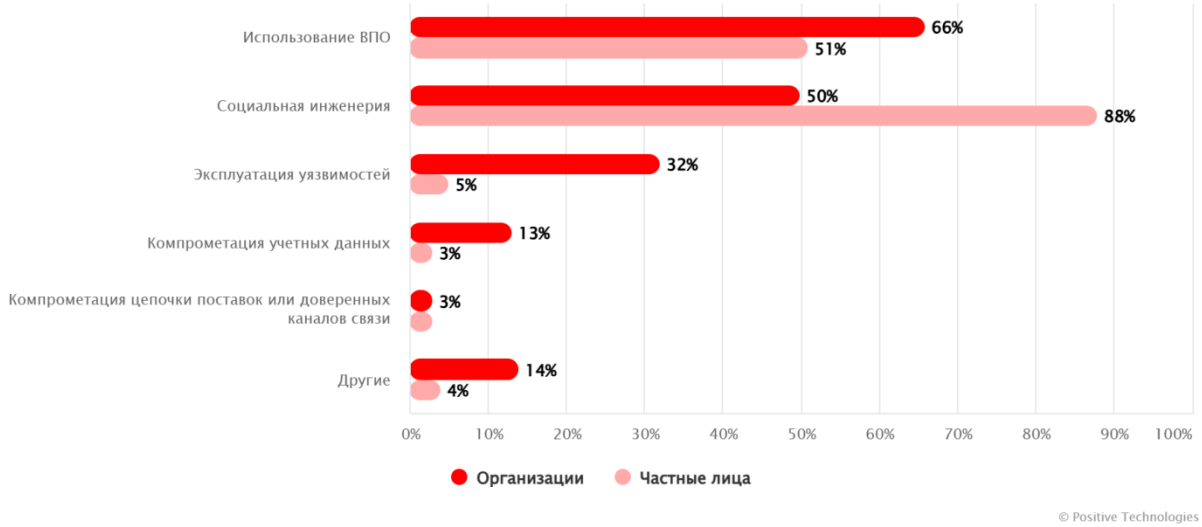


Рисунок 3 – Методы атак в 4 кв. 2024 года [14]

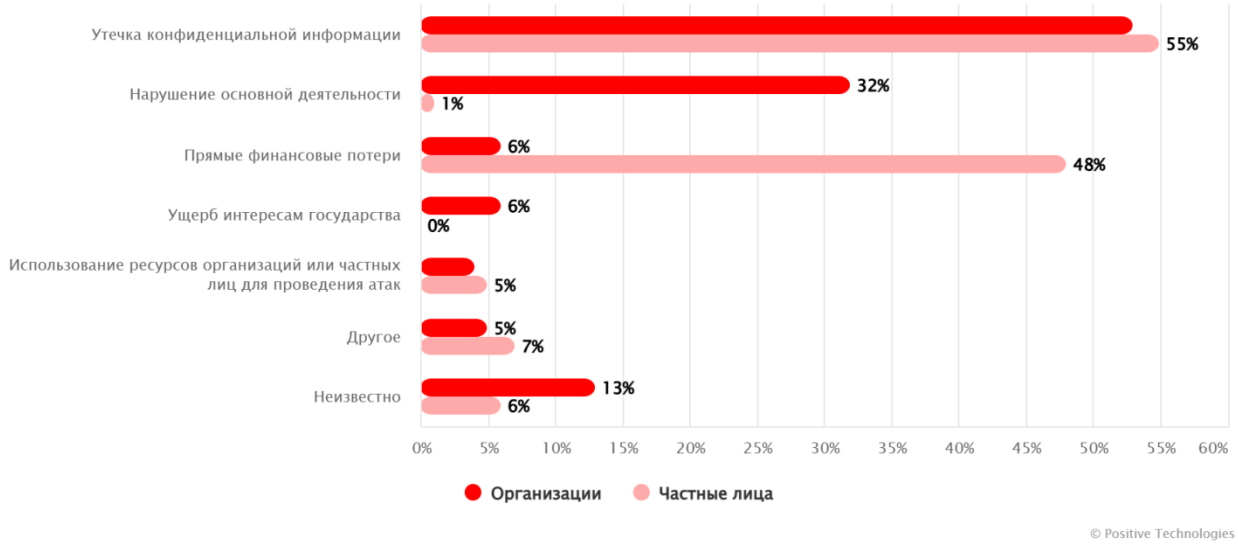


Рисунок 4 – Последствия атак в 4 кв.2024 года [14]

Смещение фокуса воздействий наблюдается на сетевые средства (Рисунок 5) и операционные системы (Рисунок 6).

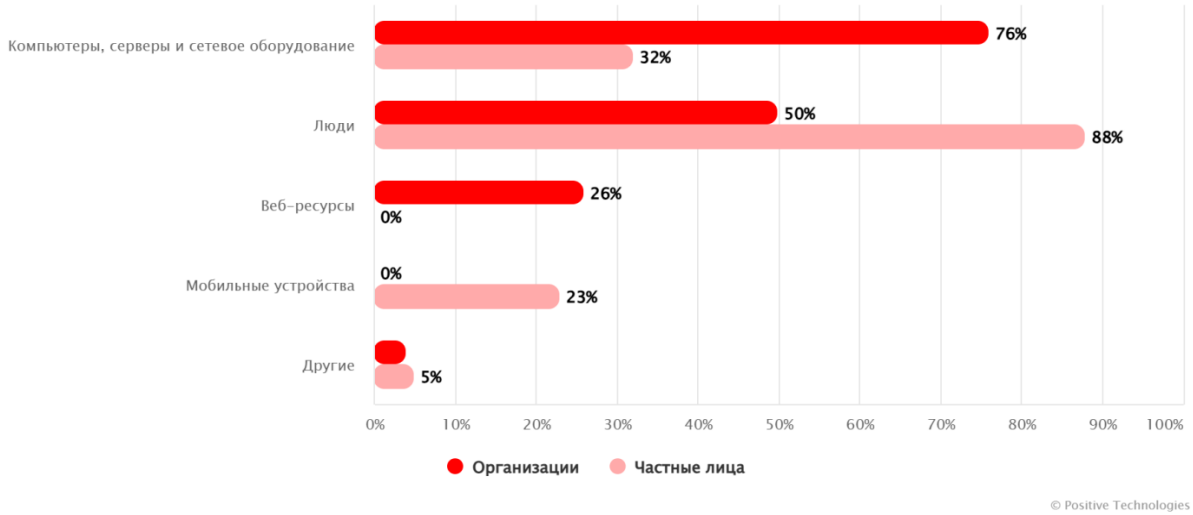


Рисунок 5 – Объекты атак в 4 кв. 2024 года [14]

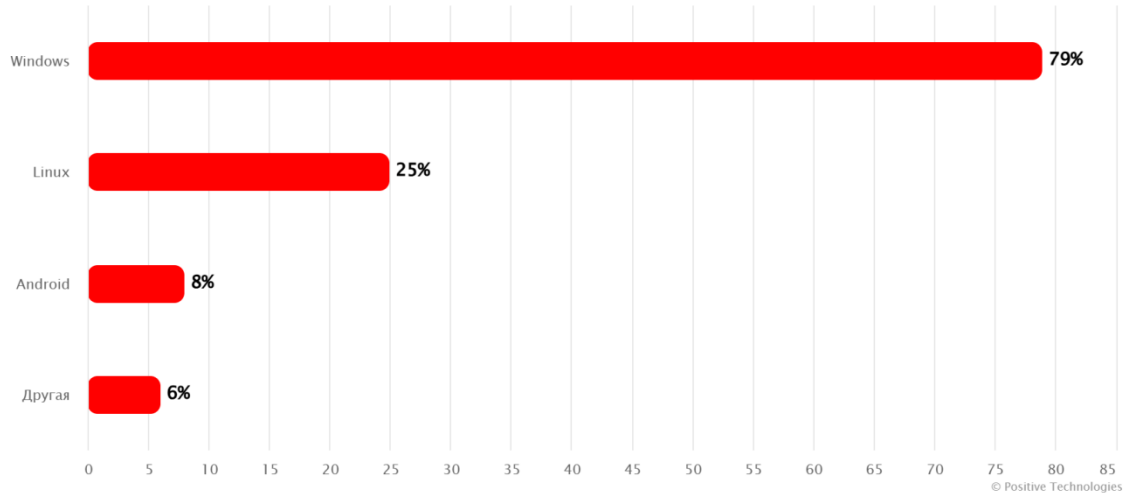


Рисунок 6 – Целевые операционные системы в 4 кв.2024 года [14]

Аналитический обзор разработан с целью выявления текущей ситуации по обеспечению организации функционирования систем мониторинга и реагирования на возможные инциденты ИБ критической информационной инфраструктуры Российской Федерации (далее – КИИ) применительно к ЦИИ, а также возможным направлениям развития нормативных правовых актов (далее – НПА), регламентирующих порядок взаимодействия элементов специально созданной ведомственной организационной структуры, уполномоченной для решения задач системы обеспечения информационной безопасности МЧС России.

Методика составления аналитического обзора

Аналитический обзор составлен по результатам выполненных исследований действующей нормативной правовой базы Российской Федерации в области ИБ, в том числе МЧС России, аналитических отчетов и обзоров в области мониторинга КИИ Российской Федерации, патентных исследований, выполненных в рамках НИР «Кибермониторинг», по результатам обобщения существующих прецедентов организации систем мониторинга и реагирования на возможные инциденты ИБ информационной инфраструктуры различного применения и возможности их технической реализации для дальнейшего использования в МЧС России.

Анализ нормативной правой базы проводился по источникам, размещенных на официальных информационных ресурсах РФ (www.kremlin.ru, pravo.gov.ru) [1, 2], федеральных органов исполнительной власти, уполномоченных в области безопасности (www.fsb.ru) [3], информационной безопасности и защиты информации (fstec.ru) [4], в сфере ГО и ЧС (mchs.gov.ru), а также специальных обзоров правовых документов в сфере ИБ [5].

Анализ результатов деятельности ученых и специалистов в области информационной безопасности КИИ Российской Федерации проводился на основе открытых публикаций, представленных на ресурсах научной электронной библиотеки (elibrary.ru) [6], государственной системы регистрации научных работ (gisnauka.ru) [7], государственной системы регистрации объектов интеллектуальной собственности (fips.ru) [8], государственной системы регистрации отечественного программного обеспечения (reestr.digital.gov.ru) [9].

Анализ актуальных угроз и уязвимостей информационной безопасности проводился на основе официальных баз данных государственных органов (bdu.fstec.ru) [10] и российских организаций, специализирующихся в сфере ИБ (threats.kaspersky.com) [11].

Анализ существующих прецедентов организации систем мониторинга и реагирования на возможные инциденты ИБ информационной инфраструктуры проводился с учетом методических подходов и на основе доступных данных аналитических отчетов, выполненных в Российской Федерации различными организациями [12-18].

Методика обзора Банка России сфокусирована на финансовом секторе, инцидентах операционной деятельности и подразделения ФинЦЕРТ-регулярной оценки ландшафта угроз, существующей практике повышения осведомленности представителей финансового рынка и превентивным мерам в области информационной безопасности [12].

Подход группы BI.ZONE Threat Intuelligence основан на исследовании особенностей киберландшафта (киберугроз, мотивации, атакуемых отраслей, методах доступа техники атак), профилирован по группировкам и методам киберпреступников [13].

Методический подход Positive Technologies исследования актуальных угроз ИБ основан как на собственном опыте расследований инцидентов, так и на иных источниках информации об изменении ландшафта киберугроз [14].

Экспертно-аналитический центр ГК InfoWatch формирует аналитические отчеты на основе собственного методического аппарата сбора, обработки и анализа сведений об утечках информации и собственной базы утечек информации, которая ведется с 2004 года [15].

Методика лучших практик для стран-участниц BRICS при проведении тестирования информационной безопасности и оценки проникновения и уязвимости базируется на общей подходах структуризации рекомендаций, принятых в международных организациях [16].

Компанией Инфосистемы Джет при составлении обзора рынка ИБ использован кластерный подход при формировании ландшафта средств и сервисов защиты информации (далее – СЗИ), представленный на Рисунке 7, которые сгруппированы по направлениям аналогично решаемых задач (Рисунок 8) [17].

Институт статистических исследований и экономики знаний НИУ ВШЭ исследования применения искусственного интеллекта в области кибербезопасности провел на основе методов опроса и обработки сведений от организаций различных отраслей экономики [18].

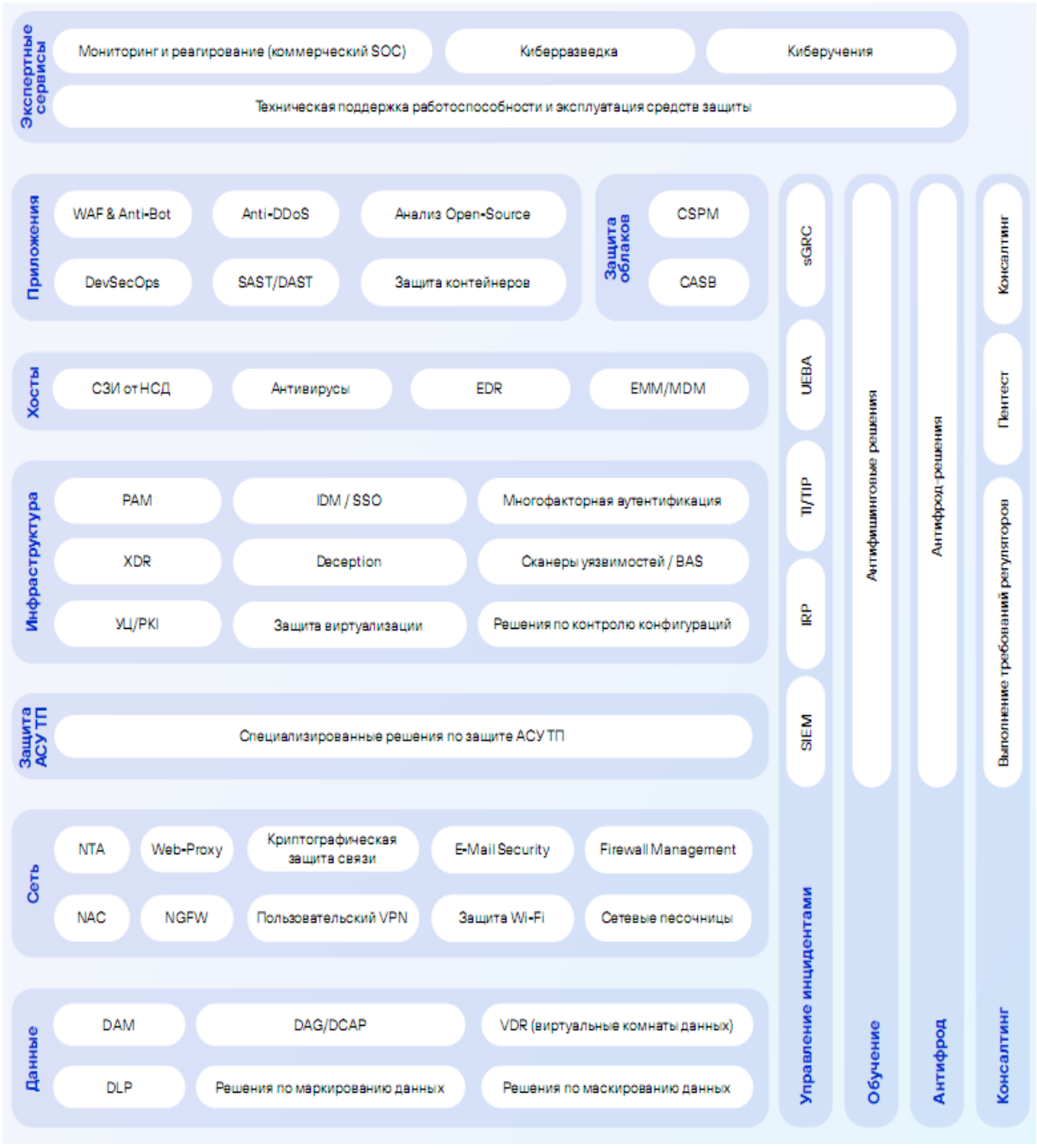


Рисунок 7 – Ландшафт средств защиты информации и сервисов Инфосистемы Джет [17]

Направление	Подсистемы
Сетевая безопасность	NGFW, криптографическая защита каналов связи, NAC[1], NTA[2], Web Proxy, Firewall Management[3], пользовательский VPN, однонаправленные шлюзы
Защита АСУ ТП	Проекты по комплексной защите АСУ ТП
Антифрод	Проекты и решения по автоматическому обнаружению признаков внутреннего и внешнего мошенничества
Мониторинг, реагирование и управление ИБ	SIEM[4], SOAR[5], TI[6]/TIP, sGRC[7]
Защита от вредоносного кода и целенаправленных атак	Сетевые песочницы, EDR[8], XDR, антиспам, антивирусы, СЗИ от НСД, Deception Tools[9], решения по защите виртуализации, EMM[10]

Рисунок 8 – Подсистемы и сервисы защиты информации по направлениям [17]

Институт статистических исследований и экономики знаний НИУ ВШЭ исследования применения искусственного интеллекта в области кибербезопасности провел на основе методов опроса и обработки сведений от организаций различных отраслей экономики [18].

Результаты исследования

Требования к мониторингу и реагированию на возможные инциденты информационной безопасности в ЦИИ, созданной в соответствии с Приказом МЧС России от 13.02.2020 №86, и уровню их технической реализации изложены в ряде НПА МЧС России, например, Приказах МЧС России от 10.03.2022 №178 и от 20.07.2022 № 725.

Основные положения указанных ведомственных НПА касаются организационной структуры, регламентации мониторинга и реагирования на компьютерные инциденты (КИ), правил взаимодействия с другими организациями, применения технических и программных средств ЦИИ, методического обеспечения мероприятий (работ) сил и средств системы обеспечения информационной безопасности МЧС России (Рисунок 9).

Рисунок 9 – Инфологическая схема положений ведомственных НПА

Анализ требований к текущему состоянию мониторинга и реагирования, сложившиеся условия и факторы воздействия на КИИ Российской Федерации, в том числе на ЦИИ МЧС России, выявил ряд аспектов, существенно влияющих на определение и оценку технического уровня разработок в соответствующей области техники:

✓ **особенности регламентации терминологии в области инцидентов информационной безопасности ЦИИ**

Перечень НПА, применительно к обеспечению информационной безопасности ЦИИ, содержит более 160 документов, которые по статусу распределены по 9 группам (Рисунок 10), в том числе:

Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ;

Указ Президента Российской Федерации от 13.06.2024 № 500 «О внесении изменений в Указ Президента Российской Федерации от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»;

Постановление Правительства РФ от 17.02.2018 № 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;

Приказ ФСТЭК России от 20.04.2023 № 69 «О внесении изменений в Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования, утвержденные приказом ФСТЭК России от 21 декабря 2017 г. № 235»;

Приказ ФСБ России от 06.05.2019 № 196 «Об утверждении требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты»;

НКЦКИ. Обобщенные рекомендации по минимизации возможных угроз информационной безопасности информационным ресурсам РФ ALRT-20220329.1 от 29.03.2022;

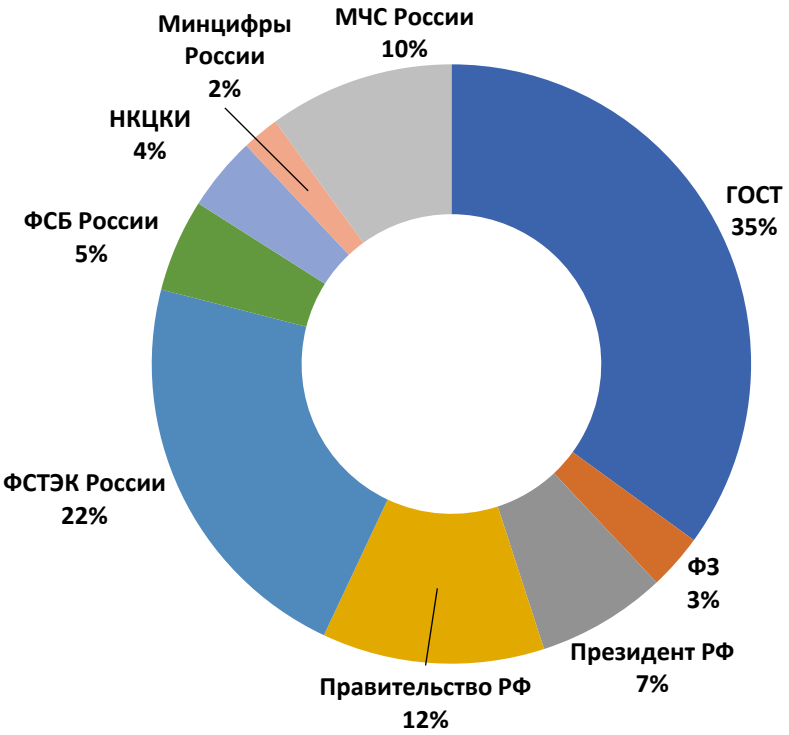


Рисунок 10 – Нормативная правовая база применительно к ИБ ЦИИ

Приказ Минцифры России от 18.01.2023 № 21 «Об утверждении Методических рекомендаций по переходу на использование российского программного обеспечения, в том числе на значимых объектах критической информационной инфраструктуры Российской Федерации, и о реализации мер, направленных на ускоренный переход органов государственной власти и организаций на использование российского программного обеспечения в Российской Федерации»;

Приказ МЧС России от 20.07.2022 № 725 «О мониторинге информации, обрабатываемой в цифровой информационной инфраструктуре МЧС России»;

ГОСТ Р 59547-2021 «Защита информации. Мониторинг информационной безопасности. Общие положения».

Терминологическая ясность является одним из проблемных вопросов для специалистов в области ИБ ЦИИ при значительном объеме требований различных НПА, которая позволяет на практике более точно реализовывать требования государственных регуляторов в области защиты информации и обеспечения информационной безопасности и отчетность (Рисунки 11-12).

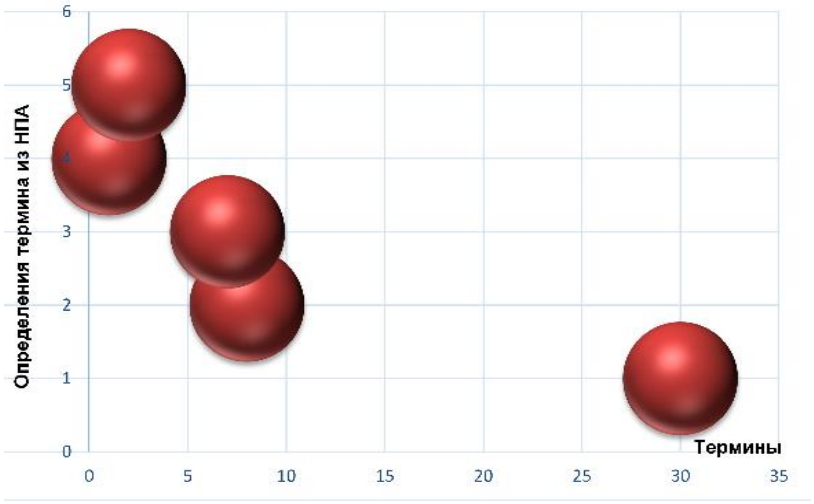


Рисунок 11 – Определения терминов в сфере ИБ

Рисунок 12 – Взаимосвязь терминов «Компьютерные атаки и компьютерные инциденты» (ГОСТ Р 59709-2022)

Использование англо-американских терминов в области ИБ, в том числе в российской информационной сфере, обусловливают актуальность согласованности терминов и гармонизации в противоречивых интеграционных и дезинтеграционных процессах в развитии русской и англо-саксонской терминосистем.

Безусловная зависимость ведомственных НПА от обязательных нормативных правовых требований государственных регуляторов в сфере защиты информации и обеспечения информационной безопасности требует полного и точного отражения в руководящих документах МЧС России содержания представленных в них правовых понятий и положений.

Существующий терминологический и понятийный аппарат и построенные на его основе ведомственные нормативные предписания должны быть в определённой гармонизации.

✓ регламентация стадийности единого структурированного подхода к организации и ведению деятельности по управлению КИ, взаимосвязанной с общей деятельностью по обеспечению ИБ в целом, направленного на обеспечение эффективного реагирования на КИ

Организация и ведение деятельности по управлению КИ регламентированы в Российской Федерации в рамках единого структурированного подхода, взаимосвязанного с общей деятельностью по обеспечению ИБ в целом и направленного на обеспечение эффективного реагирования на КИ (Рисунок 13).

Сущность регламентированных требований к управлению КИ изложена, например, в ГОСТ Р 59710, ГОСТ Р 59711, ГОСТ Р 59712.

✓ уровень регламентации требований ФОИВ, уполномоченного в области безопасности, к средствам обнаружения КА, предназначенным для управления сбором и анализом данных о регистрируемых событиях ИБ и иных данных с целью своевременного выявления КИ, произошедших, в том числе в результате КА

Требования к средствам обнаружения КА регламентированы в Российской Федерации в части перечня и содержания выполняемых функций сбора и первичной обработки событий в области нарушений ИБ, их первоначального и повторного анализа.

Сущность регламентированных требований к средствам обнаружения КА изложена в приложении к Приказу ФСБ России от 06.05.2019 №196.

✓ уровень регламентации требований ФОИВ, уполномоченного в области безопасности, к средствам поиска признаков КА в сетях электросвязи (средства ППКА), предназначенным для обнаружения в сетях электросвязи, используемых для организации взаимодействия информационных ресурсов, признаков КА по значениям служебных полей протоколов сетевого взаимодействия, а также осуществления сбора, накопления и статистической обработки результатов такого обнаружения

Требования к средствам предупреждения о КА регламентированы в Российской Федерации в части перечня и содержания выполняемых функций сбора и обработки сведений об инфраструктуре информационных ресурсов и справочной информации, а также сведений об уязвимостях, формирования рекомендаций и ведении учета.

Сущность регламентированных требований к средствам предупреждения о КА изложена в приложении к Приказу ФСБ России от 06.05.2019 №196.

✓ уровень регламентации требований ФОИВ, уполномоченного в области безопасности, к средствам обмена и криптографическим СЗИ, необходимой субъектам КИИ при обнаружении, предупреждении и (или) ликвидации последствий КА

Требования к средствам ликвидации последствий КА регламентированы в Российской Федерации в части перечня и содержания выполняемых функций учета и обработки КИ, управления реагированием, взаимодействия с НКЦКИ и сопровождения пользователей.

Сущность регламентированных требований к средствам ликвидации последствий КА изложена в приложении к Приказу ФСБ России от 06.05.2019 №196.

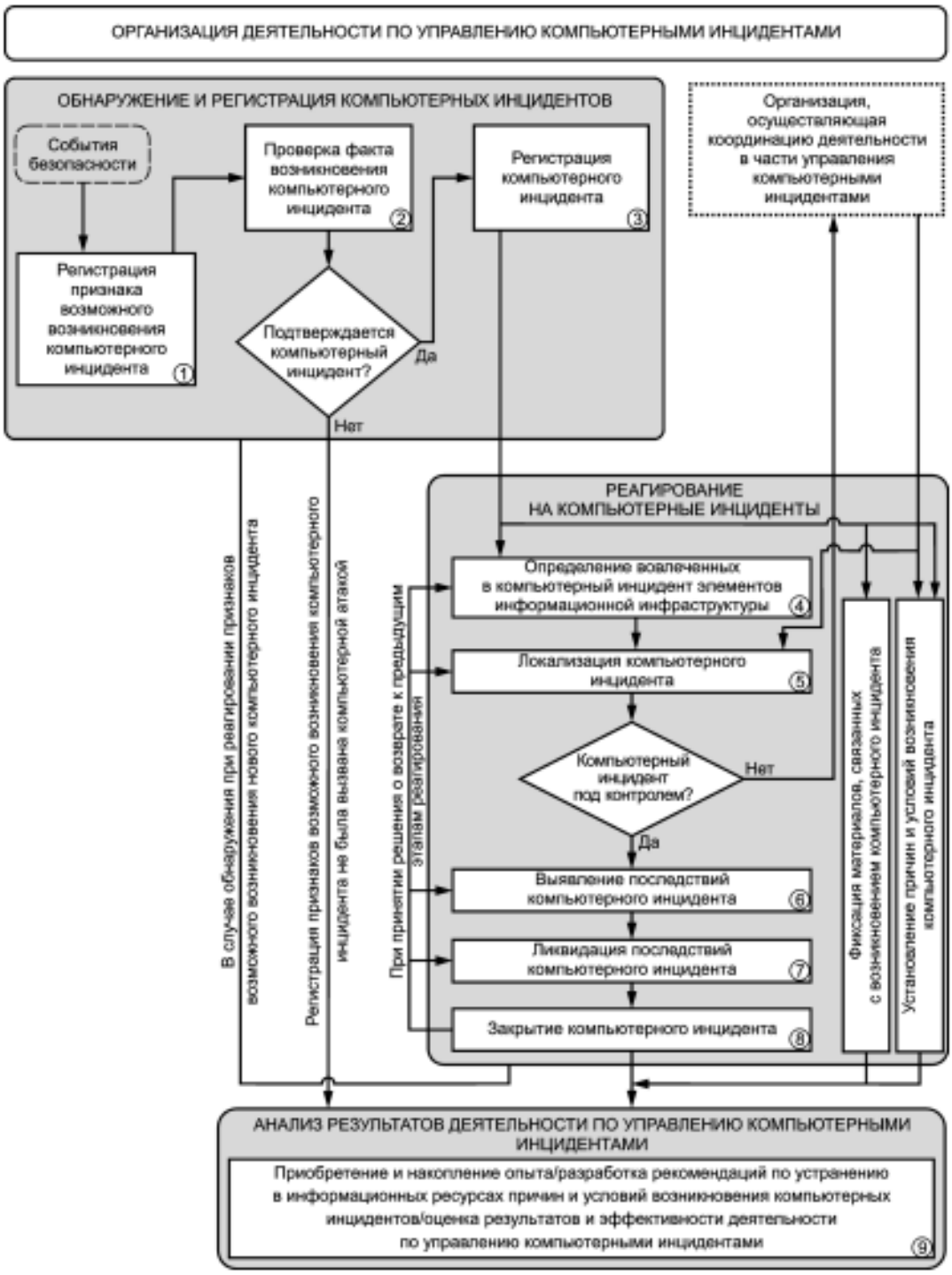


Рисунок 13 – Организация и ведение деятельности по управлению КИ (ГОСТ Р 59710-2022)

✓ **уровень регламентации требований ФОИВ, уполномоченного в области безопасности, к средствам поиска признаков КА в сетях электросвязи (средства ППКА), предназначенным для обнаружения в сетях электросвязи, используемых для организации взаимодействия информационных ресурсов, признаков КА по значениям служебных полей протоколов сетевого взаимодействия, а также осуществления сбора, накопления и статистической обработки результатов такого обнаружения**

Требования к средствам ППКА регламентированы в Российской Федерации в части перечня и содержания выполняемых функций обнаружения различных признаков КА и

технологических изменений, хранения, анализа, экспорта копий артефактов и уведомления о них.

Сущность регламентированных требований к средствам ППКА изложена в приложении к Приказу ФСБ России от 06.05.2019 №196.

✓ **уровень регламентации требований ФОИВ, уполномоченного в области безопасности, к средствам обмена и криптографическим СЗИ, необходимой субъектам КИИ при обнаружении, предупреждении и (или) ликвидации последствий КА**

Требования к средствам обмена и криптографическим СЗИ регламентированы в Российской Федерации в части перечня и содержания выполняемых функций передачи, приема и обеспечения целостности информации и их сертификации.

Сущность регламентированных требований к средствам обмена и криптографическим СЗИ изложена в приложении к Приказу ФСБ России от 06.05.2019 №196.

✓ **уровень регламентации требований ФОИВ, уполномоченного в области безопасности, к средствам обнаружения, средствам предупреждения и средствам ликвидации последствий в части реализации визуализации, построения сводных отчетов и хранения информации**

Требования к средствам предупреждения и средствам ликвидации последствий регламентированы в Российской Федерации в части перечня и содержания выполняемых функций визуализации, построения сводных отчетов и хранения информации.

Сущность регламентированных требований к средствам предупреждения и средствам ликвидации последствий изложена в приложении к Приказу ФСБ России от 06.05.2019 №196.

1. Способы (методы) мониторинга возможных инцидентов информационной безопасности в информационной инфраструктуре

Способы обнаружения вторжений регламентированы в Российской Федерации и изложены как требования к реализации СОВ.1, в части средств (датчики, анализаторы, база решающих правил), уровня локации объекта (сеть, узел, сегмент информационной системы), локальным НПА; к усилению СОВ.1 (сетевые, локальные, прикладные, РМВ СОВ, защищенности СОВ); базовой меры СОВ.1 (под класс защищенности ИС).

Обновление базы решающих правил регламентировано и изложено как требования к реализации СОВ.2, в части процедур (уведомления, актуализация, контроль целостности), и регламентации в ОРД; требования к усилению СОВ.2 (централизация управления, администрирование БД, регламентации); базовой меры СОВ.2 (под класс защищенности ИС).

Рисунок 14 – Способы обнаружения КА и инцидентов

Сущность регламентированных требований к способам обнаружения вторжений изложена в Методическом документе ФСТЭК России от 11.02.2014.

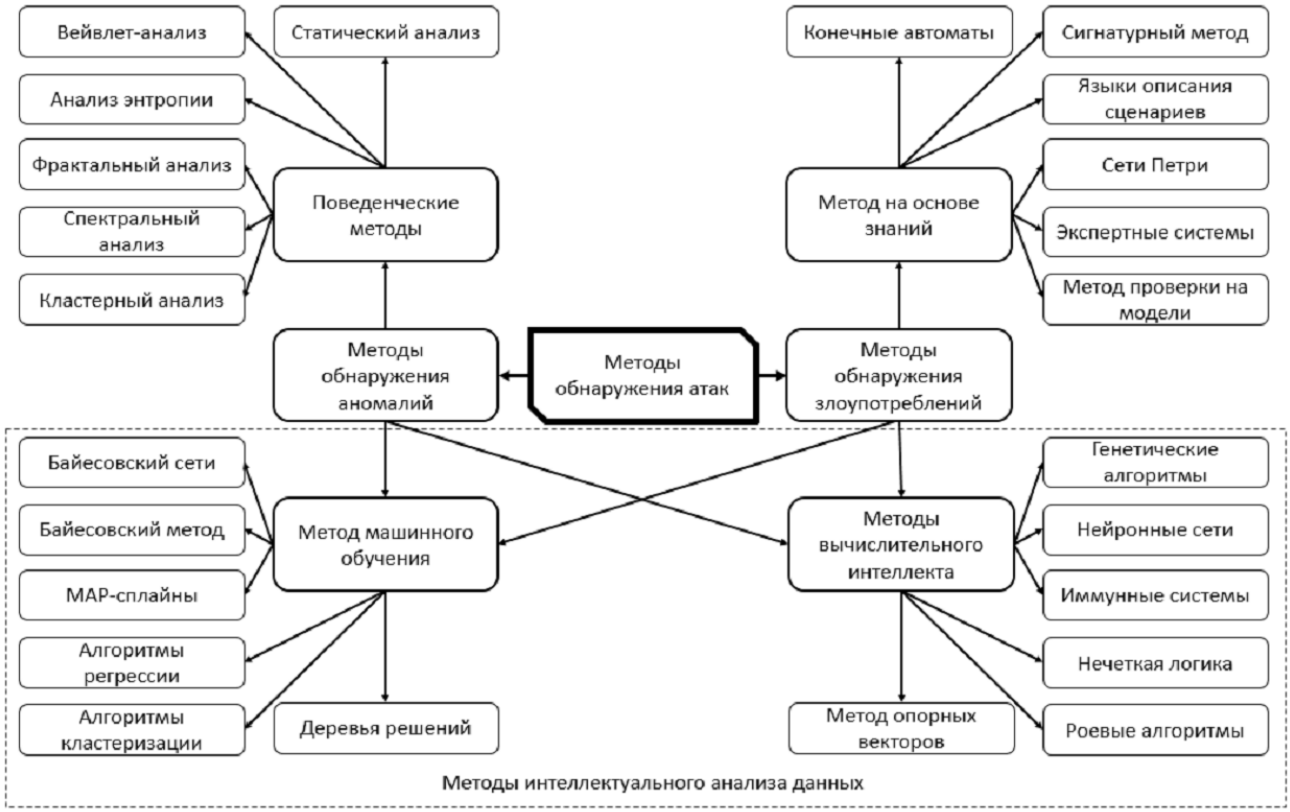


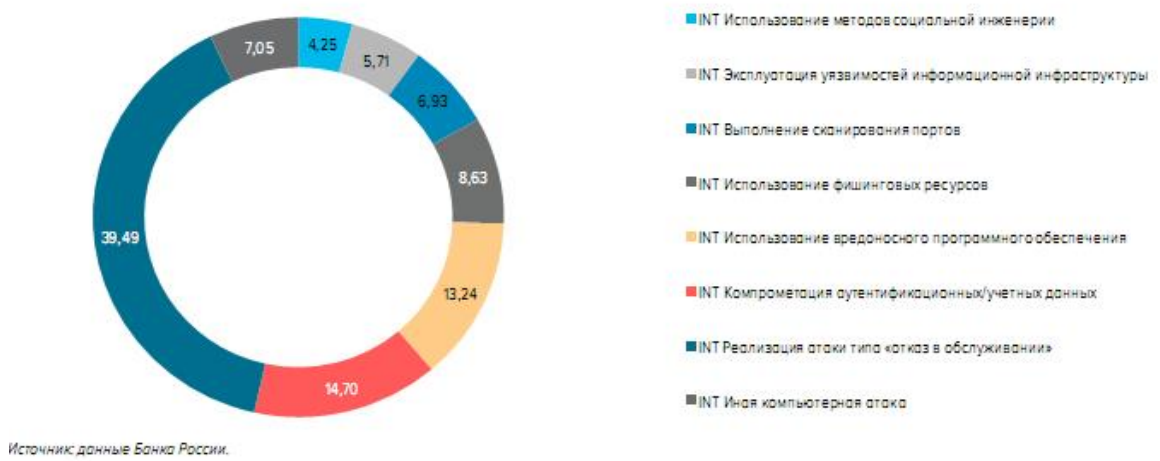
Рисунок 15 – Методы обнаружения КА (StudNet, №11/2020)

Источник: данные Банка России.

Рисунок 16 – Распределение компьютерных атак в финансовой сфере РФ (2024) [12]

В финансовой сфере РФ преобладало ВПО на учетные данные (Trojan., Trojan-PSW.MSIL.Stealer.gen), удаленное управление (Agensla.gen), шифровальщики (Trojan-Ransom) (см. Рисунок 17).

По данным компании BI.ZONE наиболее атакуемыми являются государственные организации и финансовая отрасль, а методы получения доступа – фишинговые рассылки и учетные записи пользователей (Рисунки 18-19) [13].



Источник: данные Банка России.

Рисунок 17 – Типизация компьютерных атак в финансовой сфере РФ (2024) [12]

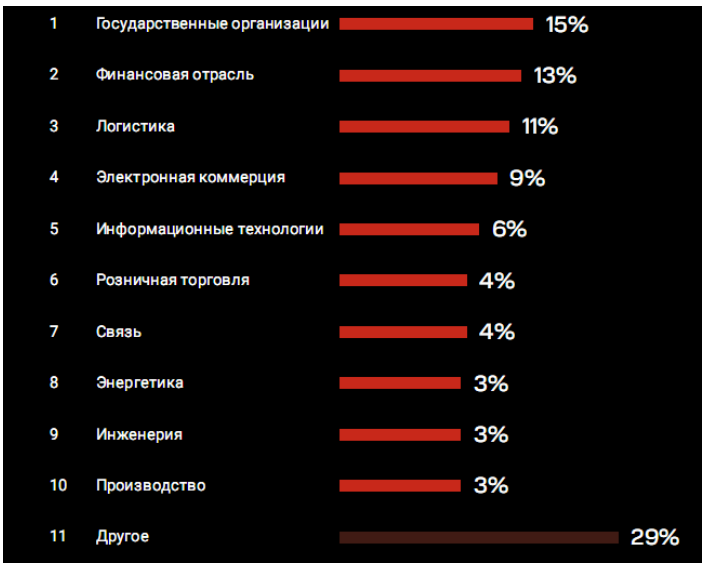


Рисунок 18 – Распределение компьютерных атак в РФ (2024) [13]

Рисунок 19 – Распределение методов атак в РФ (2024) [13]

Схематизация атак на финансовые организации представлена в отчете ЦБ России (Рисунки 20-22) [12].

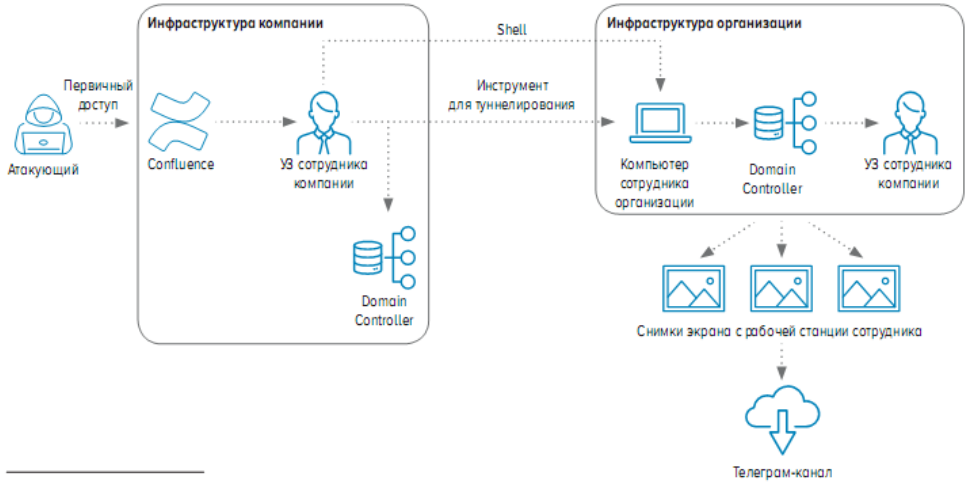


Рисунок 20 – Схема атаки на разработчика автоматизированных банковских систем (2024) [12]

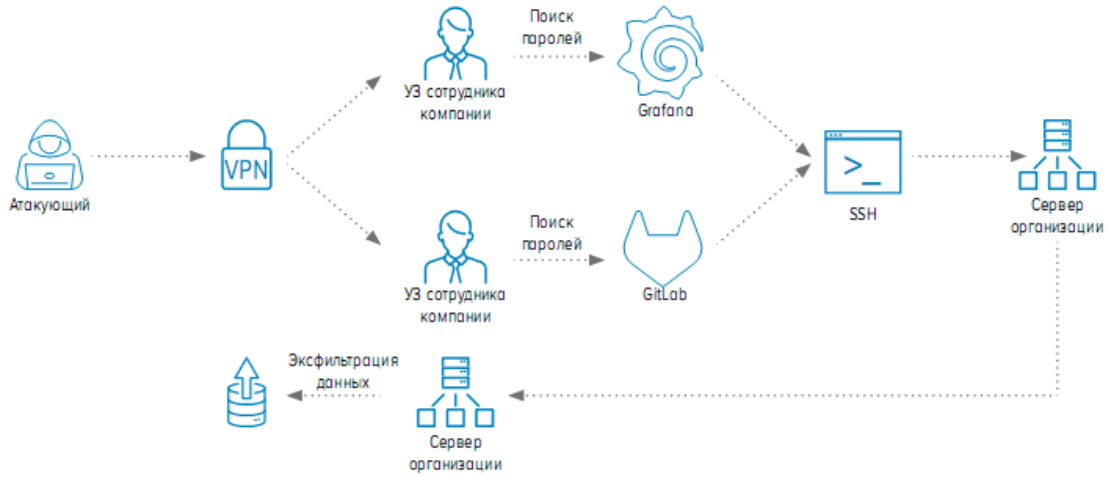


Рисунок 21 – Схема атаки на разработчика финпродуктов РФ (2024) [12]

Рисунок 22 – Схема атак на инфраструктуру организации (ФинЦЕРТ) [12]

Несанкционированный доступ к информационным ресурсам государственных организаций в 2024 году достигался туннелированием трафика и посредством удаленного доступа [13]:

- драйвер WinPmem для создания слепка оперативной памяти, отслеживается активностью одноименных созданных служб, созданием файлов (.rar), загрузкой WinPmem с подписью;
- загрузчик PhantomDL (ВПО), обнаруживается в исполняемых файлов с двойным расширением, специальной команды;
- манипуляции настройками межсетевого экрана, обнаруживается запуском определенного перечня команд;
- письма с замаскированными исполняемыми файлами (в том числе MSC-файлы), обнаруживается по русскоязычному имени с двойным расширением для исполнения;
- сервер NodeJS интерпретатор для удаленного доступа, обнаруживается активностью запуска интерпретатора, выполнением сценариев с удаленных ресурсов и планировщика задач;
- сетевой сканер Slitheris Network Discovery (SoftPerfect Network Scanner), обнаруживается по запуску одноименных файлов;

- средство Adminer управления БД (MySQL, PostgreSQL, SQLite, MS SQL и Oracle), обнаруживается по активности wget или cURL, одноименных процессов;
- средство ADRecon сбора данных Active Directory, обнаруживается активностью одноименных файлов и папок;
- средство MeshCentral удаленного управления, обнаруживается исполнением одноименных файлов, созданных служб;
- средство Ngrok обратного проксирования для удаленного доступа AnyDesk, обнаруживается активностью одноименных процессов, файлов, сетевых коммуникаций;
- средство NirCmd взаимодействия с ОС для повышения привилегий, обнаруживаются по исполнению одноименных файлов, определенным параметрам командной строки;
- средство Rclone резервного копирования данных, обнаруживается исполнением одноименных файлов, оригинальной командной строки;
- средство RemCom удаленного управления, обнаруживается исполнением одноименных файлов, созданных каналов и сервисов;
- средство revsocks (rsockstun) обратных SOCKS5-туннелей, обнаруживается в одноименных процессах, файлов, параметрах командной строки;
- средство UltraVNC удаленного управления, обнаруживается в одноименных файлах, задачах планировщика командной строки;
- утилита grabff извлечения паролей в браузерах (Mozilla Firefox, Chrome), обнаруживается по событиям копирования файлов профилей (аутентификационных данных);
- утилита Localtonet для создания туннелей на принципах обратного прокси, обнаруживается активностью одноименных исполняемых файлов, сетевого взаимодействия, файлов пути;
- утилита Mshta для выполнения файлов HTA (Microsoft HTML Application), обнаруживается запуском файлов HT с удаленных ресурсов и определенных папок;
- утилита PAExec управления в корпоративной сети, обнаруживается активностью одноименных исполняемых файлов, созданных служб;
- утилита XenArmor All-In-One Password Recovery Pro восстановления паролей, обнаруживается активностью одноименных исполняемых и создаваемых файлов, процессов;
- утилита wget передачи файлов по сети, обнаруживается при загрузке файлов с расширением определенного перечня;
- утилита WMI (Windows Management Instrumentation) командной строки для сбора данных, удалений копий и управления, отслеживается по параметрам запуска утилиты;
- JAR-файлы интерпретатора команд и сценариев Java, обнаруживается запуском одноименных файлов из определенных папок;

Tor и VPN-сервисы для сохранения анонимности, обнаруживается подключение через службы удаленного доступа с адресов одноименных узлов.

Первоначальный доступ к информационным ресурсам достигался путем эксплуатации уязвимостей общедоступных приложений Atlassian Confluence Data Center и Confluence Server (CVE-2023-22518), ActiveMQ (CVE-2023-46604); Apache Log4j (CVE-2021-44228); Citrix Application Delivery Controller (CVE-2019-19781); Confluence (CVE-2022-26134); Liferay (CVE-2020-7961); Microsoft Exchange (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207, CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065), Openfire (CVE-2023-32315); Oracle WebLogic Server (CVE-2020-14883); Pkexec Local Privilege Escalation (CVE-2021-4034); SaltStack (CVE-2020-11651,и CVE-2020-11652); F5 BIG-IP (CVE-2020-5902); WordPress File Manager (CVE-

2020-25213); в WinRAR (CVE-2023-38831); Zerologon (CVE-2020-1472); и драйверов (CVE-2018-19320, CVE-2018-19322, CVE-2018-19323, CVE-2018-19321, CVE-2019-16098).

2. Системы (средства) мониторинга и реагирования на инциденты информационной безопасности в информационной инфраструктуре

Отечественный рынок систем (средств) мониторинга и реагирования на инциденты ИБ в информационной инфраструктуре российские разработчики заполняют разнообразной продуктовой линейкой.

Отнесение систем (средств) мониторинга и реагирования на инциденты ИБ в информационной инфраструктуре к отечественному регламентировано по разделам и классам, при этом допускается учет продуктов в нескольких классах.

Программное обеспечение систем мониторинга и реагирования (ПО) регистрируется в соответствии с классификаторами и приказом Минцифры России от 22.09.2020 №486.

Раздел 02 (Системное программное обеспечение) содержит 3587 записей, а класс 02.08 (Средства мониторинга и управления) – 1819 записей (Рисунок 23).

Раздел 03 (Средства обеспечения информационной безопасности) содержит 1168 записей (Рисунок 24).

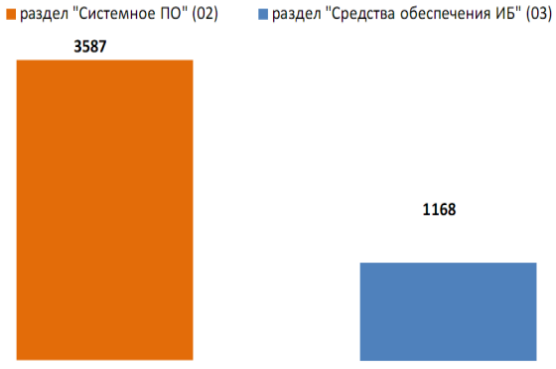


Рисунок 23 – Разделы 02 и 03 ПО Реестра Минцифры России

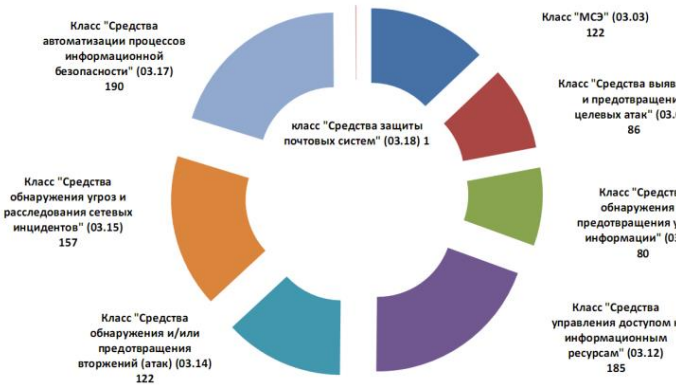


Рисунок 24 – Классы раздела 03 ПО Реестра Минцифры России

Класс 03.02 (Средства управления событиями информационной безопасности" для выявления и предотвращения КА) содержит 146 записей. Класс 03.03 (Межсетевые экраны, МСЭ) содержит 122 записи. Класс 03.07 (Средства выявления и предотвращения целевых атак) содержит 86 записей. Класс 03.09 (Средства обнаружения и предотвращения утечек информации) содержит 80 записей. Класс 03.12 (Средства управления доступом к информационным ресурсам) содержит 185 записей. Класс 03.14 (Средства обнаружения и/или предотвращения вторжений (атак)) содержит 122 записи. Класс 03.15 (Средства обнаружения угроз и расследования сетевых инцидентов) содержит 157 записей. Класс 03.17 (Средства автоматизации процессов информационной безопасности) содержит 190 записей. Класс 03.18 (Средства защиты почтовых систем) содержит 1 запись.

Наибольшее количество зарегистрированного ПО относится к средствам автоматизации процессов информационной безопасности, средствам управления доступом к информационным ресурсам, средствам обнаружения угроз и расследования сетевых инцидентов, что является следствием эволюционного процесса актуальности проблем.

Программно-аппаратные комплексы систем мониторинга и реагирования (ПАК) регистрируются в соответствии с классификаторами и приказом Минцифры России от 31.01.2023 № 62.

Раздел 03 (ПАК мониторинга и управления) содержит 74 записи (Рисунок 25).

Класс 03.01 (ПАК управления информационными ресурсами) содержит 3 записи. Класс 03.02 (ПАК мониторинга и управления) диагностики, оценки состояния, оповещения и управления содержит 61 записей. Класс 03.03 (ПАК интеллектуального управления) содержит 0 записей. Класс 03.14 (ПАК сбора, анализа и визуализации информации различных сред и процессов) содержит 3 записи. Наибольшее количество зарегистрированных ПАК мониторинга и управления относятся к традиционным системам различного назначения.

Раздел 15 (ПАК обеспечения ИБ) содержит 155 записей.

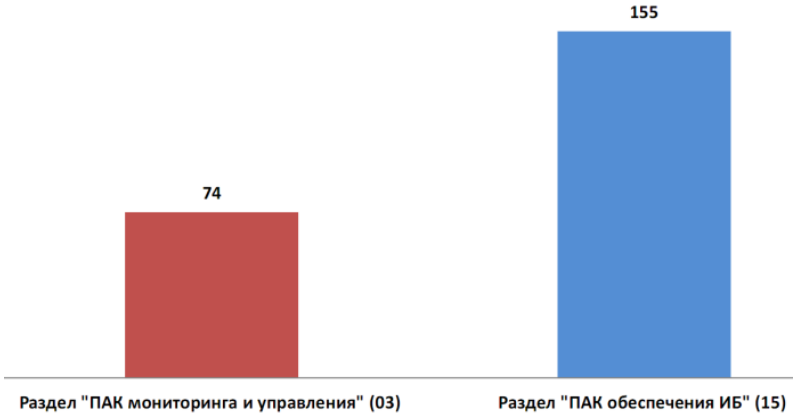


Рисунок 25 – Разделы 03 и 15 ПАК Реестра Минцифры России

Диспропорции в распределении количества изделий по разделам 03 и 15 обусловлено резким ростом внимания к разрешению проблем в области информационной безопасности, в том числе решений в составе существующих ПАК систем различного назначения (Рисунки 26-27).

Рисунок 26 – Раздел 03 ПАК Реестра Минцифры России

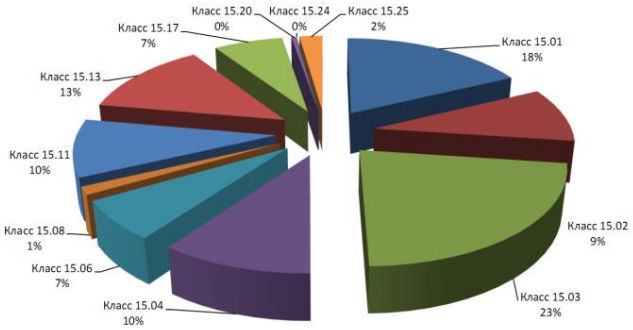


Рисунок 27 – Раздел 15 ПАК Реестра Минцифры России

Класс 15.01 (ПАК защиты от НСД к информации некриптографическими методами) содержит 40 записей. Класс 15.02 (ПАК управления событиями ИБ", в т.ч. выявления и предотвращения КА) содержит 21 запись. Класс 15.03 (ПАК МСЭ) содержит 51 запись. Класс 15.04 (ПАК фильтрации негативного контента) содержит 23 записи. Класс 15.06 (ПАК выявления целевых КА, в т.ч. DDoS и противодействия им) содержит 15 записей. Класс 15.08 (ПАК обнаружения и предотвращения утечек информации) содержит 3 записи. Класс 15.11 (ПАК управления доступом к информационным ресурсам) содержит 22 записи. Класс 15.13 (ПАК обнаружения и/или предотвращения вторжений (атак), в т.ч. уровня сети или узла) содержит 29 записей. Класс

15.17 (ПАК обнаружения угроз и расследования сетевых инцидентов) содержит 15 записей. Класс 15.20 (ПАК средств автоматизации процессов ИБ) содержит 1 запись. Класс 15.24 (ПАК безопасной разработки ПО) содержит 0 записей. Класс 15.25 (ПАК конвертации данных из внутреннего контура ИС для внешнего) содержит 5 записей.

Наибольшее количество зарегистрированных ПАК обеспечения информационной безопасности относится к межсетевому экранированию, защите от НСД, обнаружению (предотвращению) вторжений (атак) на уровне сети или узла, в то время как решениям по расследованию сетевых инцидентов, выявлению и предотвращению целевых атак уделено примерно в 2 раза меньше внимания, что является временным явлением текущего состояния.

Прогнозные оценки ИБ-технологий подтверждают сложившуюся ситуацию текущего состояния жизненного цикла технологий информационной безопасности на примере АСУ ТП, которые приведены в [19] (Рисунки 28-29).

Рисунок 28 – Состояния ИБ-технологий АСУ ТП [19]

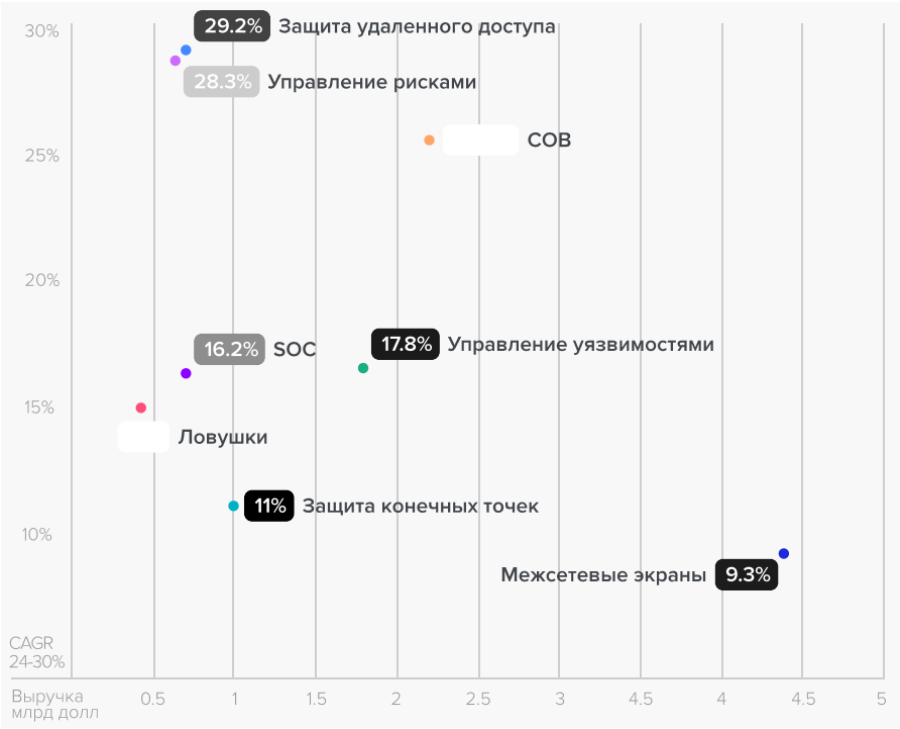


Рисунок 29 – Расходы на ИБ-технологии АСУ ТП и их рост до 2030 года [19]

Характеристика существующих решений для мониторинга и реагирования на инциденты информационной безопасности представлены в Таблицах 1-7, Рисунках 30-39.

Таблица 1 – Характеристика решений, зарегистрированных в Минцифры России

АО "Лаборатория Касперского"	
Kaspersky DDoS Protection for xSP (Коллектор, Центр очистки, Сенсор, ЛК (Портал))	Класс 03.07 (Средства выявления и предотвращения целевых атак). Реестровая запись №10709 от 08.06.2021. Распознание атаки на Сервис ы/ сервер(ы) с IP-адресами, реагирование: через систему мониторинга DDoS Intelligence и посредством инфраструктуры «Лаборатории Касперского».
Kaspersky DDoS Protection for Networks (Коллектор, Центр очистки, Сенсор, ЛК (Портал))	Класс 03.07 (Средства выявления и предотвращения целевых атак). Реестровая запись №10708 от 08.06.2021. Распознание атаки на Сервис ы/ сервер(ы) с IP-адресами, реагирование: через систему мониторинга DDoS Intelligence и посредством инфраструктуры «Лаборатории Касперского».
Kaspersky Unified Monitoring and Analysis Platform with High Availability (KUMA) класс SIEM	03.02 Средства управления событиями информационной безопасности. Реестровая запись №10055 от 02.04.2021. Централизованный сбор, обработка (анализ и корреляция событий ИБ) и хранение событий ИБ, анализ и корреляция поступающих данных, поиск по полученным событиям, создание уведомлений о выявлении признаков угроз ИБ.
Kaspersky Unified Monitoring and Analysis Platform GosSOPKA compatible with High Availability	03.02 Средства управления событиями информационной безопасности. Реестровая запись №10058 от 02.04.2021. Централизованный сбор и анализ журналов регистрации, корреляцию событий ИБ, оповещение об инцидентах, объединяя решения Kaspersky в единую платформу
Kaspersky Unified Monitoring and Analysis Platform GosSOPKA – compatible with Netflow and HA support	03.02 Средства управления событиями информационной безопасности. Реестровая запись №10060 от 06.09.2021. Централизованный сбор и анализ журналов регистрации, корреляцию событий ИБ в реальном времени, оповещение об инцидентах, объединяя решения Kaspersky в единую платформу
Kaspersky EDR Expert. Может входить в состав Kaspersky Anti Targeted Attack (KATA).	Мониторинг и визуализацию стадий расследования, обнаружение угроз на базе индикаторов компрометации (IoC), Yara-правил и уникальных индикаторов атак (IoA), анализа первопричин. Процесс расследования с ретроспективным анализом, обнаружения сопоставляются с базой знаний MITRE ATT&CK.
Kaspersky Anti Targeted Attack **(KATA)**. Может содержать модуль NDR (Network Detection & Response).	Реестровая запись №8350 от 30.12.2020. Платформа анализа сетевого трафика и комплексной защиты от сложных угроз и целевых атак. Контроль точки входа угроз (сеть, веб-трафик, электронная почта), проверка потенциально вредоносные объекты в песочнице. KATA с модулями NDR и KEDR Expert покрывает более 460 TTP матрицы MitreATTACK. Модуль NDR расширяет функции выявления сетевых угроз (глубокий анализ сетевого трафика, применение правил детектирования, индикаторов компрометации, ретроспективного анализа, карта сети и таблица сетевых сессий, определение и разбор протоколов, проактивный поиск угроз трафику, реагирование на сетевых устройствах и межсетевых экранах.

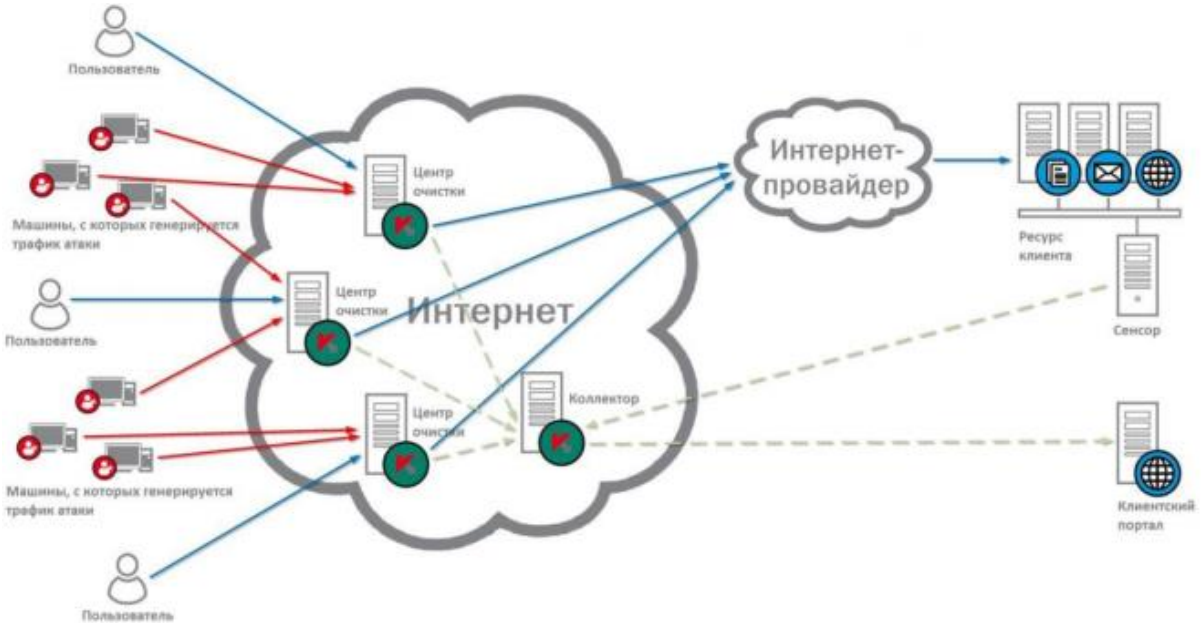


Рисунок 30 – Организационная архитектура Kaspersky DDoS Protection for Networks (https://www.kaspersky.ru)

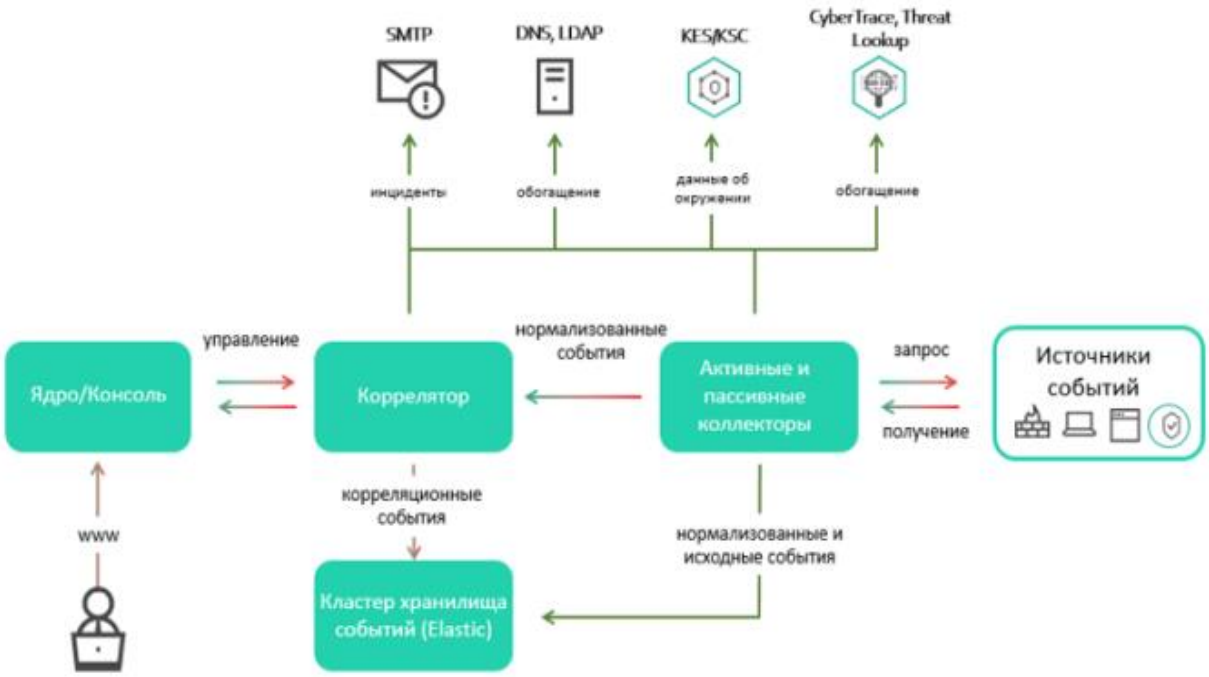


Рисунок 31 – Техническая архитектура Kaspersky Unified Monitoring and Analysis Platform (https://www.kaspersky.ru)

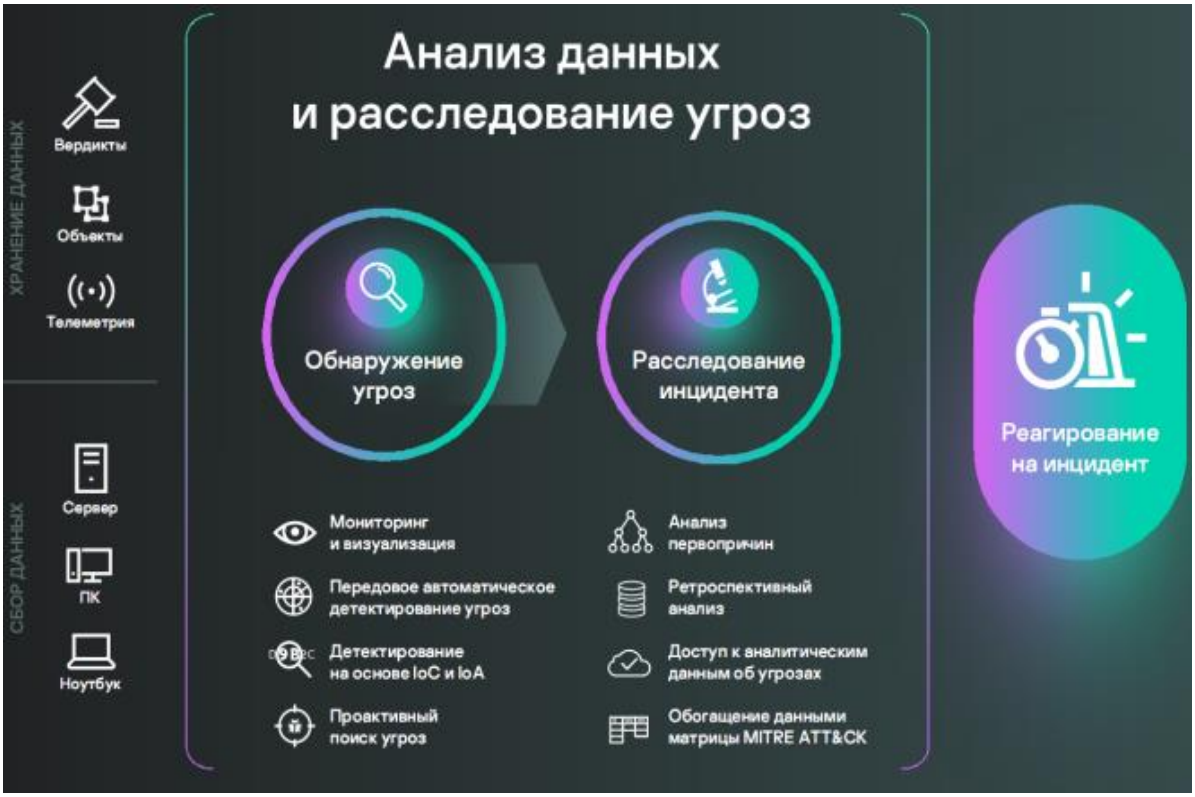
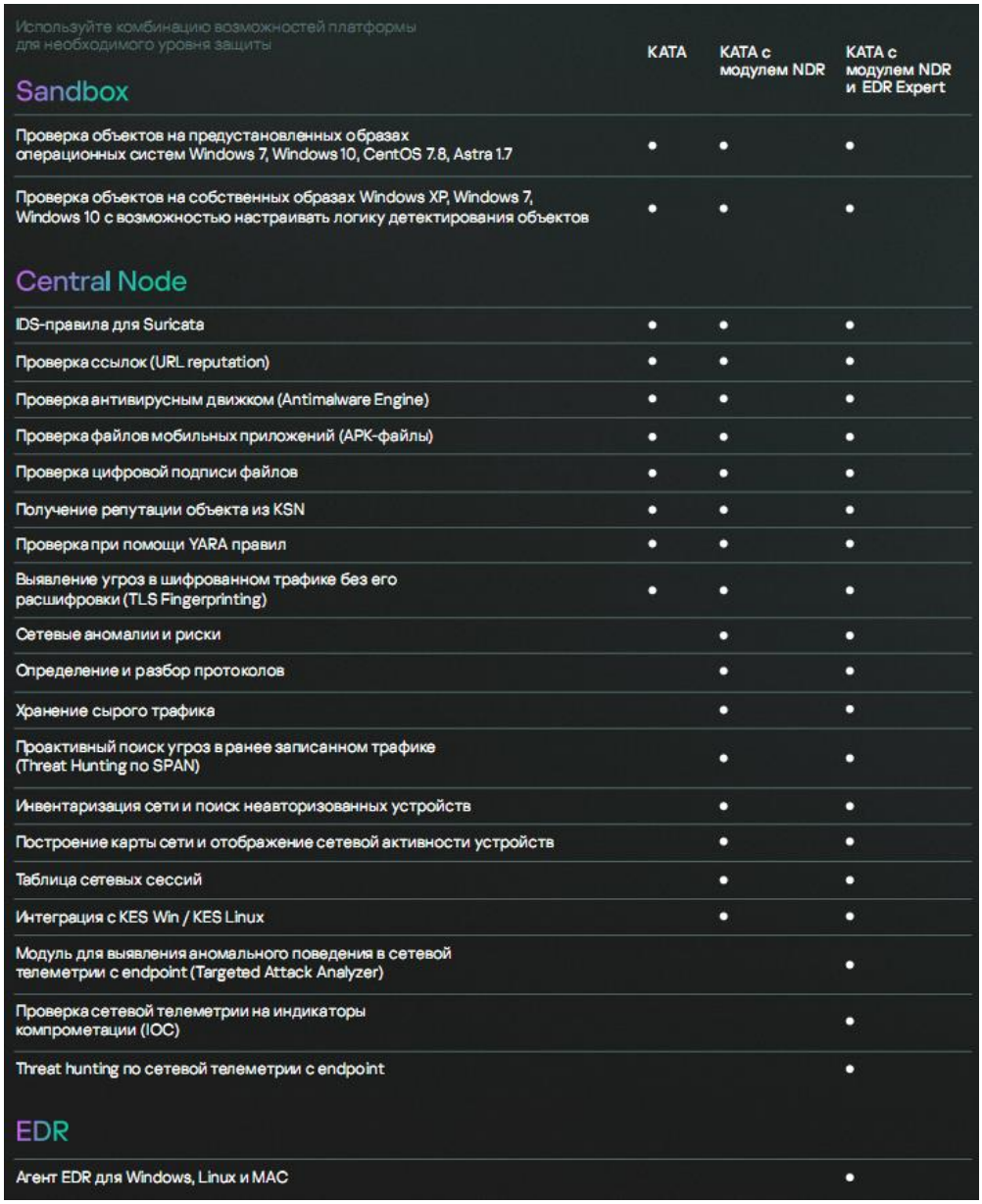


Рисунок 32 – Функциональная архитектура Kaspersky EDR Expert (https://www.kaspersky.ru)



Используйте комбинацию возможностей платформы для необходимого уровня защиты	KATA	KATA с модулем NDR	KATA с модулем NDR и EDR Expert
Sandbox			
Проверка объектов на предустановленных образах операционных систем Windows 7, Windows 10, CentOS 7.8, Astra 1.7	•	•	•
Проверка объектов на собственных образах Windows XP, Windows 7, Windows 10 с возможностью настраивать логику детектирования объектов	•	•	•
Central Node			
IDS-правила для Suricata	•	•	•
Проверка ссылок (URL reputation)	•	•	•
Проверка антивирусным движком (Antimalware Engine)	•	•	•
Проверка файлов мобильных приложений (APK-файлы)	•	•	•
Проверка цифровой подписи файлов	•	•	•
Получение репутации объекта из KSN	•	•	•
Проверка при помощи YARA правил	•	•	•
Выявление угроз в шифрованном трафике без его расшифровки (TLS Fingerprinting)	•	•	•
Сетевые аномалии и риски		•	•
Определение и разбор протоколов		•	•
Хранение сырого трафика		•	•
Проактивный поиск угроз в ранее записанном трафике (Threat Hunting по SPAN)		•	•
Инвентаризация сети и поиск неавторизованных устройств		•	•
Построение карты сети и отображение сетевой активности устройств		•	•
Таблица сетевых сессий		•	•
Интеграция с KES Win / KES Linux		•	•
Модуль для выявления аномального поведения в сетевой телеметрии с endpoint (Targeted Attack Analyzer)			•
Проверка сетевой телеметрии на индикаторы компрометации (IOC)			•
Threat hunting по сетевой телеметрии с endpoint			•
EDR			
Агент EDR для Windows, Linux и MAC			•

Рисунок 33 – Характеристики Kaspersky Anti Targeted Attack (KATA) с различными модулями (https://www.kaspersky.ru)

Таблица 2 – Характеристика решений UserGate

Общество с ограниченной ответственностью «Юзергейт»	
UserGate SIEM (SIEM)	Класс 03.02 (Средства управления событиями информационной безопасности). Реестровая запись №25528 от 20.12.2024. Решение на основе UserGate Log Analyzer (LogAn) с функциями систем SIEM (Security Information and Event Management) и IRP (Incident Response Platform): SIEM & IRP (сбор логов и событий, поиск инцидентов и реагирования на них); SOAP (Security Orchestration, Automation and Response) интеграция в экосистеме UserGate SUMMA; TI (актуализация инцидентов с различными индикаторами компрометации из разных источников)
UserGate Management Center UGMC	Класс 03.17 (Средства автоматизации процессов информационной безопасности). Реестровая запись №9311 от 01.03.2021. Вспомогательный компонент для универсального межсетевого экрана UserGate, который позволяет управлять большим количеством устройств.
UserGate LogAn	Класс 03.02 (Средства управления событиями информационной безопасности). Реестровая запись №6919 от 01.09.2020. Агрегирует данные от различных устройств, осуществляет мониторинг событий и создает отчеты

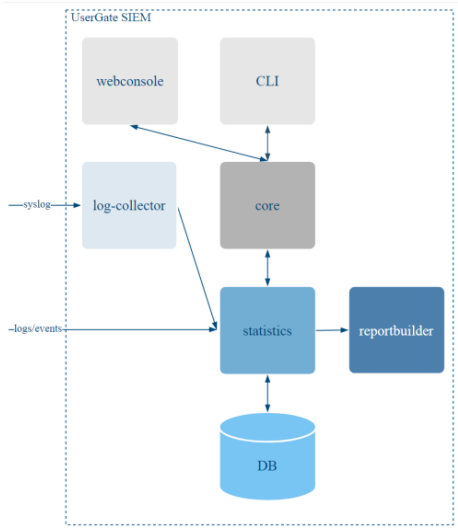


Рисунок 34 – Архитектура UserGate SIEM

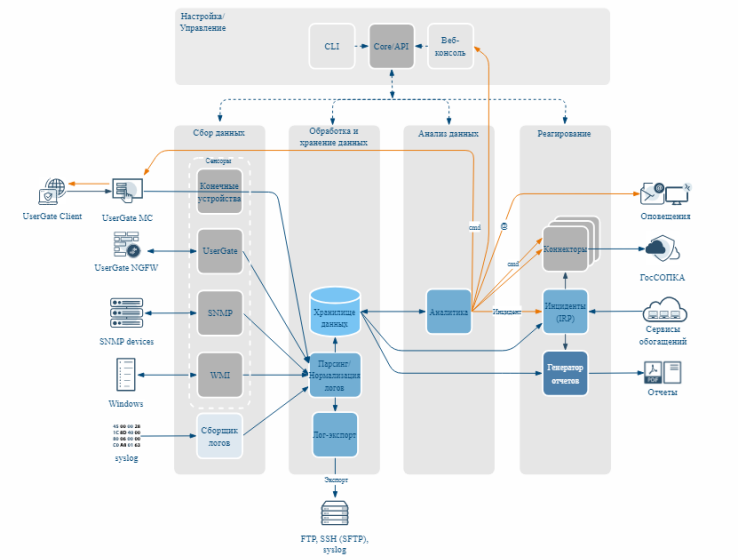


Рисунок 35 – Функциональная модель UserGate SIEM (https://docs.usergate.com)

Таблица 3 – Характеристика решений R-Vision

Общество с ограниченной ответственностью «Р-Вижн»	
R-Vision SIEM Система управления событиями информационной безопасности R-Vision Security Information and Event Management	Класс 03.02 (Средства управления событиями информационной безопасности), 03.14 Средства обнаружения и/или предотвращения вторжений (атак), 03.15 (Средства обнаружения угроз и расследования сетевых инцидентов). Реестровая запись №21323 от 08.02.2024. Единый центр работы с событиями ИБ за счет автоматизации процессов их обработки и анализа, включая: сбор, нормализацию, фильтрацию, хранение и передачу событий ИБ, мониторинг и анализ событий ИБ, управление правилами корреляции, оповещение по фактам правил корреляции
R-Vision VM Система автоматизации процесса управления уязвимостями R-Vision Vulnerability Management	Класс 03.17 (Средства автоматизации процессов информационной безопасности); 03.15 (Средства обнаружения угроз и расследования сетевых инцидентов). Реестровая запись № 21948 от 20.03.2024. Выявляет информационные активы, сканирует их на уязвимости и выдает рекомендации по итогам сканирования.
R-Vision UEBA Платформа мониторинга угроз	Класс 03.02, 03.14, 03.15. Реестровая запись №19431 от 04.10.2023. Реализация поведенческого анализа объектов защиты, в т.ч. сбор и анализ событий ИБ, идентификацию объектов защиты, формирование шаблонов поведения, выявление аномалий, построение хронологии событий, связанных с объектом защиты, оповещение при обнаружении аномальной активности.

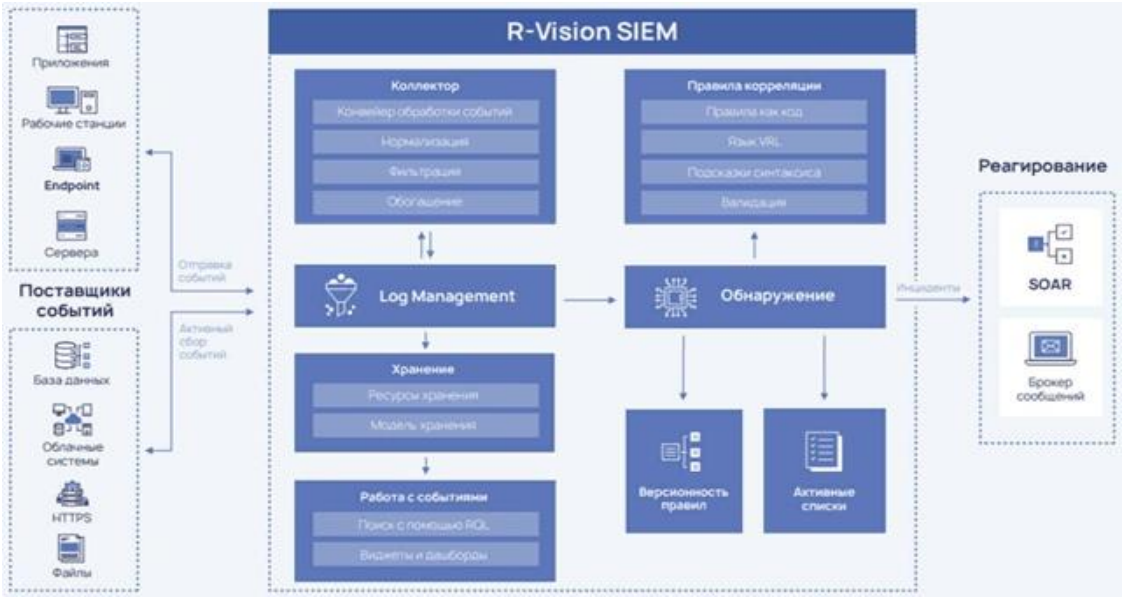


Рисунок 36 – Архитектура R-Vision SIEM (https://rvision.ru)

Таблица 4 – Характеристика решений Positive Technologies

Акционерное общество "Позитив Текнолоджиз"	
PT Dephaze	Класс 03.17 (Средства автоматизации процессов информационной безопасности). Реестровая запись №26215 от27.01.2025. Внутреннее тестирование на проникновение (коротким путем достичь заданной мишени, визуализация маршрута на карте симуляции и сообщает, с помощью чего удалось атаковать ту или иную систему).
Standoff Bug Bounty Платформа Standoff 365 Bug Bounty	Класс 03.17 (Средства автоматизации процессов информационной безопасности). Реестровая запись №24778 от 15.11.2024. Организация мероприятий по поиску уязвимостей и автоматизации проведения процесса поиска и подтверждения уязвимостей.
MaxPatrol EDR MaxPatrol Endpoint Detection and Response	Класс 03.02, 02.08, 03.01, 03.07, 03.09. Реестровая запись №20685 от 25.12.2023. ПО обнаружения и реагирования уровня узла: сбор, обработка событий безопасности, обнаружение КА, подозрительной активности, реагирование на обнаруженную активность на рабочих станциях и серверах.

Рисунок 37 – Функционирование MaxPatrol EDR (https://ptsecurity.com)

Таблица 5 – Характеристика решений InfoWatch

Общество с ограниченной ответственностью "ЛАБОРАТОРИЯ ИНФОВОТЧ"	
InfoWatch Device Control	Класс 03.09 (Средства обнаружения и предотвращения утечек информации). Реестровая запись №27416 от 11.04.2025. Задает правила доступа к внешним носителям информации для сотрудников компаний и их рабочих станций, производится контроль доступа к их внешним устройствам.
InfoWatch Prediction InfoWatch Prediction 2.1 InfoWatch Prediction 2.2	Класс 03.09 (Средства обнаружения и предотвращения утечек информации), 02.08, 03.02, 03.15, 03.17. Реестровая запись № 19043 от 18.09.2023. Предиктивная аналитика данных DLP-систем InfoWatch с учетом рейтинга пользователей для прогнозирования групп рисков ИБ на основе динамических моделей поведения сотрудника.
InfoWatch Vision InfoWatch Vision 2.2 InfoWatch Vision 2.2.0 Vision 2.2	Класс 03.02 (Средства управления событиями информационной безопасности), 03.09, 03.17, 05.13,11.03, 11.04. Реестровая запись № 10342 от 21.04.2021. Регулярный мониторинг статистики в поисках инцидентов и аномалий DLP-системы.
Traffic Monitor	Класс 03.09 (Средства обнаружения и предотвращения утечек информации), 03.02, 03.15, 03.17, 05.13, 11.03, 11.04. Реестровая запись № 10340 от 21.04.2021. DLP-система, которая предотвращает утечки конфиденциальной информации на основе полноценного контентного анализа информационных потоков.

Таблица 6 – Характеристика решений Jet

Акционерное общество "ИНФОСИСТЕМЫ ДЖЕТ"	
Программное обеспечение "Jet KuberBox" (Джет КуберБокс)	Класс 02.13 (Системы контейнеризации и контейнеры). Реестровая запись № 22300 от 24.04.2024. Платформа безопасного управления средами контейнерной оркестрации, предназначенной для управления жизненным циклом системных и прикладных сервисов, упакованных в образы контейнеров, соответствующих спецификации Open Container Initiative.
Ситуационный центр "Джет"	Класс 04.13 (Системы сбора, хранения, обработки, анализа, моделирования и визуализации массивов данных), 02.11, 04.11, 04.15. Реестровая запись № 14462 от 16.04.2018. Информационно-аналитическая система поддержки принятия решений руководителями коммерческих компаний и государственных структур
ПК "СОВ "Плутон-М1.0"	Класс 02.13 (Средства обеспечения информационной безопасности. Реестровая запись № 5129 от 26.02.2019. Программный комплекс "Система обнаружения вторжений "Плутон-М1.0".

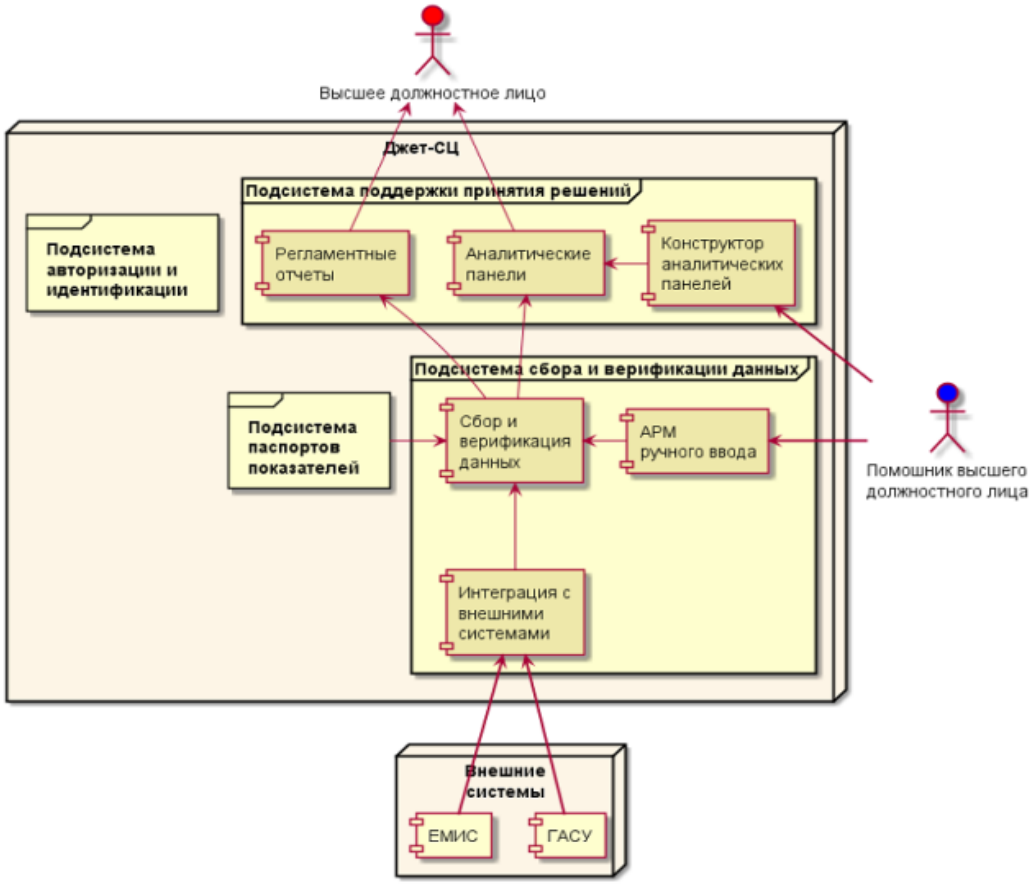


Рисунок 38 – Функциональная архитектура Джет-СЦ(https://jet.su)

Таблица 7 – Характеристика решений VipNet

Акционерное общество «Информационные технологии и коммуникационные системы»	
ViPNet NFV Platform	Класс 02.04 (Средства виртуализации). Реестровая запись № 25045 от 27.11.2024. Управление виртуализированными сетевыми функциями ViPNet (замена аппаратных устройств виртуальными машинами (ВМ), на которых выполняются сетевые функции): создание и управление виртуализированными функциями ViPNet Coordinator VA и ViPNet xFirewall xF-VA, управление ресурсами виртуализированных функций, настройка виртуальной сети, разграничение доступа и управление учетными записями ViPNet NFV Platform, создание и управление резервными копиями виртуализированных функций, создание и управление резервными копиями ViPNet NFV Platform.
ViPNet Prime	Класс 02.08 (Средства мониторинга и управления). Реестровая запись № 17449 от 02.05.2023. Объединение систем управления продуктами и решениями ViPNet в единую многомодульную систему для централизованного управления объектами и субъектами инфраструктуры системы информационной безопасности.
ViPNet IDS NS	Класс 03.14 (Средства обнаружения и/или предотвращения вторжений (атак)). Реестровая запись № 7058 от 07.10.2020. сетевой сенсор обнаружения сетевых атак и вредоносного ПО в файлах, передаваемых в сетевом трафике, и предназначенный для интеграции в компьютерные сети с целью повышения уровня защищенности информационных систем, ЦОД, рабочих станций пользователей, серверов и коммуникационного оборудования.

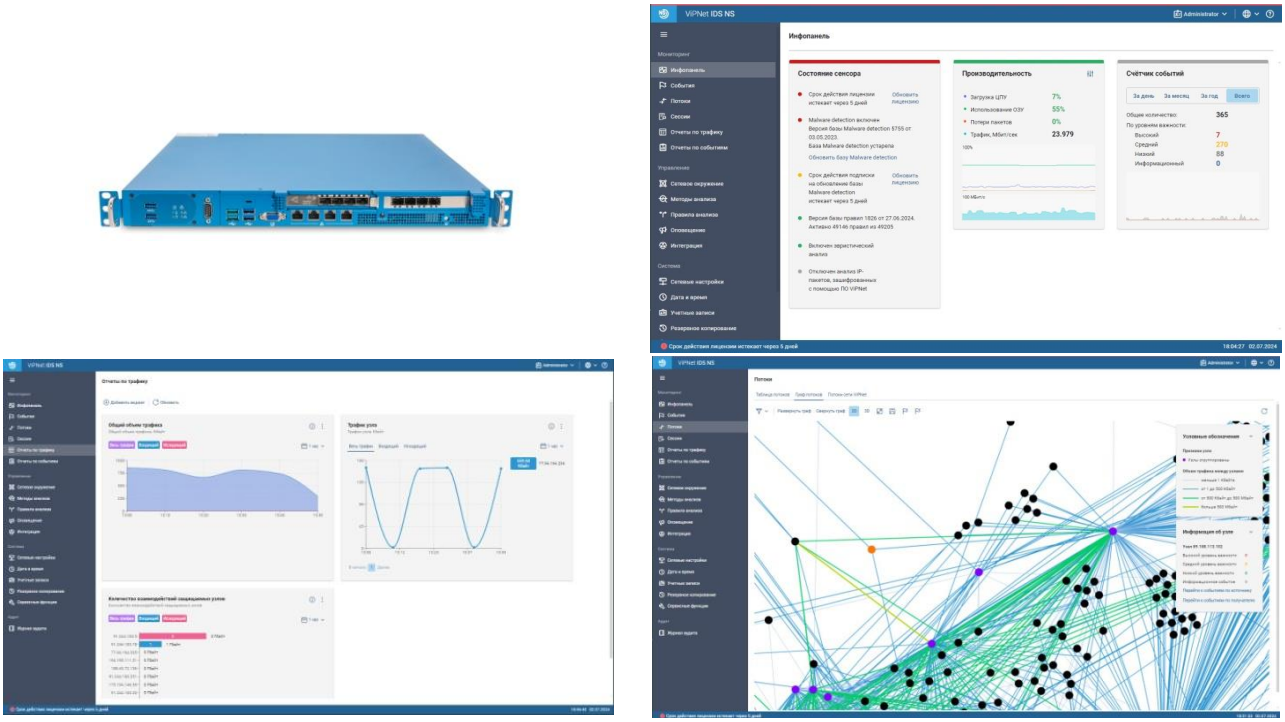


Рисунок 39 – Система обнаружения компьютерных атак ViPNet IDS NS (https://infotecs.ru/products/vipnet-ids-ns)

Бесплатные открытые платформы ПО (ПАК) для системы обеспечения ИБ (например, Wazuh, Nuclei и другие) используются организациями при сложности в закупке коммерческих (Таблица 8, Рисунки 40-41).

Таблица 8 – Характеристика открытых решений

Перечень характеристик	Wazuh
Назначение	Бесплатная, открытая платформа обеспечения информационной безопасности для предотвращения, обнаружения и реагирования на угрозы в инфраструктуре организации. Поддерживает мониторинг физических, виртуальных, контейнерных и облачных сред.
Функции	Функции управления информацией о безопасности и событиями (SIEM) и расширенного обнаружения и реагирования (XDR): - обнаружение вторжений (IDS/HIDS); - поиск вредоносного ПО и аномалий; - контроль целостности файлов (FIM); - централизованный сбор и анализ логов; - оценка соответствия нормативным требованиям (PCI DSS, HIPAA и др.); - обнаружение уязвимостей; - реагирование (например, автоматическая блокировка IP, отключение учетных записей); - мониторинг облачных инфраструктур и контейнеров (например, Docker); - визуализация данных и управление через удобный веб-интерфейс (WUI).
Состав	Сервер (менеджер): сбор, анализ, обработка и хранение данных от агентов, формирование отчетов, оповещение; управление политиками безопасности. Агент (конечные точки: серверы, рабочие станции и т.д.): сбор информации о событиях, состоянии системы, изменениях файлов, уязвимостях и др.
Системные требования к оборудованию	Сервер: ОЗУ 4 ГБ; CPU 8 ядер; 64-битный процессор Intel/AMD (x86_64/AMD64); ОС: Amazon Linux 2/2023, CentOS 7/8, RHEL 7/8/9, Ubuntu 16.04–24.04; Дисковое пространство – от числа агентов и объема событий (около 6 ГБ для 80 рабочих станций, 10 серверов и 10 сетевых устройств для хранения алертов за 90 дней). Агент: ОЗУ: 35 МБ; ОС (Windows, Linux, macOS и др.).
	Nuclei
Назначение	Open-source сканер уязвимостей, разработанный для автоматизации поиска уязвимостей, ошибок конфигурации и других проблем безопасности в веб-приложениях, сетевых устройствах, API и облачных инфраструктурах

Функции	Автоматизация поиска уязвимостей: шаблоны (templates) на базе YAML, которые описывают методы обнаружения, ранжирования и устранения уязвимостей; Поддержка протоколов: HTTP, DNS, TCP, FILE, Websockets, а также headless-браузера для сложных сценариев. Библиотека шаблонов (более 6500 шаблонов для поиска уязвимостей различного типа – от классических SQL-инъекций и XSS до ошибок конфигурации и уязвимостей в облачных платформах). Гибкость и кастомизация (разработка собственных шаблонов для поиска уникальных или специфических для инфраструктуры уязвимостей). Параллельное и масштабируемое сканирование. Аудит веб-приложений (поиск XSS, SQLi, RCE и других уязвимостей). Проверка инфраструктуры (открытые порты, ошибки конфигурации серверов, сетевых устройств) Тестирование API и микросервисов
Suricata	
Назначение	open-source решение IPS предотвращения вторжени – детектор атак, использует анализ сигнатур и эвристику.
Функции	фиксируется и хранится информация о подозрительной активности, блокируются ботнеты, DOS-атаки, а также TOR, анонимайзеры, P2P и торрент-клиенты: сбор и запись информации; оповещения администраторам администраторов сетей о произошедших изменениях (alert); создание отчетов для суммирования логов.

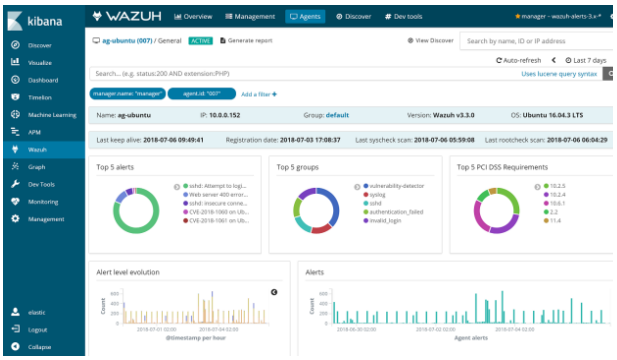


Рисунок 40 – Интерфейс Wazuh (wazuh.com)

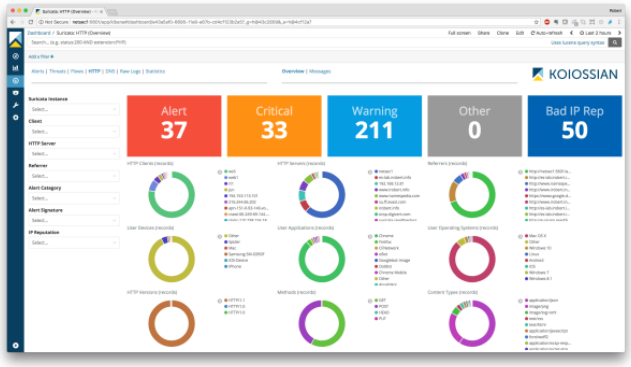


Рисунок 41 – Интерфейс Suricata (https://immunocap.ru)

3. Аналитический обзор публикаций по тематике мониторинга и реагирования на возможные инциденты информационной безопасности

Аналитический обзор открытых публикаций по тематике мониторинга и реагирования на возможные инциденты информационной безопасности, в том числе ЦИИ, проведенный за период 2015-2025 г.г. только по результатам отечественных исследователей (ресурсы научной электронной библиотеки elibrary.ru), показал, что их значительная часть (более 70%) посвящена обнаружению компьютерных атак, применяемым методам (15%), способам (2%) и алгоритмам (4%). В последние 5 лет наблюдается повышение внимания к теме предотвращения компьютерных атак.

Методы обнаружения компьютерных атак в период 2023-2025 годы представлены в 11-ти опубликованных работах в части:

- динамической теории графов (**Павленко Е.Ю., Федоров И.Р., Пагуба Г.Ю., 2023**) как развитие результатов выполненного гранта РНФ №22-21-20008 (**Павленко Е.Ю. 2022**) для систем с изменяемой топологией и поддержки принятия решений с пространственным или временным упреждением (предсказательного моделирования) по отношению к прогнозно-ожидаемым событиям с целью опережающей готовности к реагированию на компьютерные инциденты (Рисунок 44);

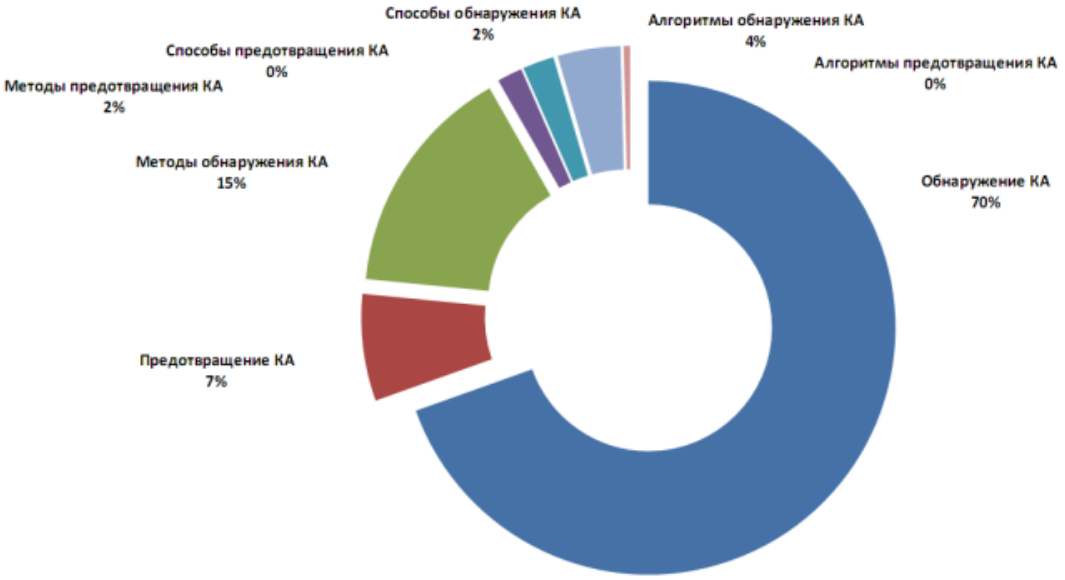


Рисунок 42 – Количество публикаций по тематикам (2015-2025)

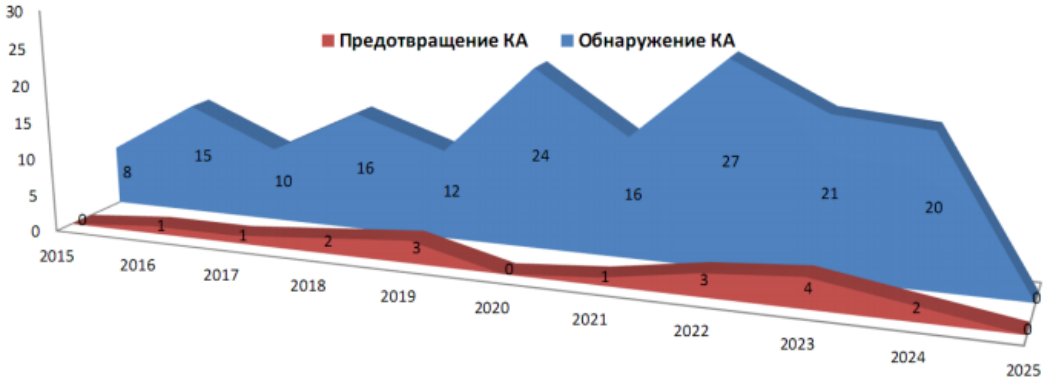


Рисунок 43 – Динамика публикаций по основным тематикам

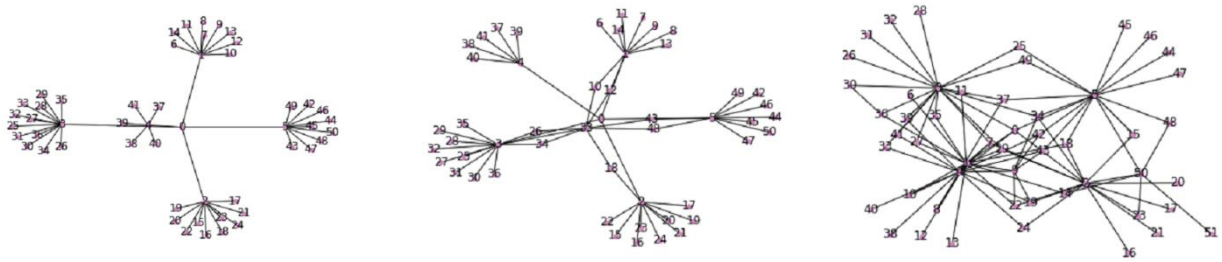


Рисунок 44 – Изменение сетевой топологии при различных КА

- самоорганизующейся карты Кохонена (класс двумерной нейронной сети без учителя; Self-organizing map, SOM; **Teuvo Kalevi Kohonen, 1984**) для обнаружения аномальных данных (**Долгачев М.В., Москвичев А.Д., Москвичева К.С., 2024**) применительно к средствам защиты веб-приложений (Рисунок 45) от атак и уязвимостей (системам класса Web Application Firewall, WAF);

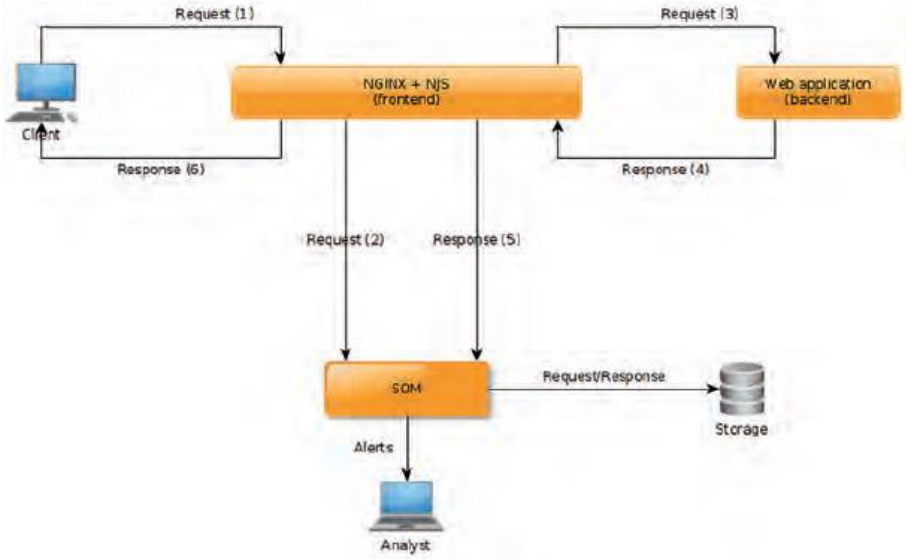


Рисунок 45 – Функционирование WAF с самоорганизующейся картой Кохонена (2024)

- методов глубокого обучения (**Сахарбеков Р.Д., 2024**) для бинарной и мультиклассовой классификации на основе глубоких нейронных сетей с несколькими скрытыми слоями (deep neural networks, DNN), сверточных нейронных сетей (convolutional neural network, CNN), на основе обработки последовательных данных и временных рядов – рекурректных нейронных сетей (Recurrent Neural Networks, RNN) (Рисунок 46);

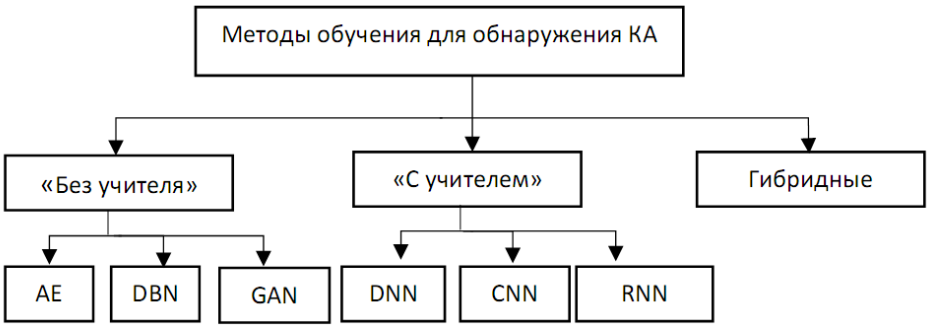


Рисунок 46 – Методы машинного обучения (2023)

- методов машинного обучения (machine learning, ML) применительно к обучению по прецедентам для выявления аномалий (**Борисенко Б.Б., Ерохин С.Д., Мартишин И.Д., 2023**), которые исследовали такие нейронные сети как многослойный персептрон (multilayer perceptron, MLP), сеть глубокого доверия (deep belief network,DBN) в виде 5 последовательных ограниченных машин Больцмана, комбинацию глубокого автоэнкодера (Deep Autoencoder, DAE) и метода градиентного бустинга (DAE+CatBoost), комбинацию разреженного автоэнкодера (Sparse Autoencoder, SAE) и метода градиентного бустинга (SAE+CatBoost), сверточную, рекурретную на основе 3 или 2 выходов (LSTM- и GRU-ячеек) (Рисунок 47);
- генетической декомпиляции и деэволюции машинного кода (Рисунок 49) при сигнатурном поиске уязвимостей (**Буйневич М.В., Израилов К.Е., 2025**);
- методов интеллектуального анализа нужных решений для СОВ (**Майоров А.В., 2023**), как развитие существующих методических подходов (**Штеренберг С.И., 2020**), в трехуровневой архитектуре обработки информации корпоративных и государственных систем;

Характеристика	Precision				Recall				F1-score				Accuracy			
Датасет / Модель																
MLP	0,97	**0,95**	**0,95**	0,01	**1,00**	**0,93**	**0,92**	0,09	**0,98**	0,91	**0,93**	0,02	**1,00**	**0,99**	**0,99**	0,09
DBN	**0,98**	**0,95**	0,05	0,01	**1,00**	0,91	0,09	0,09	**0,98**	**0,93**	0,06	0,02	**1,00**	**0,99**	0,54	0,09
DAE+CatBoost	0,96	**0,95**	0,91	0,01	0,99	0,86	0,77	0,09	**0,98**	0,90	0,81	0,02	0,99	0,98	0,96	0,09
SAE+CatBoost	0,96	**0,95**	0,94	0,01	0,99	0,89	0,85	0,09	0,97	0,92	0,88	0,02	0,99	**0,99**	0,97	0,09
CNN	0,97	0,94	0,09	0,01	0,99	0,91	0,12	0,09	**0,98**	0,92	0,10	0.02	**1,00**	**0,99**	0,54	0,09
LSTM-RNN	0,72	0,83	0,15	0,01	0,92	0,74	0,18	0,09	0,77	0,76	0,16	0,02	0,90	0,97	0,84	0,09
GRU-RNN	0,83	0,57	0,67	0,01	0,97	0,58	0,55	0,09	0,88	0,56	0,57	0,02	0,95	0,91	0,94	0,09

Рисунок 47 – Оценки качества обучения моделей (2023) семантического анализа (Шабля В.О., Коноваленко С.А., Орлов Е.О., 2024);

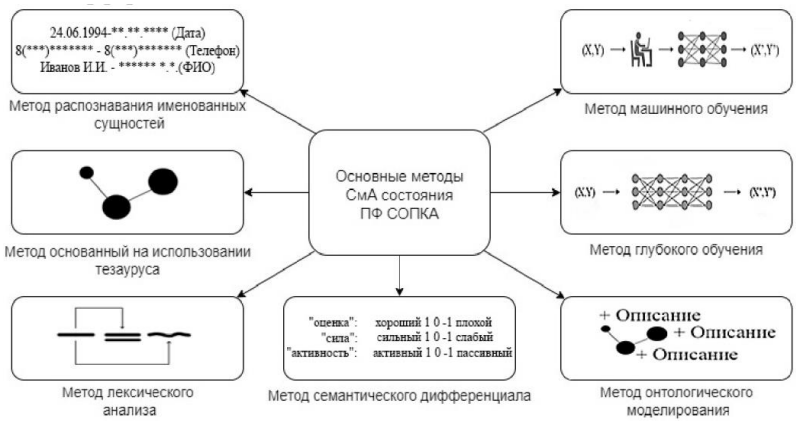


Рисунок 48 – Методы семантического анализа в проблематике ГосСОПКА

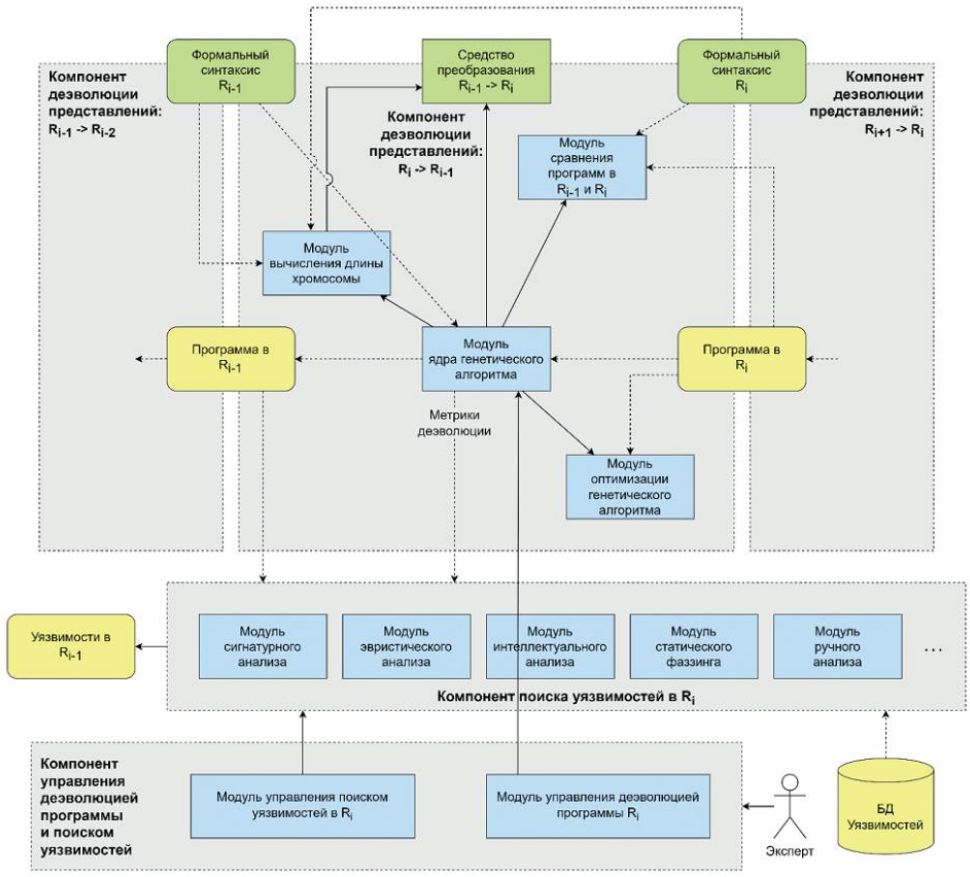


Рисунок 49 – Архитектура исследовательского комплекса

- сверточных нейронных сетей для обнаружения вторжений по изображению (Рисунок 50), преобразованному из данных сетевого трафика (**Голубев С., Новикова Е., 2023; Новикова Е.., Кузнецова Е.О., Голубев С.А., 2024, doi:10.31799/1684-8853-2024-5-57-67);**

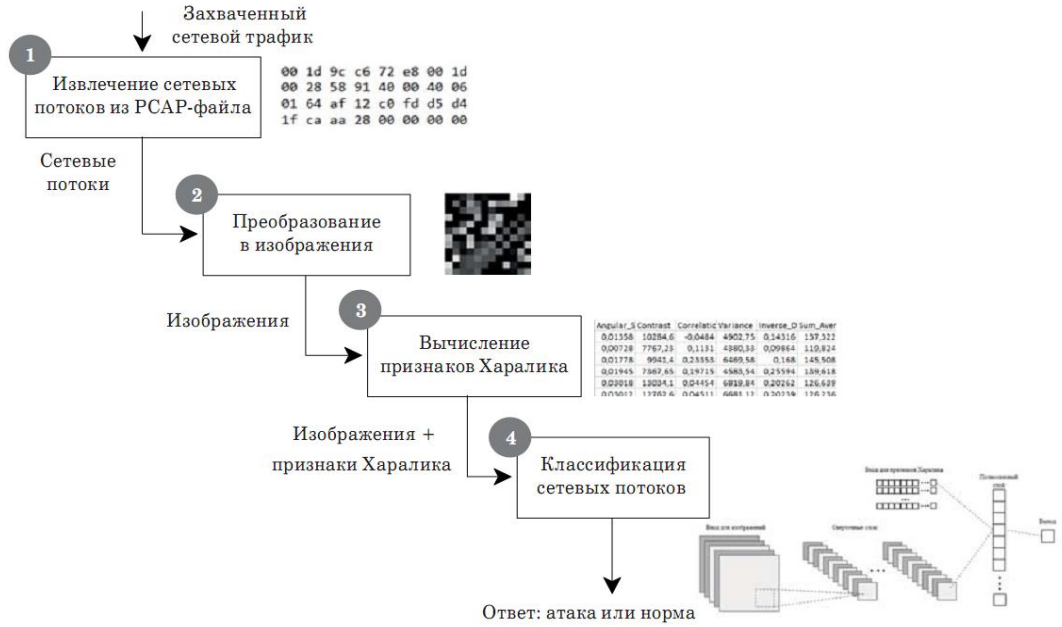


Рисунок 50 – Процедуры выявления сетевых вторжений (2024)

- федеративного обучения (Рисунок 51) на основе локальной модели с разными настройками (**Новикова Е.С., Мелешко А.В., 2024**), как развитие работы 2023 года (DOI: 10.21681/2311-3456-2023-6-50-66);

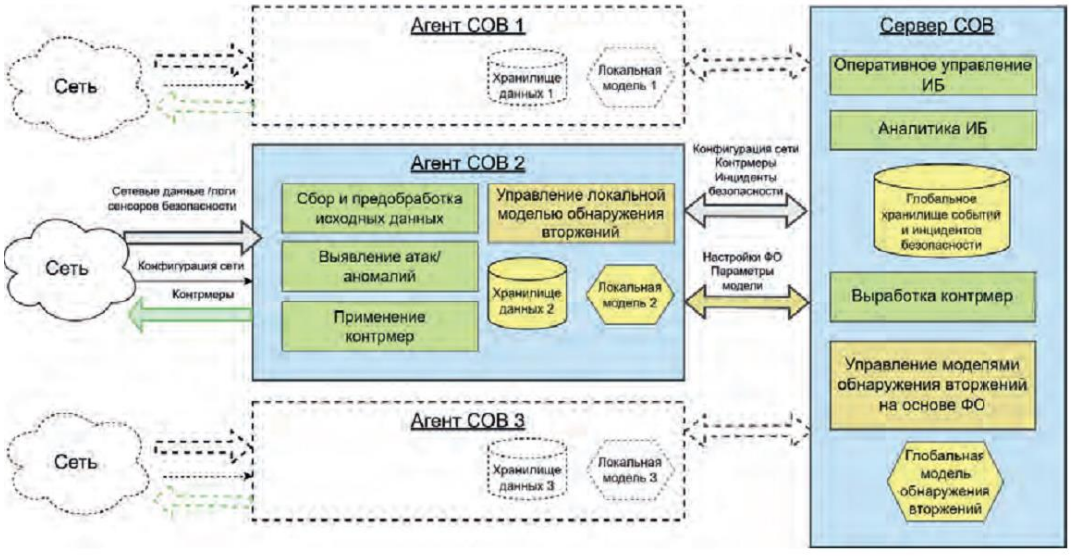


Рисунок 51 – Инфологическая схема СОВ на основе федерального обучения

- организации мониторинга защищенности информационной инфраструктуры иерархических систем учетом функций надзорных организаций (**Тукмачева М.А., Шестаков А.В., 2025**) (Рисунок 52);

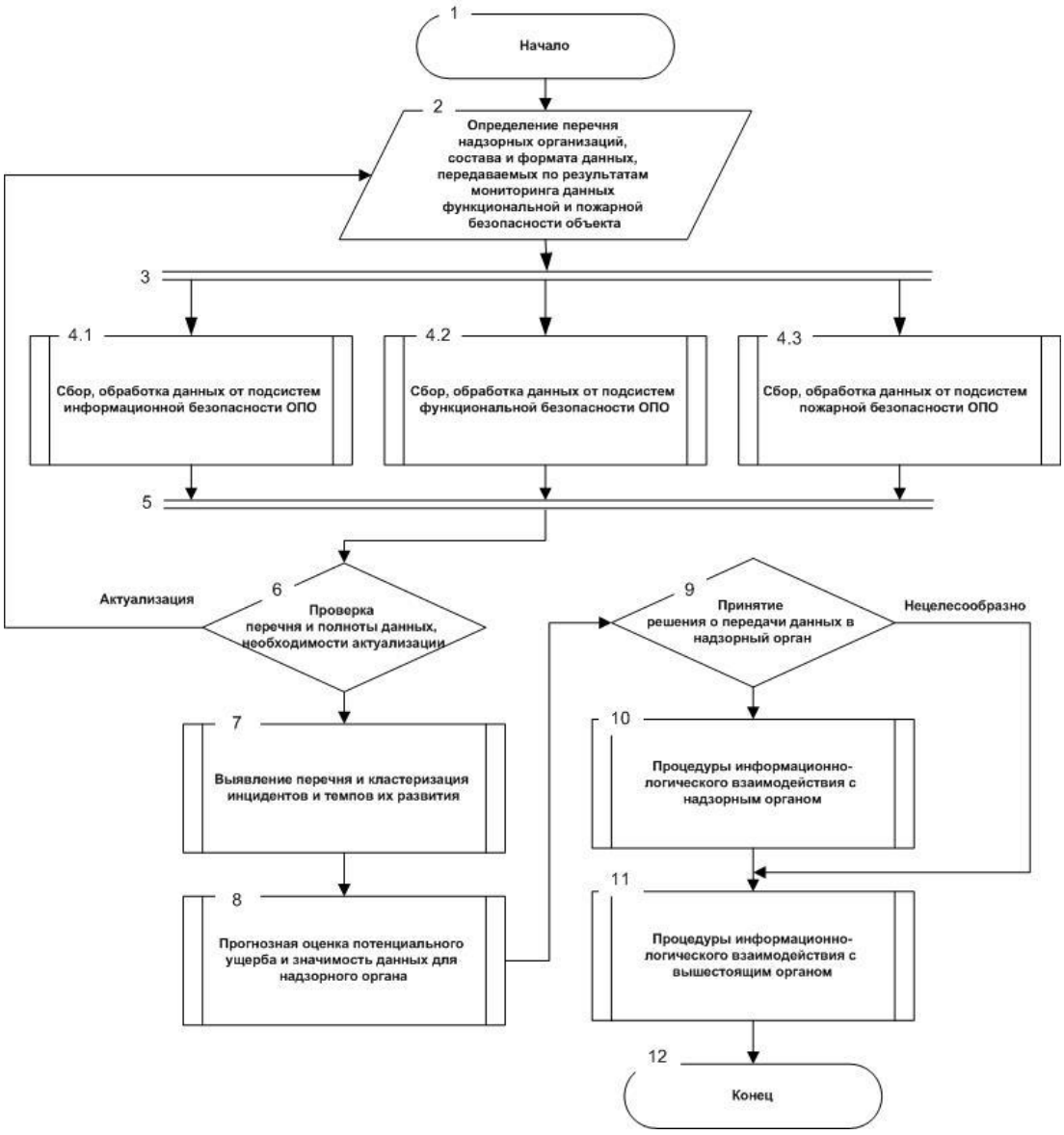


Рисунок 52 – Процедуры организации мониторинга защищенности иерархических систем (2025)

- комбинированных методов корреляции событий ИБ (Левшун Д.А., 2022, DOI: 10.17586/0021-3454-2022-65-11-833-841).

Методы обнаружения редких компьютерных атак применительно к телекоммуникационным системам мобильной связи исследованы в рамках гранта РФФИ №21-57-54002 (**Авдошин С.М., 2021**), которые в отличие от сопоставления некоторых наборов признаков известных атак реальной атаке (методы сигнатур), анализа сценариев и графов атак (методы анализа состояния защищаемого объекта), основаны на использовании для балансировки обучающей выборки генеративно-состязательных сетей (нейросетевых методов обнаружения компьютерных атак).

Методы предупреждения компьютерных атак в период 2023-2025 годы представлены в 7-ми опубликованных работах в части:

- атак типа «злоумышленник посередине» (Man In The Middle, MITM) (**Жарова А.К., Елин В.М., Аветисян Б.Р., 2024**) как развитие работ по данной проблематике (**Сычев Д.И., 2023; Anthi E., Williams L., Rhode M., Burnap P., Wedgbury A., 2021**) по результатам которой предложена авторская методика с использованием предиктивных сетевых технологий обученных

нейронных сетей логике поведения пользователей, активности сетевого и оконечного оборудования (Рисунок 53);

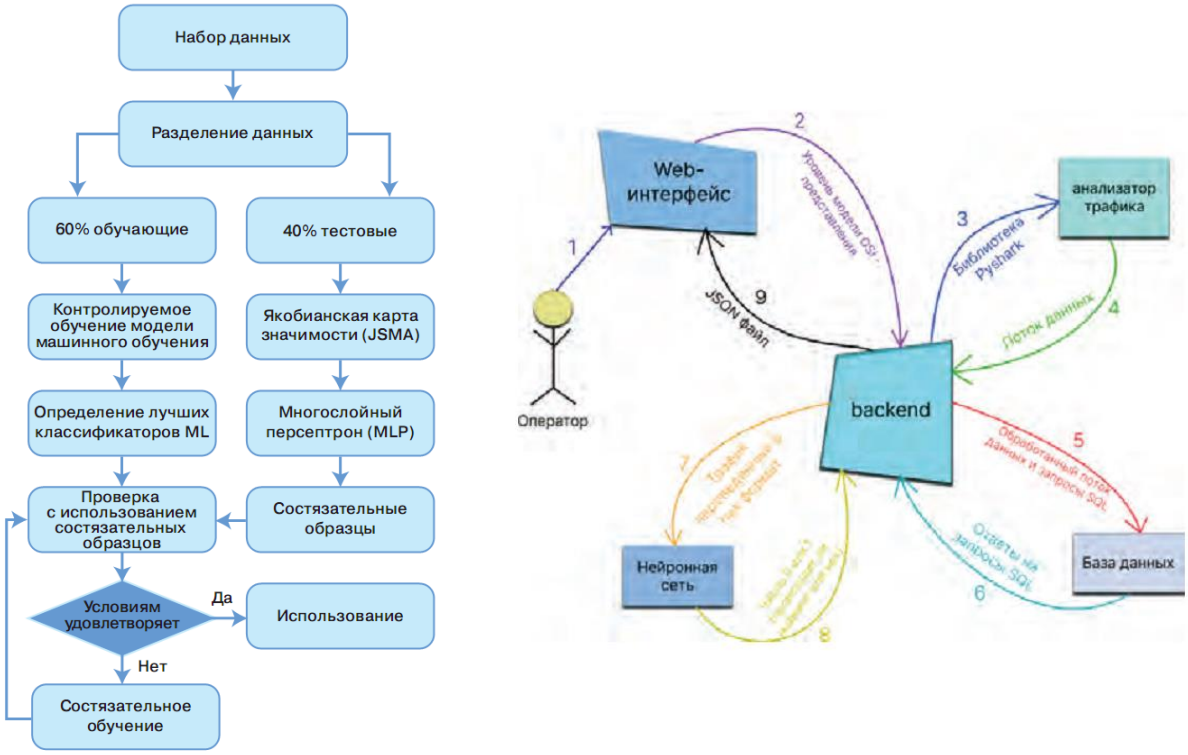


Рисунок 53 – Предлагаемые сценарии использования (Жарова А.К., Елин В.М., Аветисян Б.Р., 2024)

- анализа функционирования ГосСОПКА (**Шабля В.О., Орлов Е.О., Галямин Н.А., 2024**) как реализацию требований НПА (указов Президента Российской Федерации, приказов ФСБ России, МО России, ФСТЭК России, Минцифры России) с целью определения рационального варианта системотехнических решений по построению центральной подсистемы (Рисунок 54);

СС, структурно образующие ЦПСХКСИБ ГосСОПКА на АС		
Функции ГосСОПКА на АС	СС отечественного производства	СС иностранного производства
Централизованный сбор, хранение и корелляция СИБ с целью выявления ИИБ на объектах АС	Комрад 2.0, РАМС ИБ, Max Patrol SIEM, Intellitactics Security Manager, Ankey SIEM, NeuroDAT SIEM	ArcSight ESM, Security Information Manager, QRadar SIEM, Loglogic, NitroSecurity, LogRbythm, OSSIM, USM, Alien Vault SIEM, RSA Security Analytics

Рисунок 54 – Варианты специальных средств (Шабля В.О., Орлов Е.О., Галямин Н.А., 2024)

- анализа функционирования объекта КИИ (**Котенко И.В., Саенко И.Б., Захарченко Р.И., Величко Д.В., 2023, 2024**) и для этапа разведки – предложенных механизмов корреляции событий с автоматической адаптацией к текущей структуре и функциям КИИ с использованием SIEM-систем с учетом внедрения методов искусственного интеллекта и технологий больших данных (Рисунки 55-57);

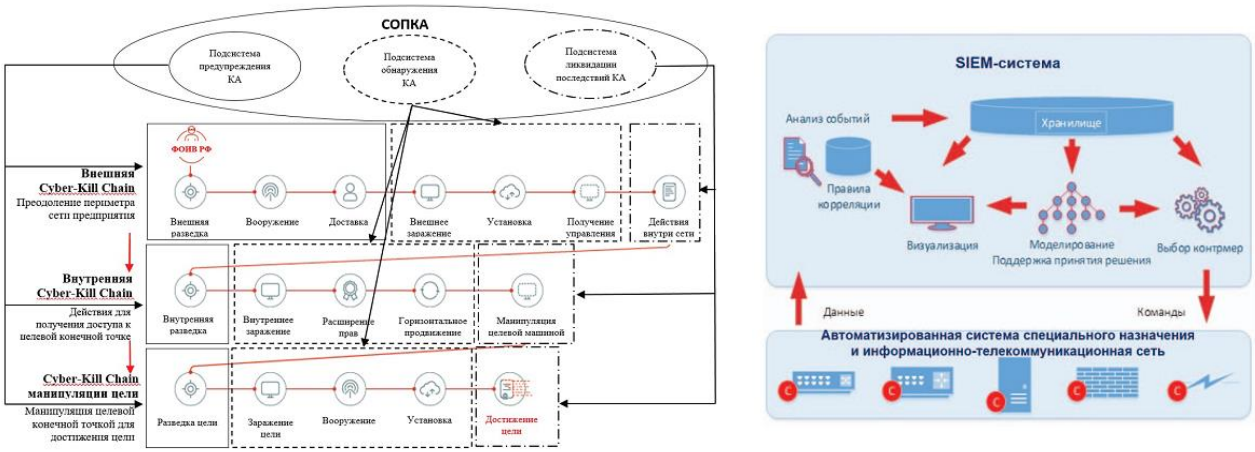


Рисунок 55 – Инфологическая схема подсистем КИИ (2023)

Рисунок 56 – Функциональность подсистем КИИ (2023)

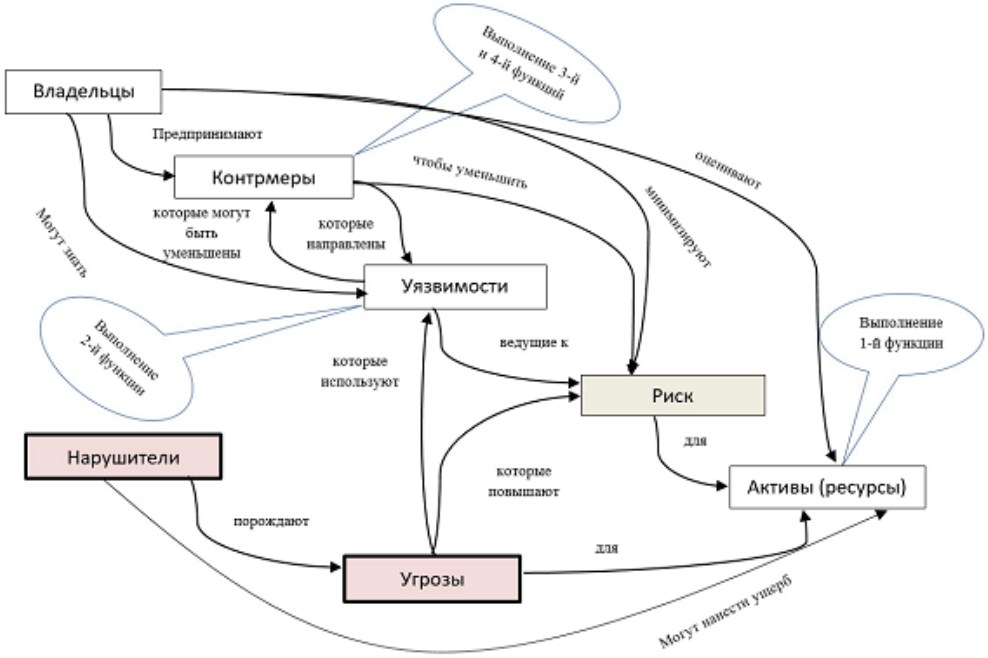


Рисунок 57 – Функциональность подсистемы предупреждения КА (2023)

- оценки функциональной устойчивости средств реагирования (**Коноваленко С.А., 2023**) при реализации соответствующих функциональных устройств, разработанных при участии автора (**Патент на изобретение РФ №204094**), структурно-функциональной модели системы комплексного оценивания устойчивости гетерогенных сегментов ГетСОПКА (Рисунки 58-59).

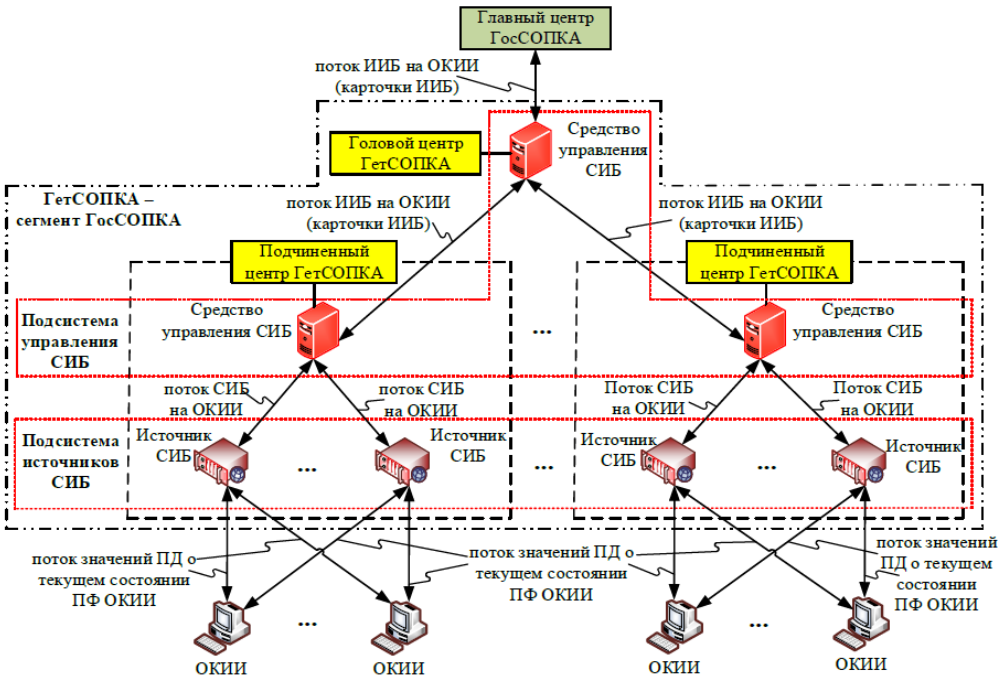


Рисунок 58 – Структура ГетСОПКА (Коноваленко С.А., 2023)

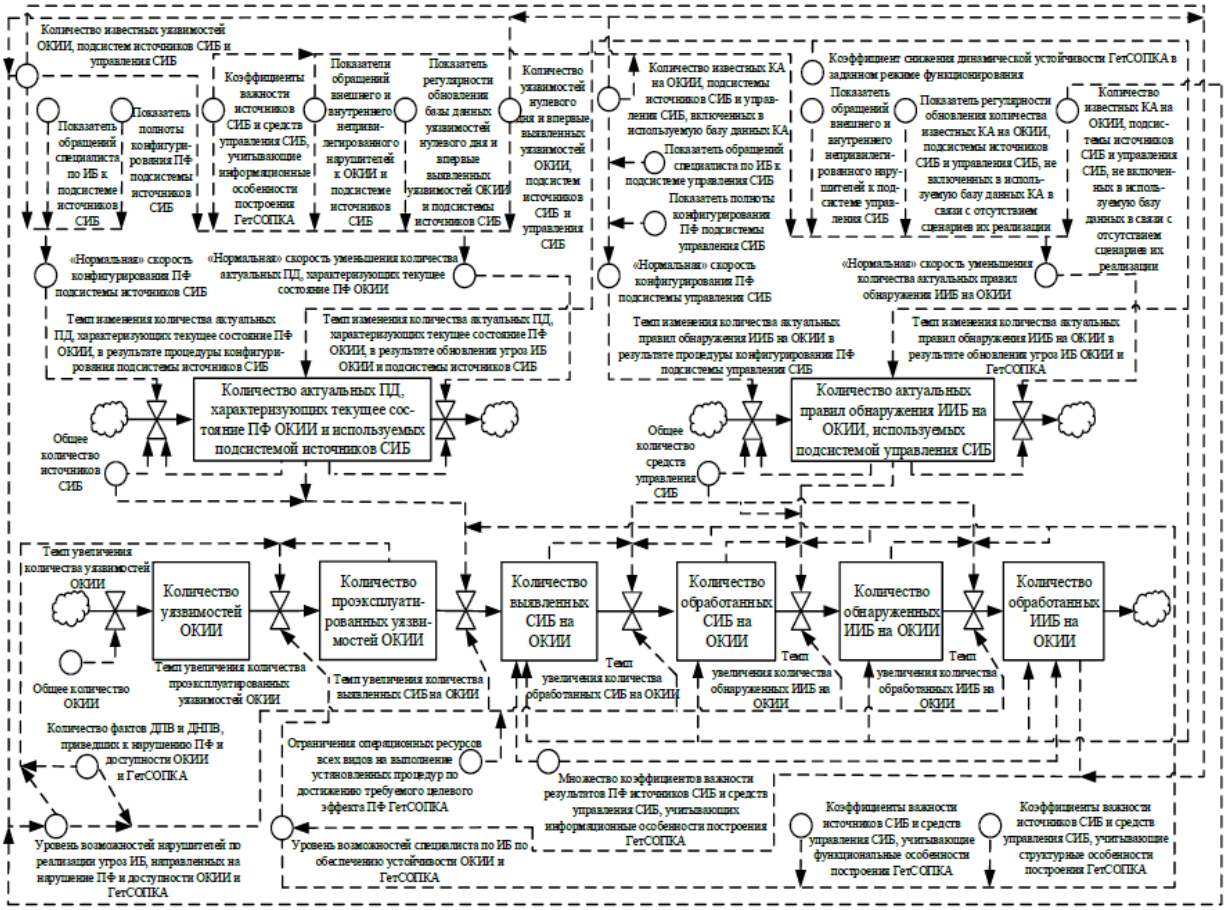


Рисунок 59 – Системно-динамическая модель ГетСОПКА (Коноваленко С.А., 2023)

Дополнительно к рассмотренным источникам следует отметить:

- интеграцию сканеров уязвимостей с системами мониторинга ИБ-рисков посредством оригинальных алгоритмов (**Мунтян М.М., 2023**);
- методическое обеспечение контроля систем мониторинга ИБ (**Вайц Е.В., Грачева Ю.В., Владыченская В.А., Гальцев Б.С., 2024**);
- типы угроз, векторы атак и факторы, влияющие на уровень защищенности критической инфраструктуры (**George A. S., Baskar T., Srikaanth P. B., 2024**);
- применение генеративного искусственного интеллекта в прикладных задачах (**Susarla A. et al., 2023**);
- применение фреймворка TOGAF в управлении киберугрозами (**Judijanto L. et al., 2023**);
- организационные драйверы для углубленного пост-инцидентного анализа (ISRA), увязанные с воспринимаемыми издержками и вниманием руководства (**Shaikh F. A., Siponen M., 2023**);
- ландшафт киберугроз, инциденты и стратегии реагирования на них на примере стран G4 (Германия, Япония, Бразилия, Индия) (**Bhardwaj G. et al., 2021**);
- интегрированная система управления рисками кибербезопасности (i-CSRM), ориентированная на защиту критических инфраструктур (**Kure H. I., Islam S., Mouratidis H., 2022**);
- подход к автоматизации процессов обнаружения, идентификации и первоначального реагирования на инциденты информационной безопасности (**Токарев В.Л., Сычугов А.А. DOI: 10.26102/2310 6018/2023.40.1.006., 2023**).

Анализ специальных публикаций Национального института стандартов и технологий США (NIST, National Institute of Standards and Technology) по регламентации способов (алгоритмов) обнаружения, предупреждения и противодействия компьютерным атакам на информационную инфраструктуру показывает следующий уровень подходов:

- таксономия и терминология в области обеспечения информационной безопасности на основе доверенного и ответственного искусственного интеллекта (**doi.org/10.6028/NIST.AI.100-2e2025, 2025**);
- приоритизация рисков для бизнеса и реагирование на них (**doi.org/10.6028/NIST.IR.8286D-upd1, 2025**);
- постквантовая криптография (**doi.org/10.6028/NIST.IR.8545, 2025**);
- приоритизация киберисков в корпоративных рисках (**doi.org/10.6028/NIST.IR.8286B, 2025**);
- гармонизация в области кибербезопасности и конфиденциальности (**doi.org/10.6028/NIST.IR.8477, 2024**);
- реагирование на инциденты безопасности (**doi.org/10.6028/NIST.SP.800-61r3.ipd, 2024**);
- измерение информационной безопасности (**doi.org/10.6028/NIST.SP.800-55v1, 2024**);
- формализация уязвимостей (**doi.org/10.6028/NIST.SP.800-231, 2024**);
- требования обеспечения несекретной информации (**doi.org/10.6028/NIST.SP.800-171Ar3, 2024**);
- безопасность аппаратно-программных средств (**doi.org/10.6028/NIST.IR.8517, 2024**);
- сетевой ландшафт организации (**doi.org/10.6028/NIST.SP.800-215, 2022**);
- управление ИТ-активами (**doi.org/10.6028/NIST.SP.1800-5, 2018**);
- безопасность приложений (**doi.org/10.6028/NIST.SP.800-190, 2017**);
- восстановление событий инцидентов (**doi.org/10.6028/NIST.SP.800-184, 2016**);
- обмен сведениями о киберугрозах (**doi.org/10.6028/NIST.SP.800-150, 2016**);
- регламентированная очитка данных (**doi.org/10.6028/NIST.SP.800-88r1, 2014**).

4. Аналитический обзор исследований зарегистрированных в Единой государственной системе НИОКТР по тематике мониторинга и реагирования на возможные инциденты информационной безопасности

Аналитический обзор исследований зарегистрированных в Единой государственной системе НИОКТР по тематике мониторинга и реагирования на возможные инциденты информационной безопасности, проведенный за период 2015-2025 г.г. характеризуется результатами в части:

- моделей, методов, методик, алгоритмов и программ интеллектуальных систем кибербезопасности (**Рег. номер НИР 125031703826-6 от 17.03.2025, СПБ ФИЦ РАН**);
- моделей, методов и алгоритмов обнаружения уязвимостей ВПО (**Рег. номер НИР 225012302107-9 от 23.01.2025, МГУ им. М.В. Ломоносова, Факультет ВМК);**
- методов управления и алгоритмов анализа инцидентов в телекоммуникационных сетях (**Рег. номер НИР 225031513511-9 от 15.03.2025, Оренбургский государственный университет);**
- Марковских моделей кибератак (**Рег. номер НИР 225031313370-4 от 15.03.2025, Омский государственный технический университет);**
- метода поиска аномалий с использованием нейронных сетей (**Рег. номер НИР 124103000017-3 от 30.10.2024, СПБ ФИЦ РАН);**
- цифрового двойника должностного лица, осуществляющего деятельность в области информационной безопасности и защиты информации, с учетом модели информационного противоборства **(Рег. номер НИР 224051500040-9 от 15.05.2024, Российский экономический университет им. Г.В. Плеханова);**
- методы (технологии) обеспечения кибербезопасности (**Рег. номер НИР 122040800208-4 от 08.04.2022, СПБ ФИЦ РАН**).

Аналитический обзор исследований регламентации проведения защищенности ведомственных информационных ресурсов выполнен на основании анализа нормативной правовой базы прецедентов ФОИВ, ведомств, органов и организаций государственной власти, а также органов местного самоуправления за период 2023-2025 г.г. и характеризуется следующими результатами.

Структурными элементами Регламента проведения мониторинга защищённости ведомственных информационных ресурсов являются:

- введение, которое содержит краткие сведения о документе;
- общие положения, которые содержат назначение документа; перечень НПА на основании которых разработан документ; термины и определения, используемые в документе; наименование контролирующего органа за исполнением документа; исполнительные органы и организации; перечень информационных ресурсов; перечень мероприятий и обеспеченность ресурсами; задачи, объекты и уровни мониторинга;
- основные требования, которые содержат ответственность, силы и средства; распределение обязанностей;
- организацию информационного и документального взаимодействия;
- бизнес процессы менеджмента информационной безопасности;
- контактные данные.

Структурными элементами Регламента управления КИ ИБ ведомственных информационных ресурсов являются:

- введение, которое содержит краткие сведения о документе;

- общие положения, которые содержат назначение документа;
- правовые основы взаимодействия, которые содержат перечень НПА на основании которых разработан документ;
- термины и определения, используемые в документе;
- перечень мероприятий, проводимых в ходе реагирования на КИ, и мерп по ликвидации последствий КА;
- организацию информационного и документального взаимодействия;
- сроки предоставления информации, сведениями различного характера, и контроль;
- сроки действия документа и его актуализация.

Аналитический обзор объектов интеллектуальной собственности (ОИС), которые характеризуют технический уровень решений в области мониторинга и реагирования на возможные инциденты информационной безопасности, в том числе ЦИИ, проведенный за период 2013-2025 г.г. только по выданным документам правовой охраны Роспатента **программам для ЭВМ** (базы данных ФИПС fips.ru), показал, что значительная их часть (более 60%) посвящена обнаружению компьютерных атак, применяемым методам (14%), способам (1%) и алгоритмам (9%). За последние 5 лет наблюдается повышение внимания ОИС к вопросам обнаружения (Рисунки 60-61).

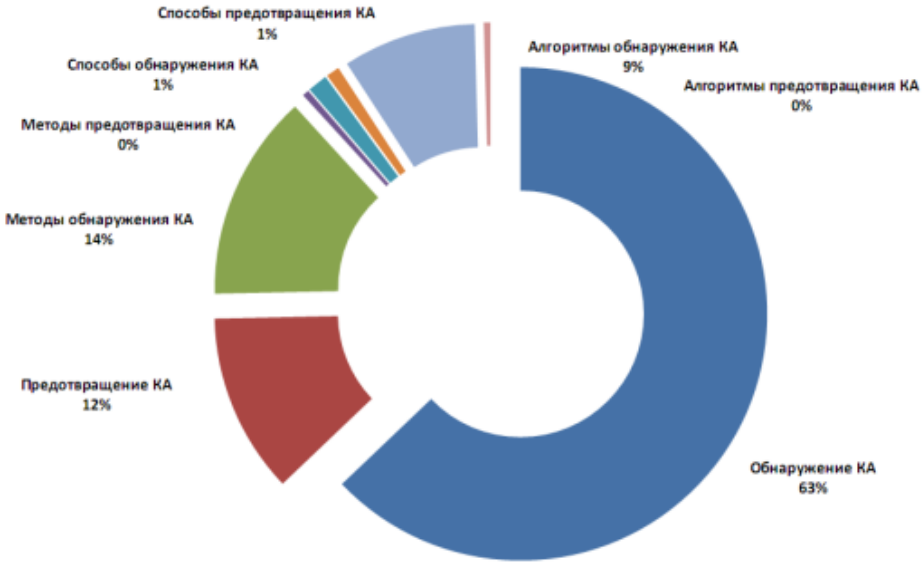


Рисунок 60 – Количество ОИС по тематикам (2013-2025)

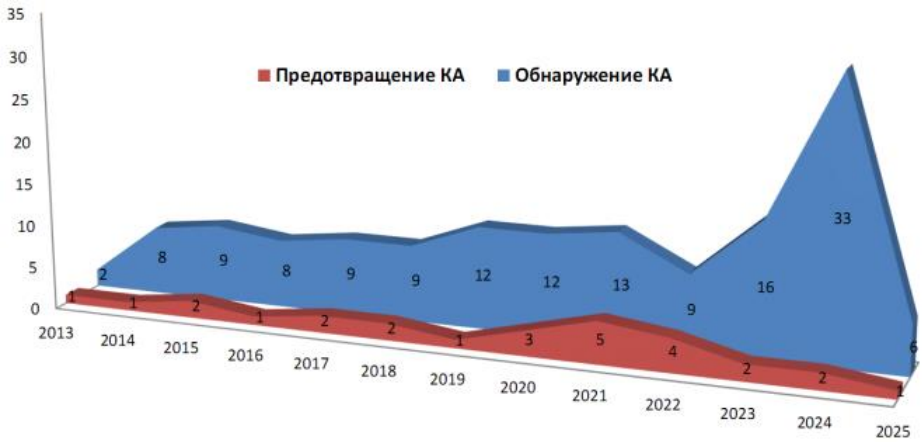


Рисунок 61 – Динамика ОИС по основным тематикам

Решения в области мониторинга и реагирования на возможные инциденты информационной безопасности ориентированы на:

- создание ведомственных компонент ГосСОПКА, например, в РЖД (Свидетельство о регистрации **№2020611311, 2020**);
- платформенные решения систем обеспечения информационной безопасности организаций, например, класса SIEM (Свидетельство о регистрации **№2021661865, 2021** – Kaspersky Unified Monitoring And Analysis Platform), класса SOAR (**№2021615434, 2021** – Security Vision Security Orchestration Automation and Response);
- интеграцию систем реагирования на компьютерные инциденты, например, в центрах мониторинга ИБ организаций (Свидетельство о регистрации **№2024615566**, **№202468021, 2024; №2021616099, №2021661631, 2021**);
- автоматизацию процесса сканирования веб-приложений (Свидетельство о регистрации **№2024665769, 2024**); сетевого трафика (**№2023687672, 2023**); функций службы IDS/IPS (**№2024669349, №2024665032, 2024; №2021666257, 2021**), SIEM (**№2024662407, 2024; №2022611631, 2022**);
- определение техник реализации КА (Свидетельство о регистрации **№2025613600, 2025**);
- задачи ликвидации последствий компьютерных атак, например, стратегий (Свидетельство о регистрации **№2021669290, 2021**);
- расследование КИ (Свидетельство о регистрации **№2021618235, 2016**).

Отечественные организации и компании при регистрации ОИС в анализируемой предметной области имеют следующую активность: Акционерное общество «Лаборатория Касперского» (34); Федеральное государственное казенное военное образовательное учреждение высшего образования «Краснодарское высшее военное орденов Жукова и Октябрьской Революции Краснознаменное училище имени генерала армии С.М.Штеменко» Министерства обороны Российской Федерации (19); Академия Федеральной службы охраны Российской Федерации (13); Российская Федерация, от имени которой выступает Министерство обороны Российской Федерации (4); Федеральное государственное бюджетное образовательное учреждение высшего образования «МИРЭА – Российский технологический университет» (2); федеральное государственное казенное военное образовательное учреждение высшего образования «Военная академия связи имени Маршала Советского Союза С.М.Буденного» Министерства обороны Российской Федерации (2); Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Белгородский государственный технологический университет им. В.Г. Шухова» (1); Федеральное государственное автономное образовательное учреждение высшего образования «Новосибирский национальный исследовательский государственный университет» (Новосибирский государственный университет, НГУ) (1); ООО «Код Безопасности» (1), АО «ЦентрИнформ» (1).

В части алгоритмизации предложен алгоритм обнаружения компьютерных атак (Свидетельство о регистрации **№2019666737, 2019**), включающий формирование файла с данными сетевых пакетов заданного формата (PCAP) сетевым анализатором (Wireshark), хранение сетевых дампов, анализ трафика и параметров функционирования сети, на основе технологий БоД в составе кластера Hadoop (распределенных вычислений и обработки информации).

Зарегистрирована программа (**№2022618520, 2020**) в которой функции IDS реализуют алгоритмы обучения нейронной сети, выявления потока ИБ-событий, определения аномалий по показателю роста ошибок предсказания.

Механизм выбора методов машинного обучения для систем обнаружения вторжений зарегистрирован применительно к текущим характеристикам сетевых атак на основе перебора заданного комплекта алгоритмов (**№2023662222, 2023**), в частности, из возможного подмножества, включающего логистическую регрессию (линейная модель для бинарной

классификации), случайный лес (ансамблевое обучение для классификации), метод k-ближайших соседей (непараметрический алгоритм классификации), градиентный бустинг (многоклассовая классификация), многослойный персептрон, AdaBoost (алгоритм бустинга), CatBoost (бинарной классификации), XGBoost (алгоритм градиентного бустинга), LightGBM (градиентный бустинг на основе гистограмм). В общетеоретическом аспекте известно, что основными показателями эффективности механизма выбора являются сбалансированная точность, полнота/чувствительность, точность, коэффициент F1 и коэффициент Бриера.

Алгоритмы предотвращения компьютерных атак при администрировании информационной безопасности корпоративных сетей в зарегистрированном программном компоненте (**№2021618193, 2021**) основаны на результатах определения значений коэффициента Херста (Г.Э. Херст, H.E. Hurst) (показателей скейлинга) как меры фрактальности предварительно сформированных групп пакетов трафика по результатам тестирования и анализа характеристик самоподобного трафика. В общетеоретическом аспекте фракталов и методов оценки самоподобия известно применение расширенного теста Дики-Фуллера (проверка на стационарность, Augmented DF-тест, Dickey-Fuller test, 1979), R/S анализа (метод нормированного размаха при анализе фрактальности структуры временных рядов), метода DFA (Detrended Fluctuation Analysis, дисперсионный анализ нестационарных рядов измерений) (**DOI: 10.22184/2070-8963.2021.98.6.64.70**), а также фактор Фано (U. Fano, индекс разброса дисперсии).

Комплекс методов сбора, фильтрации и анализа данных при расследовании компьютерных инцидентов реализован в зарегистрированной программе для ЭВМ (**№2021618235**) с поиском объектов учета по заданным параметрам, в т.ч. записей системных журналов, историй посещений, загрузок и активности сетевых средств, подключений, реестров.

Методы определения техник реализации компьютерных атак зарегистрированы как программный модуль в составе ПО персонального компьютера (**№2025613600, 2025**), которые реализуют сбор данных о межпроцессорном взаимодействии, обнаружение паттернов и преобразование в геометрическую форму представления для пользовательского интерфейса.

Реализация решений, представленных в ОИС, предусматривает использование ЭВМ, как правило, IBM PC-совместимых. Операционные системы – преимущественно Astra Linux, Unix.. Языки программирования: Bash, C#, Delphi, Go, Java, JavaScript, Lua, Python, PowerShell script, Scala, Typescript, Visual Studio C#.

Реестр российских изобретений Роспатента содержит **74 патента** на изобретение, которые направлены на:

- обнаружение компьютерных атак (Патент РФ №2782711, №2731467; №2713759; №2634211, №2680756; №2661533; №2587426; №2566331, №2540838, №2538292, №2531878);
- выявление компьютерных атак (Патент РФ №2601147) посредством обнаружения подозрительного признака в информации о ресурсе источника и дополнительной об этом ресурсе, выявляют группу систем, а при повторном обнаружении выявляют атаку (Рисунок 62);
- предотвращения компьютерных атак (Патент РФ №2768567; №2740027);
- противодействия компьютерным атакам (Патент РФ №2682108);
- обновление техник реализации КА (Патент РФ №2809929, 2023; №2833413, 2025) (Рисунки 63-64);
- способы выявления угроз ИБ (Патент РФ №2833172; №2802539);
- моделирование оценки ущерба (Патент РФ №2625045);
- контроль поверхности защиты (Патент РФ №2824314, 2023) (Рисунок 65);
- построения системы обнаружения инцидентов ИБ (Патент РФ №2742179, 2021) (Рисунок 66);

• формирование перечня актуальных угроз заданным способом (Патент РФ №2833173, 2024) (Рисунок 67).

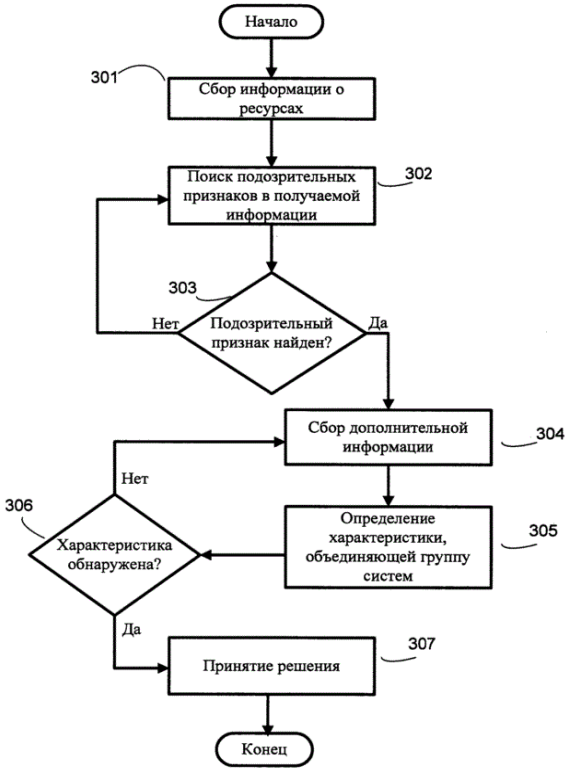


Рисунок 62 – Способ выявления компьютерной атаки (Патент РФ №2601147)

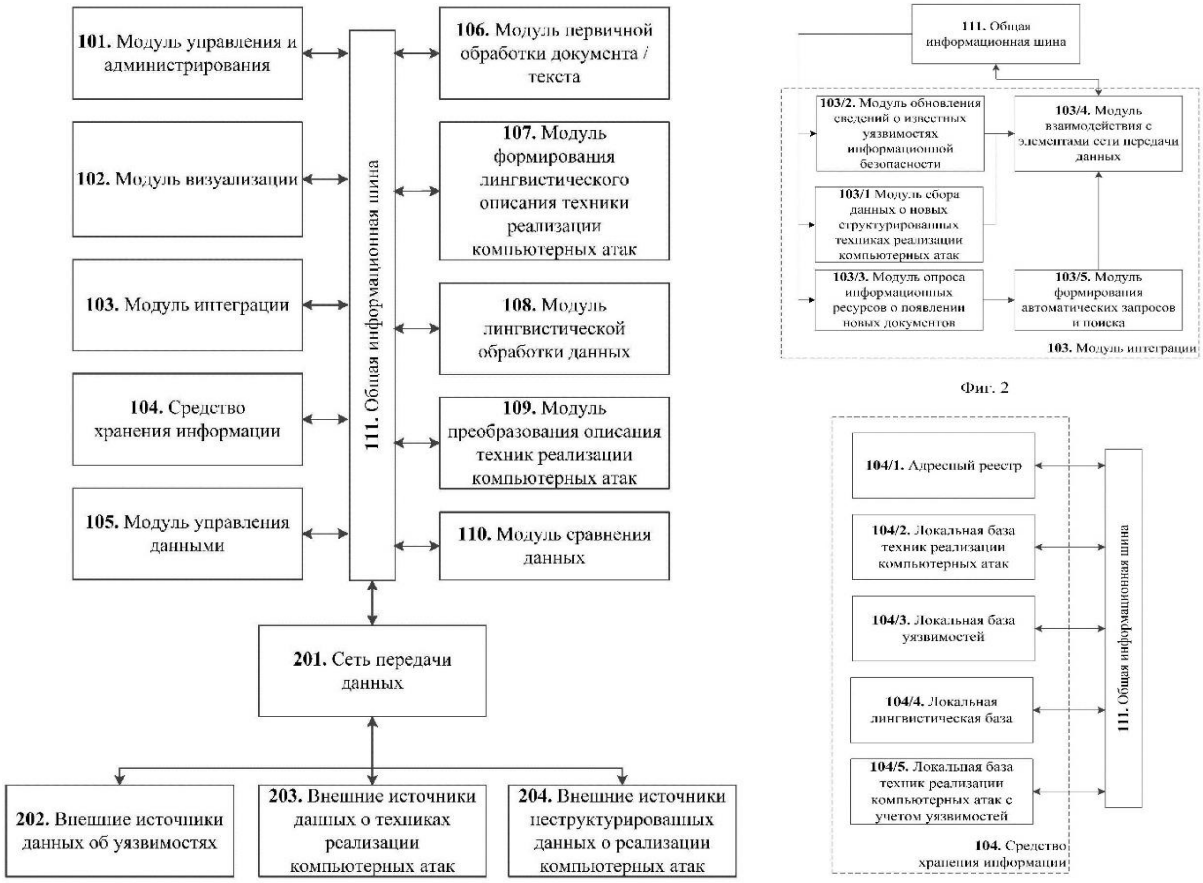


Рисунок 63 – Процедуры автоматического обновления и формирования техник реализации КА (Патент РФ №20809929)

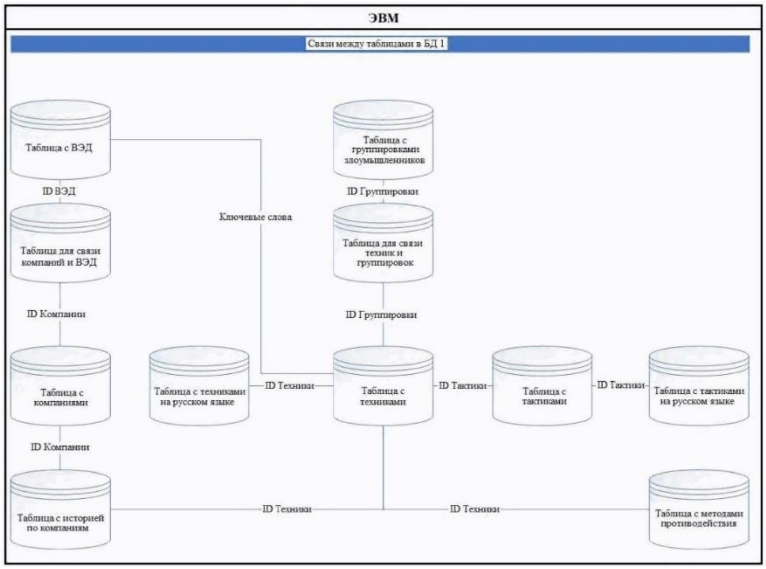


Рисунок 64 – Процедуры приоритизации угроз информационной безопасности (Патент РФ №2833413)

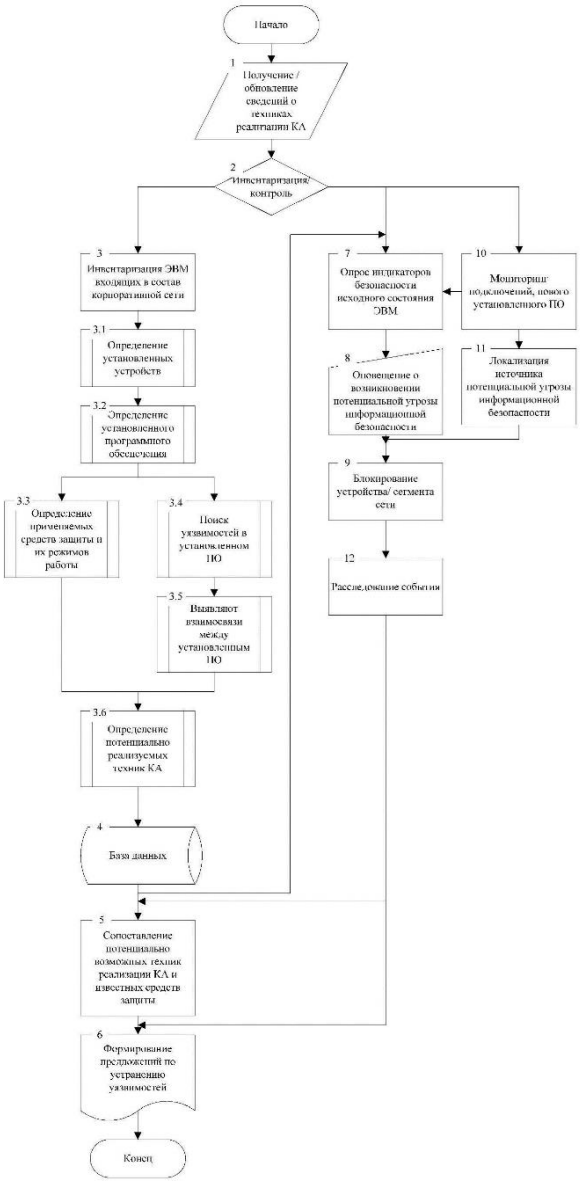


Рисунок 65 – Процедуры оценки и принятия мер по предотвращению техник реализации КА (Патент РФ №2824314)

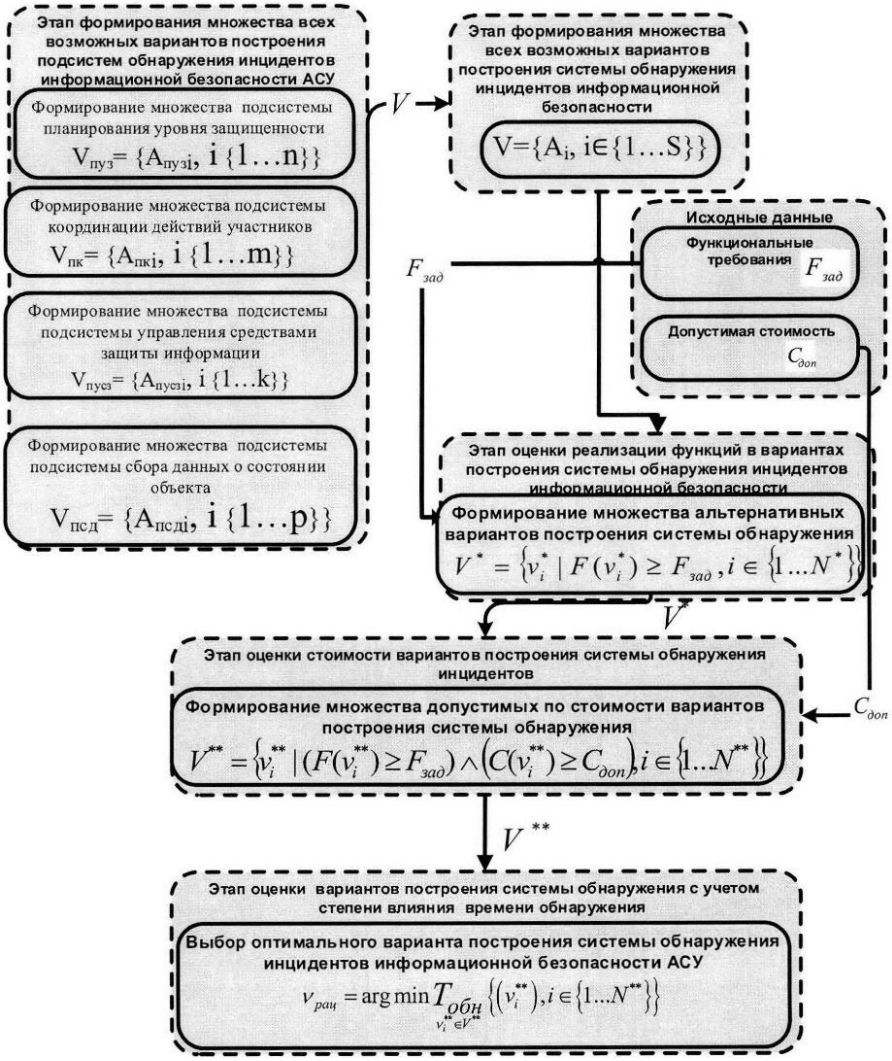


Рисунок 66 – Процедуры построения системы обнаружения инцидентов ИБ (Патент РФ №2742179)

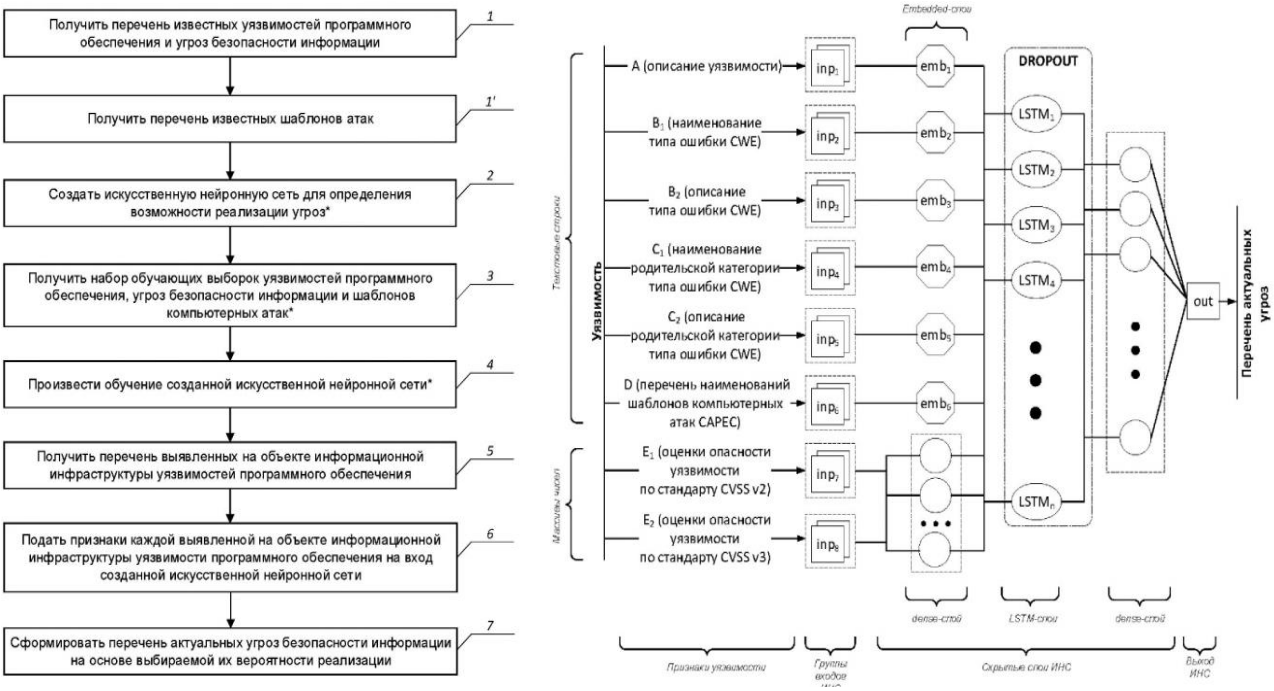


Рисунок 67 – Способ определения актуальных угроз ИБ (Патент №2833173)

Заключение и выводы

Способы мониторинга и реагирования на возможные инциденты информационной безопасности в информационных инфраструктурах различного назначения развиваются и совершенствуются в рамках достижения технологического суверенитета вследствие объективного возрастания интенсивности и расширения спектра преднамеренных компьютерных атак на различные управленческие и бизнес-процессы организаций и человеческий ресурс в современных геополитических условиях и продолжающегося санкционного давления на Российскую Федерацию.

Цифровая информационная инфраструктура МЧС России должны выполнять не только функции своего целевого предназначения в сфере защиты информации и обеспечения информационной безопасности МЧС России, а также, как показывают результаты настоящего аналитического обзора, обеспечивать информационное взаимодействие по вопросам ИБ-инцидентов с системами обеспечения информационной безопасности организаций, учреждений и предприятий, в отношении которых МЧС России осуществляет надзорные и, главное, координирующие функции.

Система обеспечения информационной безопасности ЦИИ МЧС России должна реализовывать системотехнические решения, которые выработаны в соответствии с требованиями нормативных правовых документов Российской Федерации, построены на основе имеющихся в нашей стране технологий, способах, методах и алгоритмах мониторинга и реагирования на возможные инциденты информационной безопасности.

Подсистема предупреждения компьютерных атак ведомственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак должна заблаговременно выявлять и предупреждать попытки проведения компьютерных атак на объекты ЦИИ МЧС России. Функции предупреждения компьютерных атак в отечественных технических решениях реализованы не в полном объеме, наблюдается подмена понятия «предупреждение компьютерных атак» на «контрольно-технические мероприятия».

Организационно-техническое обеспечение мониторинга и реагирования на возможные инциденты информационной безопасности в ЦИИ МЧС России при ограниченных ресурсах сил и средств субъектов ЦИИ может быть сосредоточено на рациональном сочетании распределения функций между должностными лицами, выполняющими профессиональную деятельность в области информационной безопасности и защиты информации, соответствующих требованиям государственных регуляторов в сфере технической защиты информации минимально необходимых организационных мер, апробированного поэтапного внедрения и эксплуатации программного обеспечения и программно-аппаратных комплексов мониторинга и реагирования на возможные инциденты информационной безопасности с открытыми кодами и бесплатными лицензиями, прошедших процедуру обязательного подтверждения соответствия продукции в форме серитификации, для фрагментов ЦИИ МЧС России.

Аналитический обзор способов мониторинга и реагирования на возможные инциденты информационной безопасности в цифровой информационной инфраструктуре МЧС России и уровня их технической реализации разработан с целью выявления текущей ситуации по обеспечению организации функционирования систем мониторинга и реагирования на возможные инциденты информационной безопасности в цифровой информационной инфраструктуре МЧС России, а также возможным направлениям развития нормативных правовых документов, регламентирующих порядок взаимодействия элементов специально созданной организационной структуры МЧС России, уполномоченной для решения задач системы обеспечения информационной безопасности МЧС России.

Список литературы

1. Банк документов // http://www.kremlin.ru/acts/bank
2. Официальный интернет-портал правовой информации // http://pravo.gov.ru
3. Нормативные правовые акты Федеральной службы безопасности Российской Федеации. URL: http://www.fsb.ru/fsb/npd.htm
4. Нормативные документы Федеральной службы по техническому и экспортному контролю. Все документы. URL: https://fstec.ru/dokumenty/vse-dokumenty
5. Основные нормативные правовые акты, организационные и методические документы по обеспечению безопасности критической информационной инфраструктуры Российской Федерации. 30.01.2025 / Экспертно-аналитический центр ГК InfoWatch. 2025. – 14 с.
6. Научная электронная библиотека. URL:https://elibrary.ru
7. ЕГИСУ НИОКТР. URL: https://gisnauka.ru
8. Базы данных ФИПС. URL: https://www1.fips.ru/iiss
9. Реестр программного обеспечения. URL: https://reestr.digital.gov.ru
10. Банк данных угроз безопасности информации. URL: https://bdu.fstec.ru/threat
11. Kaspersky vulnerabilities & threats database. URL: https://threats.kaspersky.com/ru
12. Обзор основных типов компьютерных атак в финансовой сфере в 2024 году. Банк России. – М.: ДИБ Банка России, 2025. – 35 с.
13. Исследование российского ландшафта киберугроз. Treat Zone 2025 //Bi.Zone. 2025. – 175с.
14. Актуальные киберугрозы: IV квартал 2024 года – I квартал 2025 года. / Positive Technologies. URL: https://www.ptsecurity.com/ru-ru/research/analytics/aktualnye-kiberugrozy-iv-kvartal-2024-goda-i-kvartal-2025-goda/#id1
15. Аналитический отчет. Утечки информации в мире 2023-2024 годы / Экспертно-аналитический центр ГК InfoWatch, 2024. – 15 с.
16. Best Practices In Conducting Penetration Testing And Vulnerability Assessments Of Information Infrastructure Facilities. BRICS RUSSIA 2024. 16 с.
17. Обзор рынка информационной безопасности за 2024 год / Инфосистемы Джет. JET.SU, 2024. – 28 с.
18. Искусственный интеллект для кибербезопасности: тренды и востребованность. // Искусственный интеллект. Серия информационно-аналитических материалов Института статистических исследований и экономики знаний НИУ ВШЭ. – 2024. – №7. – 3 с.
19. Аналитический отчет. Тенденции в сфере обеспечения ИБ АСУ ТП 2024-2025 годы / Экспертно-аналитический центр ГК InfoWatch, 2024. – 17 с.