ISSN 1680-2772

АКАДЕМИЯ ВОЕННЫХ НАУК
ЦЕНТР ПРОБЛЕМ СТРАТЕГИЧЕСКИХ ЯДЕРНЫХ СИЛ

РОССИЙСКАЯ ИНЖЕНЕРНАЯ АКАДЕМИЯ
СЕКЦИЯ «ИНЖЕНЕРНЫЕ ПРОБЛЕМЫ СТАБИЛЬНОСТИ И КОНВЕРСИИ»

СТРАТЕГИЧЕСКАЯ СТАБИЛЬНОСТЬ

№ 1
2018

СТРАТЕГИЧЕСКАЯ СТАБИЛЬНОСТЬ №1 (82) 2018

Научно-практический междисциплинарный журнал
Военная теория, военное строительство, конфликтология, стратегическое планирование и управление, безопасность социально-экономических систем.

Отрасли наук: военные науки [военно – теоретические науки (20.01.00), военно – специальные науки (20. 02.00)].

АКАДЕМИЯ ВОЕННЫХ НАУК
ЦЕНТР ПРОБЛЕМ СТРАТЕГИЧЕСКИХ ЯДЕРНЫХ СИЛ

РОССИЙСКАЯ ИНЖЕНЕРНАЯ АКАДЕМИЯ
СЕКЦИЯ «ИНЖЕНЕРНЫЕ ПРОБЛЕМЫ СТАБИЛЬНОСТИ И КОНВЕРСИИ»

Издается с ноября 1997 г.
Свидетельство о регистрации ПИ №77-3705 от 09.06.2000 г.
ISSN 1680-2772.

Выходит 4 раза в год.

Журнал включен в «Перечень ведущих периодических изданий» ВАК.

Для аспирантов и адъюнктов публикация статей в журнале бесплатная.

СОДЕРЖАНИЕ

I. ВОЕННО-ТЕОРЕТИЧЕСКИЕ ПРОБЛЕМЫ

Подкорытов Ю.А.
Методический аппарат прогнозирования поведения военно-политического руководства государств ходе военной фазы конфликта 2

Ромашкина Н.П.
Информационная безопасность как часть проблемы обеспечения стратегической стабильности 8

Винокуров Г.Н., Ковалев В.И., Коняхин Б.А.
Геополитическая динамика Украины в различных сценарных условиях развития военно-политической обстановки: опыт количественного прогнозирования 14

Акиншина Н.Ю.
Методика оценки эффективности формирования инновационной инфраструктуры оборонно-промышленного комплекса 18

Гриняев С.Н., Гулина Е.В.
Транспортная составляющая геополитического положения России в Центрально-Азиатском и Азиатско-Тихоокеанском регионах 21

II. ВОЕННО-СПЕЦИАЛЬНЫЕ ПРОБЛЕМЫ

Ефремов Е.В.
Построение моделей для исследований применения наземных ударных робототехнических комплексов 25

Ефремов Е.В., Агафонов А.Ю.
Апробация численной методики моделирования боя и информационной модели мотопехоты вероятного противника .. 27

Герасимов В.А., Филоженко А.Ю., Илларионов Г.Ю., Пашкеев С.В.
Подводное базирование автономных необитаемых подводных аппаратов на донных причальных устройствах 30

Викулов С.Ф.
Страницы истории становления нового научного направления – военно-экономический анализ 37

Щербаков Г.Н., Юдин С.С., Моташенко С.В., Верёвкин А.С., Проценко О.П., Сержантов К.Е.
О возможности применения многочастотного метода нелинейной радиолокации для обнаружения террористических взрывных устройств с готовыми поражающими элементами 42

Малков С.Ю., Билюга С.Э., Давыдова О.И.
Использование «ловушек развития» в межгосударственном противоборстве. «Ловушка средних доходов»: моделирование и анализ 47

Кривошонок С.О., Попков Ю.А., Морару А.А.
Совершенствование элементов системы управления боевых бригад сухопутных войск США 57

Кривошонок С.О., Степанов С.В., Морару А.А.
Силы и средства разведывательных формирований перспективных соединений модульного типа сухопутных войск США 60

Аксененко Ю.И., Василенко В.В., Сидак А.А.
Методологический подход к построению комплексных систем мониторинга и реагирования на инциденты информационной безопасности 64

Рыжов Б.С., Володина Н.И., Таразевич Е.С.
Особенности использования автономной системы управления движением автомобиля в условиях информационно-технических воздействий 68

УДК 004.056

© Аксененко Ю.И., Василенко В.В., Сидак А.А.
Aksenenko Y., Vasilenko V., Sidak A.

МЕТОДОЛОГИЧЕСКИЙ ПОДХОД К ПОСТРОЕНИЮ КОМПЛЕКСНЫХ СИСТЕМ МОНИТОРИНГА И РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

METHODOLOGIC APPROACH FOR CONSTRUCTING COMPLEX SYSTEMS OF MONITORING AND RESPONSE ON INFORMATION SECURITY INCIDENTS

Аннотация. *В статье изложен новый подход и на основе обобщения отечественного и зарубежного опыта предложена схема построения комплексных систем мониторинга и реагирования на инциденты информационной безопасности в информационной инфраструктуре. Рассмотрены основные уровни предложенной схемы: сбор, хранение, агрегация, анализ, представление данных, регистрация и отработка инцидентов информационной безопасности. Приведены системные свойства предложенной схемы, отличающие ее от других схем мониторинга, и определены направления ее развития.*

Abstract. *The article describes the new approach and on the basis of generalization of national and foreign experience the scheme for constructing complex systems of monitoring and response on information security incidents in the information infrastructure is proposed. The main levels of the proposed scheme are considered: collection, storage, aggregation, analysis, data representation, registration and information security incident response. The system properties of the proposed scheme are described, which distinguish it from other monitoring schemes, and the directions of its development are determined.*

Ключевые слова*. Информационная безопасность, мониторинг, реагирование на инциденты, агрегация, корреляция.*

Key words. *Information security, monitoring, incident response, aggregation, correlation.*

В настоящее время в сферах управления обороной страны, государственного управления, транспорта, энергетики, авиации, связи и иных критически важных направлениях и отраслях все активнее применяются новые цифровые технологии: обработка и анализ больших массивов данных, технологии искусственного интеллекта, облачные, туманные и мобильные технологии, интернет вещей, системы виртуальной и дополненной реальности.

Преимущества новых цифровых технологий открывают принципиально новые возможности по их использованию в различных сферах, в том числе в сфере межведомственного информационного взаимодействия.

Вместе с тем такие факторы новых цифровых технологий, как концентрация больших объемов чувствительной информации, распределенный характер ее обработки, в том числе с применением различных мобильных устройств, вовлеченность большого количества пользователей, усиливают существующие и порождают новые угрозы и риски для информационной инфраструктуры.

В этой связи актуальность развития мер и средств защиты информации возрастает. Одними из наиболее важных направлений защиты информации являются мониторинг информационной безопасности и реагирование на возникающие инциденты.

При этом в автоматизированных системах как минимум подлежат выявлению следующие типы инцидентов информационной безопасности (по видам контролируемых последствий): несанкционированный доступ, утечка данных, модификация (подмена) данных, отказ в обслуживании, нарушение функционирования (работоспособности) технических средств и систем, неправомерное использование вычислительных или иных ресурсов.

Выявление инцидентов информационной безопасности, как правило, включает (см. рис.1): обнаружение нарушения безопасности информации, идентификацию вида возможных последствий, регистрацию инцидента (с учетом видов контролируемых последствий).

При этом регистрация инцидентов информационной безопасности, как правило, предусматривает создание карточки инцидента информационной безопасности, в которой отражаются дата и время регистрации инцидента информационной безопасности, идентификатор зарегистрированного инцидента информационной безопасности, а также признаки, на основании которых был зарегистрирован инцидент информационной безопасности.

В настоящее время наработан целый ряд различных подходов, методик и инструментов для мониторинга информационной безопасности как в России, так и за рубежом. Существенный импульс развитию направле-

Аксененко Юрий Иванович *– кандидат технических наук, старший научный сотрудник, председатель, ООО «Центр безопасности информации»;*
Василенко Владимир Васильевич *– доктор технических наук, профессор, заместитель председателя, ООО «Центр безопасности информации»;*
Сидак Алексей Александрович *– кандидат технических наук, старший научный сотрудник, заместитель председателя, ООО «Центр безопасности информации», тел. 8(926)296-98-99.*

Aksenenko Yuriy *– candidate of technical sciences, senior researcher, chairman, LLC "Information Security Center";*
Vasilenko Vladimir *– doctor of technical sciences, professor, deputy chairman, LLC "Information Security Center";*
Sidak Alexey *– Candidate of Technical Sciences, Senior Researcher, Deputy Chairman, LLC "Information Security Center", tel. 8 (926) 296-98-99.*

Рис. 1. Общая схема выявления инцидентов информационной безопасности

ния мониторинга информационной безопасности дает новое законодательство [1], нормотворческая и практическая деятельность ФСБ России и ФСТЭК России по обеспечению безопасности объектов критической информационной инфраструктуры Российской Федерации, созданию государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (ГосСОПКА), поддержанию банка данных угроз и уязвимостей, регламентации требований к деятельности по мониторингу и применяемым средствам.

Обобщение и развитие этих результатов на принципах системного подхода позволило сформировать схему (см. рис. 2) построения комплексных систем мониторинга и реагирования на инциденты информационной безопасности в информационной инфраструктуре. В данной схеме выделено четыре унифицированных уровня:

- уровень сбора данных (методы, инструментальные средства, опросные листы) от источников данных (люди, программное обеспечение, программно-технические средства, процессы, технологии, информационные сервисы, среда функционирования, СОПКА);
- уровни хранения и первичной обработки данных (агрегация данных, анализ данных, включая оценку рисков, обработка запросов потребителей информации мониторинга, корреляция событий безопасности информации);
- уровень представления информации мониторинга потребителям (ответы на запросы, информационные панели для осведомленности о ситуации, представление аналитики, выводы, заключения);
- уровень регистрации и отработки инцидентов информационной безопасности (правила, регламенты, средства поддержки групп реагирования на инциденты информационной безопасности и стадий управления инцидентами).

В автоматизированных системах должны применяться автоматизированные средства для выявления инцидентов информационной безопасности. При этом в целях выявления инцидентов информационной безопасности целесообразно использовать потоки данных об угрозах (FEEDs), содержащие индикаторы компрометации (IOC), которые при их обнаружении в информационной (автоматизированной) системе могут свидетельствовать о нарушении безопасности информации.

На каждом из приведенных на рис. 2 уровней схемы обеспечена возможность реализации следующих системных свойств:

- многомерности, обеспечивающей ее вертикальную интеграцию в организационную структуру управления безопасностью ведомств, корпораций и организаций, а также горизонтальное масштабирование по структурным элементам информационной инфраструктуры;
- масштабируемости за счет подключения новых источников информации о событиях безопасности информации;
- адаптивности к новым компьютерным атакам и иным видам нарушений безопасности информации за счет развития правил корреляции событий и регистрации инцидентов безопасности, в том числе с использованием нейронных сетей и иных методов искусственного интеллекта;
- унификации протоколов взаимодействия различных элементов системы мониторинга.

Кроме того, рассматриваемая схема предоставляет следующие возможности:

- развития активной составляющей реагирования на инциденты информационной безопасности;
- развития форм и способов доведения информации мониторинга специалистам служб безопасности;
- наращивания возможностей аналитической работы по оценке выполнения требований безопасности, прогнозированию рисков, определению актуальных угроз безопасности информации, обобщению опыта обработки инцидентов информационной безопасности;
- взаимодействия с иными системами управления информационной безопасностью, в том числе создаваемыми и поддерживаемыми уполномоченными федеральными органами исполнительной власти.

Предлагаемая схема соответствует требованиям нормативных правовых актов и национальным стандартам в области информационной безопасности [2, 3, 4], предполагает использование ресурсов уполномоченных федеральных органов исполнительной власти, содержащих информацию об угрозах, уязвимостях и атаках, ориентирована на использование доверенных средств сбора данных мониторинга.

Отмеченные свойства позволяют использовать предложенную схему мониторинга в масштабных динамично развивающихся ведомственных и корпоративных информационных инфраструктурах.

Архитектура предложенной схемы позволяет проводить модификацию системы мониторинга на уровне сбора данных (под новые источники), на уровне хранения, агрегации и аналитики (для добавления новых типов данных), на уровне представления (для добавления новых форм и каналов доведения информации мониторинга).

Стандартизация (унификация) протоколов взаимодействия различных элементов систем мониторинга и их схем построения позволит получить синергетиче-

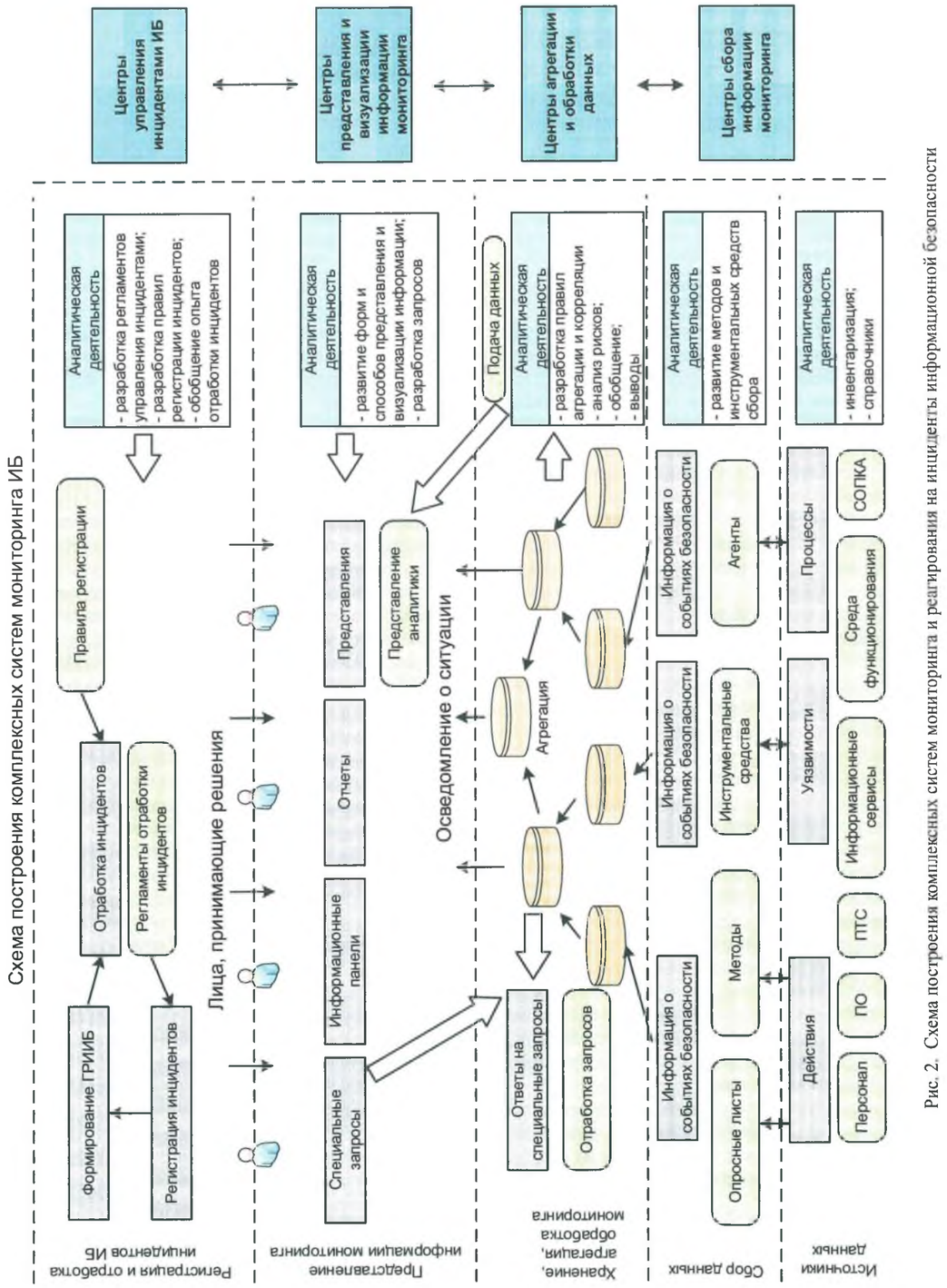

Рис. 2. Схема построения комплексных систем мониторинга и реагирования на инциденты информационной безопасности

ский эффект от применения отечественных средств защиты информации и контроля.

Результаты апробации предложенной схемы в государственных органах и отраслях экономики на базе средств NeuroDAT свидетельствуют о перспективности ее использования при реализации государственной программы «Цифровая экономика» [5], межведомственного информационного взаимодействия, в информационных инфраструктурах различного назначения.

При этом, в связи с внедрением новых цифровых технологий, потребуется постоянная модернизация элементов системы мониторинга и решение интеграционных вопросов:

• развития справочников по информационной инфраструктуре, развития баз уязвимостей, решающих правил, определение новых точек (узлов) контроля;

• определения новых типов критических событий;

• разработки новых политик контроля, агентов, коннекторов и других средств мониторинга;

• разработки новых правил регистрации и регламентов реагирования на инциденты информационной безопасности;

• интенсификации взаимодействия в рамках ГосСОПКА.

Реализация изложенного методологического подхода к построению комплексных систем мониторинга и реагирования на инциденты информационной безопасности, с одной стороны, позволяет организовать эффективное ситуационное управление инцидентами ИБ в информационной инфраструктуре, а с другой стороны, является источником получения достоверных исходных данных для определения актуальных угроз БИ, формирования функциональных требований безопасности автоматизированных систем [6], выбора мер и средств защиты информации.

Литература

1. О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон Российской Федерации от 26 июля 2017 г. №187-ФЗ // Собр. Законодательства Рос. Федерации. – 2017. – № 31, ст. 4736.

2. Указ Президента РФ от 15 января 2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» // СПС ГАРАНТ.РУ.

3. Приказ ФСТЭК России от 11.02.2013 № 17 (ред. от 15.02.2017) «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», зарегистрирован в Минюсте России 31.05.2013 г. №28608 // СПС КонсультантПлюс.

4. ГОСТ Р ИСО/МЭК ТО 18044-2007 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. – М.: Стандартинформ, 2009. – 50 с.

5. Программа «Цифровая экономика Российской Федерации» (утверждена распоряжением Правительства Российской Федерации от 28 июля 2017 г. N 1632-р) // СПС Консультант плюс.

6. Сидак А.А. Обоснование требований по защите информации в автоматизированных системах // Стратегическая стабильность, № 4, 2009, стр. 7–9.

Материал поступил в редакцию 12. 02. 2018 г.