УДК 004.056.5
DOI: 10.26102/2310-6018/2024.46.3.015

Оценка уровня зрелости центра мониторинга информационной безопасности в условиях обеспечения устойчивости риск-управления

А.В. Пономарев✉

Финансовый университет при Правительстве Российской Федерации, Москва, Российская Федерация

Резюме. Оценка эффективности работы центров мониторинга и управления безопасностью является актуальной задачей, от решения которой зависит как надежность всей системы, так и мониторинг, прогнозирование управляемости. Цель работы – провести системный анализ факторов и метрик (индикаторов), влияющих на уровень зрелости центров мониторинга. Данная задача реализуется с помощью идентификации управляющих параметров и прогнозирования (моделирования) устойчивости риск-управления центров при обслуживании запросов. В частности, интерес представляет формирование интегрального показателя устойчивости. В качестве гипотез исследования рассматриваются приемлемая «полоса допусков», устойчивость управления, планирование атак и анализ уязвимостей, необходимость проведения ситуационного моделирования. Использованы методы системного анализа и синтеза, моделирования, теории вероятностей, эвристический подход. Основные результаты статьи: 1) проведен анализ устойчивости политики информационно-экономической безопасности и классификация прямых и косвенных угроз в цифровой бизнес-экосистеме; 2) на основе проведенного анализа предложены адаптивная схема моделирования риск-устойчивости корпоративной системы и формальная оптимизационная модель прогноза устойчивой защиты (по затратам на обеспечение требуемой меры защищенности); 3) в качестве практических приложений предложены вероятностная модель обслуживания запросов в распределенной системе (при заданной интенсивности «подмешивания» запросов злоумышленников) и эвристическая процедура оценки уровня мониторинга устойчивости. Работа развиваема в направлении усложнения моделей, их эластичности и «глубины» учета рисков.

Ключевые слова: оценка, устойчивость, зрелость, центр информационной безопасности, мониторинг, риск, управление.

Для цитирования: Пономарев А.В. Оценка уровня зрелости центра мониторинга информационной безопасности в условиях обеспечения устойчивости риск-управления. *Моделирование, оптимизация и информационные технологии.* 2024;12(3). URL: https://moitvivt.ru/ru/journal/pdf?id=1631 DOI: 10.26102/2310-6018/2024.46.3.015

Assessment of the maturity level of the information security monitoring center in the context of ensuring the sustainability of risk management

A.V. Ponomarev✉

Financial University under the Government of the Russian Federation, Moscow, the Russian Federation

Abstract. Assessment of the effectiveness of the security monitoring and management centers is an urgent task, the solution of which depends on both the reliability of the entire system and monitoring and forecasting. The purpose of the work is to conduct a systematic analysis of factors and metrics (indicators) affecting the maturity level of monitoring centers. This problem is realized by identifying

control parameters and predicting (modeling) the stability of risk management of centers when servicing requests. In particular, the formation of an integral stability index is of interest. The hypotheses of the study are considered an acceptable "tolerance band," control stability, attack planning and vulnerability analysis, the need for situational modeling. Methods of system analysis and synthesis, modeling, probability theory, heuristic approach were used. The main results of the article: 1) analysis of the sustainability of information and economic security policies and classification of direct and indirect threats in the digital business ecosystem; 2) based on the analysis done, an adaptive scheme for modeling the risk stability of a corporate system and a formal optimization model for predicting sustainable protection (based on the cost of ensuring the required security measure) were proposed; 3) as practical applications, a probabilistic model of servicing requests in a distributed system (at a given intensity of "mixing" requests of intruders) and a heuristic procedure for assessing the level of stability monitoring are proposed. The work is developed in the direction of complication of models, their elasticity and "depth" of risk accounting.

Keywords: assessment, sustainability, maturity, information security center, monitoring, risk, management.

For citation: Ponomarev A.V. Assessment of the maturity level of the information security monitoring center in the context of ensuring the sustainability of risk management. *Modeling, Optimization and Information Technology*. 2024;12(3). URL: https://moitvivt.ru/ru/journal/pdf?id=1631 DOI: 10.26102/2310-6018/2024.46.3.015 (In Russ.).

Введение

Цифровые трансформации и усложнение сетевых взаимодействий, в частности, запросов, актуализировали задачи мониторинга, системного анализа и прогнозирования надежности. Критерии, меры оценивания эффективности работы SOC (Центра мониторинга и управления безопасностью, Security Operation Center) должны давать ответ компании-заказчику на вопрос: насколько релевантно (полно, оперативно и устойчиво по рассматриваемым целям компании) SOC-центр реализует свои задачи? Ответ позволит идентифицировать уязвимости, риски, как слабые, так и сильные стороны компании, ее инфраструктуры, а также возможности ее совершенствования (инновационный потенциал, например, базирующийся на KPI [1]).

SOC – автоматизированная система, в условиях цифровых трансформаций управления безопасностью – это подсистема цифровой экосистемы организации. Это экосистема взаимосвязанных проектов для обеспечения инфо-коммуникационной безопасности на основе единого процессного подхода, знаний и языка, описывающего принципы как для поиска, так и идентификации, нейтрализации атак на систему и организации взаимодействий. Такой язык описывает программно-технические принципы как по атакам, так и по их идентификации и противодействию им.

Метрикой (индикатором) релевантности может служить интегральный показатель, опирающийся, например, на количество инцидентов (в мес., квартал или по отношению к прошлому году, в %), KPI, тестирование и др. В работе проводится системный анализ метрик, влияющих на уровень зрелости SOC, и исследуется задача ситуационного моделирования и идентификации управляющих параметров устойчивости обслуживания SOC-запросов.

С использованием системного анализа-синтеза и модельного подхода проведен анализ и классификация угроз в цифровой экосистеме, предложены адаптивные модели риск-устойчивости корпоративной системы и прогноза устойчивости защиты по затратам на защиту.

Материалы и методы

Несмотря на эффективность экспертно-эвристических подходов к оценке зрелости SOC-центров, тем не менее, важно применять формализуемые и структурируемые метрики эффективности, а также соответствующие унифицируемые системы [2], когнитивные модели (карты) [3] и прогнозирование на основе временных рядов [4].

Единого системного подхода и универсальных моделей оценки уровня зрелости SOC [5] нет, но требования к результатам оценивания сформулируем следующим образом:

1) достоверность, массовость и воспроизводимость;
2) четкость, простота и последовательность проведения;
3) охват всего жизненного цикла;
4) универсальность набора учитываемых показателей уровня зрелости;
5) формализация и ранжирование оценочных критериев, шкалирование оценок;
6) методологическая поддержка процедуры оценивания с учетом уровня подготовки оценивающего;
7) адаптивность к потребностям организации и др.

Основными гипотезами рассматриваемых задач являются следующие условия:

1) недопущение снижения показателей устойчивости в требуемом периоде («полосе допусков»);
2) устойчивость управления согласно спецификациям по обеспечению устойчивости и ресурсных затрат на мониторинг сети и аудит безопасности для возврата на устойчивую траекторию функционирования;
3) атаки планируются, поэтому при анализе уязвимостей, меры и методы анализа адаптируют под уязвимости, под ситуационное моделирование.

Для распределенной сети необходимо учитывать динамическое состояние, например, в системах VPN, неопределенности вносит и их гибридная структура, устойчивость к шумам в данных, потоках и транзакциях.

Результаты

Проблема и аналитика обеспечения единства информационной и экономической безопасности и устойчивости цифровой экосистемы

Защищенность цифровой инфраструктуры – актуальная проблема в условиях разнообразных рисков и уязвимостей системы [6–7]. В информационной распределенной системе (далее, система) чаще организуются целевые атаки на ИТ-инфраструктуру, цифровую экосистему (далее, экосистема). Такие атаки направлены на ключевые подсистемы, в частности, управления. Это критически важные и чувствительные к деструктивным воздействиям информационные подсистемы.

Информационная безопасность компании – обеспечение защищенности ее инфраструктуры от случайных или запланированных воздействий и минимизации возможного ущерба при реализации таких действий.

Согласно данным TAdviser, опросам ГК «Солар» (крупнейший российский коммерческий SOC) 153 компаний сегментов типа B2G, B2B, B2D и B2SMB из больших городов России, 92 % из них профессионально заняты проблемой безопасности инфраструктуры, а 31 % уже выявляют веб-угрозы для нейтрализации. Наиболее частыми и опасными угрозами компаний стали утечки данных (33 %), атаки с выводом информационных активов (26 %), фейк-новости (25 %) и публикации в СМИ негативного характера (16 %). Средний («поинцидентный») ущерб превысил 2 млн. руб.

Заслуживает внимания факт, что более 56 % специалистов на рынке систем и услуг информационной безопасности недостаточно освоили сервисы идентификации интернет-угроз и только 11 % компаний хорошо освоили такие сервисы (43 % остальных пока не тестировали подобные решения), в отличие от представителей крупного бизнеса, агенты среднего бизнеса лучше ознакомлены с сервисами.

Сервис мониторинга цифровых угроз со стороны бизнес-окружения идентифицировал в 2023 году, что 92 Тб конфиденциальных данных российских организаций появилось в открытом доступе.

Основные цели компьютерных преступлений – шифрование с целью вымогательства, шпионаж. На проектирование, взлом киберпреступники в среднем тратят 7 дней. Их привлекает уже не отдельные подсистемы, а вся ИТ-инфраструктура государства, корпорации, критических сфер, например, энергетических. Но российские компании усиливают стойкость внешнего периметра. Уязвимости во внешнем параметре, в частности, слабость паролей и отсутствие вторичной аутентификации, позволяют часто получать контроль ресурсов, осуществлять SQL-инъекции кодов.

В 2023 году по данным «РТК-Солар» усиление за год достигло почти 30 %, по сравнению с годом раньше (23 %). Уровень защищенности корпоративных веб-решений (считаются традиционно наиболее слабым звеном во внешнем периметре) вырос до 53 % (в 2022 году – 20 %).

Большое внимание стали уделять и защищенности персональных данных, повышению ответственности обрабатывающих их операторов и приложений. К этой группе относят все данные, прямо или косвенно относящиеся к человеку.

Закон[1] обязывает компании и индивидуальных предпринимателей уведомлять Роскомнадзор об инцидентах, утечках в течение 24 часов, а в течение 72 часов – сообщать о результатах внутреннего расследования по ним. Большое внимание в законе уделяется трансграничной передаче личных данных, а именно, срокам, ограничениям и потенциальному ущербу.

Есть сложности с реализацией закона № 266. По данным опросов группы ИБ-консалтинга компании «К2 Интеграция», около 66 % компании не приступили еще к выполнению последних требований и только 3 % полностью реализовали все требования ФЗ-266. Многим сложно самостоятельно разбираться в нюансах оценки ущерба (53 %).

Устойчивость бизнес-инфраструктуры к различным классам рисков ИТ-инфраструктуры и ее моделирование

Моделирование риск-устойчивости – это многокритериальная задача, требующая учета неопределенности, возможного ущерба [8].

Распространены прямые и косвенные атаки на цифровую бизнес-экосистему. Классификация необходима, поэтому предложим следующую классификацию атак для распределенной корпоративной системы:

1) IP-спуфинг, подмена IP-адреса («камуфляж злоумышленника под пользователя») с имитацией прав доступа (внедрением вредоносных команд в поток);

2) SQL-инъекция, несанкционированное внедрения вредоносных команд (сценариев в код запроса) управления потоком информации;

3) «уязвимость нулевого дня», обнаруженный злоумышленником раньше программиста баг без патчей;

[1] Федеральный закон от 14.07.2022 № 266-ФЗ «О внесении изменений в Федеральный закон «О персональных данных», отдельные законодательные акты Российской Федерации и признании утратившей силу части четырнадцатой статьи 30 Федерального закона «О банках и банковской деятельности».

4) DDoS-атака, воздействие на трафик с целью блокирования сервера;

5) вирусная атака и внедрение в систему с последующим воздействием на клиентские устройства (приложения);

6) сетевая разведка, несанкционированное сканирование информации, например, с помощью DNS-запросов;

7) нарушение работоспособности, устойчивости сетевого обеспечения и др.

Общим классом спуфинга, хакинга и других типов атак является MITM-атаки (Man In The Middle) [9].

Следует поддерживать систему в состоянии, устойчивом функционально и по управлению, причем в течение задаваемого минимального промежутка времени (наработки на отказ, как в технических системах) и для эволюционного процесса всей системы.

Предлагается адаптивная схема моделирования риск-устойчивости корпоративной системы (Рисунок 1).

Рисунок 1 – Схема моделирования риск-устойчивости
Figure 1 – Risk-robustness modeling scheme

Сформулируем такую оптимизационную задачу: если x_i – количество (объем) необходимого для устойчивой защищенности системы цифрового ресурса типа i, то необходимо минимизировать форму

$$\min \sum_{i=1}^{n} (L_i + T_i + S_i + R_i)$$

$$t_i \le T, \;\; L_i,\, T_i,\, S_i, R_i \ge 0,$$

где L_i – затраты на обеспечение безопасности, T_i – затраты на технологическую поддержку канала актуализации информации, S_i – затраты на мониторинг и сбор данных

(ЦОД, БД), R_i – ущерб от риска в получении данных (например, недостоверного предоставления данных).

Можно считать, что $R_i = p_i I_i$, где p_i – вероятность некачественной информации, I_i – снижение устойчивости из-за некачественной обработки информации, t_i – срок актуальности данных, удовлетворения потребностей клиентов при выборе цифрового ресурса, технологии *i.*

При атаках на распределенные сетевые ресурсы строятся соответствующие модели с учетом вероятностей обслуживания запросов в момент t в объеме $n = 0, 1, \dots, N$, где $T -$ длительность обслуживания операций, а P_n – вероятность блокирования запросов во время атак.

Из потока выбирается и обслуживается регулярный поток, а обслуживание прекращается до завершения атаки. Для системы входной поток считается также распределенным, например, по Бернулли, а именно, запрос с вероятностью α_0 сразу запускается, запрос с вероятностью $(1 - \alpha_0)$ ставится в очередь.

Интенсивность «подмешивания» запросов злоумышленников в поток может увеличить ожидание в очереди.

Распределение заявок по теории массового обслуживания полагаем равным величине:

$$P_n = \frac{(1-P)P^n}{1-P^{N+1}},$$

где

$$P = \lambda b, \lambda = \lambda_0 k$$

являются, соответственно, интенсивностью общего потока, а k – количеством заявок, b – средним временем обслуживания.

Интенсивность выбираем по условию:

$$\lambda \neq 1/b.$$

Тогда

$$P_N = \frac{(1-P)P^N}{1-P^{N+1}},$$

а среднее количество заявок равно:

$$L = \sum_{n=1}^{N} n\, P_n.$$

Подстановкой выражения P_N и итеративными рекуррентными подстановками можно получить выражение:

$$L = \frac{P(1-(N+1)P^N + NP^{N+1})}{(1-P^{N+1})(1-P)}.$$

По формуле Литтла [10], среднее время обслуживания запросов равно:

$$T = \frac{L}{(1-P^N)}$$

или

$$T = \frac{P^{N+1}(NP-N-1)+P}{(1-P^N)(1-P)}.$$

Тестовый пример. Для входных параметров

$$N = 10, b = 0{,}001,\ \lambda_0 = 3\ (1/\text{сек}), k = 101,$$

получаем время $T = 0{,}00135$ сек. Можно проигрывать различные ситуации, варьируя b, λ_0, N.

Пусть запрос «проскочил» фильтр защиты и перешел на уровень данных, то политика безопасности явно «провалила» защиту.

Часто используются экспертно-эвристические подходы к оценке уровня мониторинга устойчивости. Если a_{ij} $(i = 1,2, \dots, n; j = 1,2, \dots, m)$ – оценка j-го эксперта по i-ой характеристике (i-му фактору) x_i риска, то можно сформировать матрицу

$$A = \|a_{ij}\|_{i=1,\dots,n}^{j=1,\dots,m}.$$

Это последовательность матриц

$$A^{(k)} = \left\|a_{ij}^{(k)}\right\|_{i=1,\dots,n}^{j=1,\dots,m}$$

последовательно уточняемых оценок

$$y_i^{(k)} = A^{(k)} y_i^{(k-1)}.$$

Можно определить оценку «шума» (энтропии) в классической форме:

$$H_i^{(k)} = -\sum_{j=1}^{m} d_{ij}^{(k)} \log_2 d_{ij}^{(k)}.$$

Оценка потенциала защищенности и устойчивости распределенных систем опирается на классификацию угроз по опасности и защитных мер по классам. Класс защищенности определим «индексом риска», размахом:

$$R = R_{max} - R_{min},$$

где R_{max}, R_{min} – максимальный рейтинг защищенности данных и минимальный рейтинг допуска пользователей.

Сложность оценивания защищенности и сложность мониторинга безопасности определяют сложность проведения мониторинга.

Обсуждение

Сетевые атаки могут быть «многоволновыми» и «многоуровневыми». Например, четырехуровневой: уровня аттестации, уровня сертификации DevNet, уровня бизнес-почты и уровня базы клиентов корпорации.

Следует поддерживать систему в состоянии, устойчивом как функционально, так и по управлению, причем в течение задаваемого минимального промежутка времени (наработки на отказ, как в технических системах). Это необходимо и для эволюционного процесса всей системы.

Значения метрик и их учет важны, но анализ тенденции (трендов) и эволюционных изменений – более важны. Они позволят контролировать и адаптировать, корректировать процессы на всех рассмотренных выше уровнях.

Эффективность SOC и политики стратегической безопасности организации определяют метрики и результативность оценки эффективности SOC-центра, его команды.

Заключение

Особенностью современного рынка является ликвидация промежуточных звеньев цепи «поставщики-потребители». Инфраструктура бизнеса к этому адаптируется, реагирует оперативно на риски и уязвимости управления сложными, хаотическими

процессами. Эффективный и полный системный анализ-синтез целей и возможностей рынка необходим для моделирования и прогнозирования возможностей компании с цифровой инфраструктурой.

Предложенные в работе подход и ситуационные модели прогноза устойчивости SOC позволят на практике выстроить политику безопасности с оптимизацией затрат на обслуживание запросов при заданной интенсивности «подмешивания» запросов злоумышленников. Приведена и соответствующая эвристическая процедура оценки уровня устойчивости. Работа развиваема в направлении усложнения моделей, их эластичности и «глубины» учета рисков.

Усложнение структур, подходов и критериев устойчивости требует интеграции политики риск-менеджмента и безопасности инфраструктуры, персонала, ресурсов. Работа может быть развита в направлении усложнения моделей, их эластичности.

СПИСОК ИСТОЧНИКОВ / REFERENCES

1. Kaziev M.V., Medvedeva L.B., Tyutrin N.O., Khizbullin F.F., Takhumova V.O. Improvement and modeling of the company's activity based on the innovative KPI system. *Journal of Fundamental and Applied Sciences*. 2018;10(5S):1406–1415.
2. Велигодский С.С., Милославская Н.Г. Унифицированная модель зрелости центров управления сетевой безопасностью информационно-телекоммуникационных сетей. *Известия ЮФУ. Технические науки*. 2023;(3):157–172. https://doi.org/10.18522/2311-3103-2023-3-157-172
   Veligodskiy S.S., Miloslavskaya N.G. Unified model of maturity of network security centers of information and telecommunication networks. *Izvestiya YuFU. Tekhnicheskie nauki = Izvestiya SFedU. Engineering Sciences.* 2023;(3):157–172. (In Russ.). https://doi.org/10.18522/2311-3103-2023-3-157-172
3. Максимова Е.А. Когнитивное моделирование деструктивных злоумышленных воздействий на объектах критической информационной инфраструктуры. *Труды учебных заведений связи.* 2020;6(4):91–103. https://doi.org/10.31854/1813-324X-2020-6-4-91-103
   Maksimova E. Cognitive modeling of destructive malicious impacts on critical information infrastructure objects. *Trudy uchebnykh zavedenii svyazi = Proceedings of Telecommunication Universities.* 2020;6(4):91–103. (In Russ.). https://doi.org/10.31854/1813-324X-2020-6-4-91-103
4. Андрюхин Е.В., Ридли М.К., Правиков Д.И. Прогнозирование сбоев и отказов в распределенных системах управления на основе моделей прогнозирования временных рядов. *Вопросы кибербезопасности*. 2019;(3):24–32.
   Andryukhin E.V., Ridli M.K., Pravikov D.I. Prediction of faults and failures in distributed control systems based on time series forecasting models. *Voprosy kiberbezopasnosti.* 2019;(3):24–32. (In Russ.).
5. Скрыль С.В., Гайфулин В.В., Домрачев Д.В., Сычев В.М., Грачёва Ю.В. Актуальные вопросы проблематики оценки угроз компьютерных атак на информационные ресурсы значимых объектов критической информационной инфраструктуры. *Безопасность информационных технологий*. 2021;28(1):84–94. https://doi.org/10.26583/bit.2021.1.07
   Skryl' S.V., Gaifulin V.V., Domrachev D.V., Sychev V.M., Gracheva Yu.V. Topical issues of the problem of assessment of threats of cyber attacks on information resources of significant facilities of critical information infrastructure. *Bezopasnost' informatsionnykh tekhnologii = IT Security (Russia)*. 2021;28(1):84–94. (In Russ.). https://doi.org/10.26583/bit.2021.1.07

6. Гаськова Д.А., Массель А.Г. Технология анализа киберугроз и оценка рисков нарушения кибербезопасности критической инфраструктуры. *Вопросы кибербезопасности*. 2019;(2):42–49.
Gaskova D.A., Massel A.G. The technology of cyber threat analysis and risk assessment of cybersecurity violation of critical infrastructure. *Voprosy kiberbezopasnosti.* 2019;(2):42–49. (In Russ.).
7. Лапсарь А.П., Назарян С.А., Владимирова А.И. Повышение устойчивости объектов критической информационной инфраструктуры к целевым компьютерным атакам. *Вопросы кибербезопасности*. 2022;(2):39–51.
Lapsar' A.P., Nazaryan S.A., Vladimirova A.I. Ensuring the resistance of critical information infrastructure objects to advanced persistent threats. *Voprosy kiberbezopasnosti.* 2022;(2):39–51. (In Russ.).
8. Таныгин М.О., Будникова Ю.А., Булгаков А.С., Марченко М.А. Модель оценки ущерба от инцидентов информационной безопасности. *Безопасность информационных технологий*. 2021;28(2):98–106. https://doi.org/10.26583/bit.2021.2.09
Tanygin M.O., Budnikova Yu.A., Bulgakov A.S., Marchenko M.A. A model for assessing information security incidents damage. *Bezopasnost' informatsionnykh tekhnologii = IT Security (Russia)*. 2021;28(2):98–106. (In Russ.). https://doi.org/10.26583/bit.2021.2.09
9. Золотавин В.С., Нечта И.В. Обзор сетевых атак типа Man-in-the-middle (MITM). В сборнике: *Обработка информации и математическое моделирование: Материалы Всероссийской научно-технической конференции с международным участием, 19–20 апреля 2023 года, Новосибирск, Россия.* Новосибирск: Сибирский государственный университет телекоммуникаций и информатики; 2023. С. 279–285.
Zolotavin V.S., Nechta I.V. Overview of Man-in-the-middle (MITM) network attacks. In: *Obrabotka informatsii i matematicheskoe modelirovanie: Materialy Vserossiiskoi nauchno-tekhnicheskoi konferentsii s mezhdunarodnym uchastiem, 19–20 April 2023, Novosibirsk, Russia*. Novosibirsk: Siberian State University of Telecommunications and Information Science; 2023. pp. 279–285. (In Russ.).
10. Тихоненко О.М. Система обслуживания с разделением процессора и ограниченными ресурсами. *Автоматика и телемеханика*. 2010;(5):84–98.
Tikhonenko O.M. Queuing system with processor sharing and limited resources. *Automation and Remote Control*. 2010;71(5):803–815. https://doi.org/10.1134/S0005117910050073

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Пономарев Александр Владимирович, аспирант кафедры информационной безопасности, Финансовый университет при Правительстве Российской Федерации, Москва, Российская Федерация.
e-mail: ponomarevsandr@gmail.com

Aleksandr V. Ponomarev, Postgraduate student of the Department of Information Security, Financial University under the Government of the Russian Federation, Moscow, the Russian Federation.

Статья поступила в редакцию 15.07.2024; одобрена после рецензирования 22.07.2024; принята к публикации 31.07.2024.

The article was submitted 15.07.2024; approved after reviewing 22.07.2024; accepted for publication 31.07.2024.