ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004.492.4
DOI: 10.21822/2073-6185-2025-52-3-135-151 Оригинальная статья/ Original article

Методология выбора критериев эффективности системы информационной безопасности при имитационных атаках Red Team

С.А. Резниченко [1,2,3], Д.Р. Турабов[1]
[1] Финансовый университет при Правительстве Российской Федерации,
[1]125167, г. Москва, Ленинградский пр-т, 49/2, Россия,
[2] Национальный исследовательский ядерный университет «МИФИ»,
[2]115409, г. Москва, Каширское шоссе, 31, Россия,
[3] Российский государственный гуманитарный университет,
[3]125047, г. Москва, Миусская площадь, д. 6, Россия

Резюме. Цель. В статье предлагается методология выбора критериев оценки эффективности системы информационной безопасности организации на основе проведения имитационных атак типа Red Team. Актуальность исследования обусловлена ростом сложности кибератак и потребностью в объективной проверке готовности организаций различного масштаба – от объектов критической информационной инфраструктуры до финансового и государственного секторов – противостоять целенаправленным атакам. **Метод.** Методология сочетает сравнительный анализ существующих подходов, кейс-стади реальных киберучений, моделирование угроз (с опорой на матрицу MITRE ATT&CK) и экспертные интервью со специалистами по безопасности. **Результат.** Проведен обзор нормативных документов (российских ГОСТ и федеральных законов, стандартов ФСТЭК, международных стандартов ISO/IEC 27001, рекомендаций NIST SP 800-53) и современных практик команд Red Team/Blue Team, включая использование систем SIEM, SOAR и XDR. Произведена классификация показателей эффективности защиты (время обнаружения инцидента, скорость реагирования, полнота выявления атак и др.), иллюстрированные примерами из практики и схемами архитектуры центров мониторинга безопасности с интеграцией SIEM/SOAR. **Вывод.** Представлены альтернативные подходы к оценке (аудит без активных атак, пентесты), ограничения и риски Red Team-методов, даны рекомендации по учету результатов имитационных атак в нормативном регулировании и корпоративном аудите.

Ключевые слова: информационная безопасность, имитационные атаки, Red Team, Blue Team, критерии эффективности, SIEM, SOAR, критическая инфраструктура, показатели безопасности, оценка защищенности

Для цитирования: С.А. Резниченко, Д.Р.Турабов. Методология выбора критериев эффективности системы информационной безопасности при имитационных атаках Red Team**.** Вестник Дагестанского государственного технического университета. Технические науки. 2025; 52(3):135-151. DOI:10.21822/2073-6185-2025-52-3-135-151

Methodology for selecting effectiveness criteria of information Security Systems during Red Team simulated attacks

S.A. Reznichenko[1,2,3], D.R.Turabov[1]
[1]Financial University under the Government of the Russian Federation,
[1]49 Leningradsky Ave., Moscow 125167, Russia,
[2]National Research Nuclear University "MEPhI",
(Moscow Engineering Physics Institute),
[2]31, Kashirskoe Highway, Moscow 115409, Russia,
[3] Russian State University for the Humanities,
[3]6, Miusskaya Square, Moscow 125047, Russia

Abstract. Objective. A methodology is proposed for selecting criteria for assessing the effectiveness of an organization's information security system based on conducting simulated Red Team attacks. This urgency is driven by the growing sophistication of cyberattacks and the need to test the readiness of organizations of various sizes - from critical information infrastructure facilities to the financial and government sectors - to withstand targeted attacks. **Method.** The methodology combines a comparative analysis of existing approaches, case studies of real cyber exercises, threat modeling (based on the MITRE ATT&CK matrix), and expert interviews with security specialists. **Result.** A review of regulatory documents (Russian GOST standards and federal laws, FSTEK guidelines, international standards ISO/IEC 27001 and NIST SP 800-53) and modern Red Team/Blue Team practices, including the use of SIEM, SOAR, and XDR systems, is conducted. A classification of security performance indicators (incident detection time, response speed, attack detection rate, etc.) is provided, illustrated with practical examples and architecture diagrams of security monitoring centers with SIEM/SOAR integration. **Conclusion.** Alternative approaches to assessment (audit without active attacks, pentests), limitations and risks of Red Team methods and recommendations for taking into account the results of simulated attacks in regulatory frameworks and corporate audits are provided.

Keywords: information security, simulated attacks, Red Team, Blue Team, effectiveness criteria, SIEM, SOAR, critical infrastructure, security metrics, security assessment

For citation: S.A. Reznicenko, D.R. Turabov. Methodology for selecting effectiveness criteria of information Security Systems during Red Team simulated attacks. Herald of Daghestan State Technical University. Technical Sciences. 2025;52(3):135-151. (In Russ) DOI:10.21822/2073-6185-2025-52-3-135-151

Введение. Интенсивность и изощренность современных кибератак непрерывно возрастают, особенно в отношении критически важных систем – объектов критической информационной инфраструктуры (КИИ), финансовых организаций и государственных информационных систем. Традиционные подходы к обеспечению информационной безопасности (ИБ) основаны на внедрении средств защиты и соответствии нормативным требованиям, однако одним из ключевых вызовов остается оценка реальной эффективности системы ИБ: насколько быстро и полно организация способна обнаружить и пресечь сложную целевую атаку.

Все большее распространение получают учения типа Red Team vs Blue Team, при которых группа экспертов (Red Team) имитирует действия злоумышленника, а команда защиты (Blue Team) пытается обнаружить и отразить эти действия. Такой подход позволяет проверить безопасность «боем» и выявить *слепые зоны* в защите, недоступные при обычных аудиторских проверках. Актуальность применения Red Team-упражнений подтверждается как мировыми трендами, так и требованиями нормативных документов. Так, российский Закон о персональных данных №152-ФЗ обязывает до ввода в эксплуатацию информационных систем проводить оценку эффективности мер защиты персональных данных. Для субъектов КИИ закон №187-ФЗ устанавливает необходимость создания системы безопасности, обеспечивающей непрерывное обнаружение атак и взаимодействие с государственной системой обнаружения и предотвращения атак (ГосСОПКА) [1]. Международные стандарты менеджмента ИБ (ISO/IEC 27001) также косвенно требуют проверки защитных мер, а в новой редакции NIST SP 800-53 Rev.5 прямо введены требования проактивного *adversarial testing* (включая Red Team-упражнения) для повышения киберустойчивости. Тем не менее, единых методических рекомендаций по выбору критериев эффективности при таких проверках пока недостаточно.

Как количественно измерять результативность работы Blue Team? Какие метрики считать ключевыми для оценки защищенности? Эти вопросы становятся все более значимыми [2].

Постановка задачи. Цель исследования состоит в разработке и обосновании методологии выбора критериев оценки эффективности системы информационной безопасности

при проведении имитационных атак (учений типа Red Team) в организациях различного масштаба.

Для достижения цели в работе решаются следующие задачи: анализ нормативной базы и существующих практик Red Team/Blue Team с выявлением используемых показателей; формализация системы критериев и показателей эффективности ИБ, пригодных для различных сфер (КИИ, финсектор, госорганы); разработка методики их применения, включающей сценарии угроз, интеграцию с инструментами мониторинга (SIEM, SOAR) и процедуру сбора данных; апробация методологии на примерах (кейсах) и сравнение с альтернативными подходами; выработка рекомендаций для нормативного регулирования и корпоративной практики.

Российская нормативная база в области ИБ закрепляет необходимость оценивать эффективность защиты информации. В частности, Федеральный закон №152-ФЗ «О персональных данных» требует от операторов персональных данных принятия мер защиты, включая *оценку эффективности этих мер до ввода системы в эксплуатацию*. Это означает, что организации должны проверять, насколько действенны реализованные средства защиты ПДн. Закон обязывает обеспечивать обнаружение фактов несанкционированного доступа и реагирование на инциденты – фактически, наличие процессов мониторинга и реагирования.

Для критической информационной инфраструктуры закон №187-ФЗ «О безопасности КИИ» устанавливает принципы непрерывной защиты: система безопасности значимых объектов КИИ должна предотвращать несанкционированные доступы и обнаруживать атаки с взаимодействием с ГосСОПКА. Также вводится понятие *оценки безопасности КИИ*, проводимой уполномоченным органом (ФСТЭК/ФСБ) для прогнозирования угроз и выработки мер по повышению устойчивости.

Таким образом, на государственном уровне регламентирована потребность в периодической оценке защищенности, хотя конкретные методики этих оценок могут различаться. ФСТЭК России выпускает ведомственные приказы и методические документы (например, требования к защите персональных данных, к системам ГосСОПКА и др.), в которых, как правило, оговаривается необходимость проведения испытаний защиты, аттестационных тестов или аудитов.

Однако терминология «Red Team» прямо в российских стандартах пока не употребляется, хотя, по сути, имитационные атаки могут являться инструментом выполнения требований по «оценке эффективности мер» (формулировка 152-ФЗ) или «тестированию уязвимостей» (в контексте аттестации систем) [1]. Для финансового сектора Банк России ввел стандарт ГОСТ Р 57580.1-2017, устанавливающий требования по защите информации в банковской сфере. Стандарт ориентирован на обеспечение соответствия банков требованиям ИБ и предусматривает комплекс мер, включая анализ рисков, мониторинг событий и регулярные проверки.

При оценке соответствия ГОСТ Р 57580 рекомендуются моделирование угроз и тестирование на проникновение как способы проверки эффективности как организационных, так и технических мер. В рамках аудита по ГОСТ 57580 банковские организации фактически проводят Red Team/PenTest-упражнения, проверяя способность своих систем обнаружить и остановить проникновение. Нормативные акты высшей силы (законы) формулируют требования *что должно быть сделано*, тогда как подзаконные акты и стандарты (приказы ФСТЭК, ГОСТ) уточняют *как достигать* этого – в том числе через регулярное тестирование безопасности [3].

Международные стандарты также адресуют проблему измерения эффективности ИБ. ISO/IEC 27001:2013 (ГОСТ Р ИСО/МЭК 27001-2019) требовал внедрения системы управления информационной безопасностью (СУИБ) с циклом непрерывного улучшения (PDCA), но напрямую не регламентировал показатели эффективности – предоставляя организациям самостоятельный выбор контролируемых метрик [4].

Для восполнения этого, стандарт ISO/IEC 27004:2016 был разработан специально для измерения результативности СУИБ. ISO 27004 дает руководящие указания по выбору и применению *метрик информационной безопасности*, включая установление измеримых целей, сбор и анализ данных, а также отчетность. Хотя ISO 27004 фокусируется на общей эффективности процессов ИБ, многие предлагаемые в нем метрики (например, время реагирования на инцидент, количество инцидентов по типам, степень покрытия политики безопасности) релевантны и для оценки работы Blue Team. Таким образом, при разработке критериев в нашем исследовании мы учитываем принципы ISO 27004 – в частности, требование четкой привязки метрики к цели безопасности и возможности ее количественного измерения [5].

Еще один важный международный ориентир – рекомендации NIST (США). Специальное издание NIST SP 800-53 Rev.5 «Security and Privacy Controls for Information Systems» содержит контроллер CA-8 (Penetration Testing) и новый контроль CA-9 (Red Team Exercises) для систем высокого уровня воздействия. Например, NIST 800-53 рекомендует «*employ red-team exercises to simulate attempts by adversaries to compromise organizational systems»*– т.е. проводить регулярные игры с участием “команды противника” для проверки защиты. Эти упражнения должны выполняться в рамках определенных правил (Rules of Engagement) и в координации с руководством организации.

На уровне лучших практик признано, что Red Team-ассессмент является неотъемлемой частью комплекса мер по обеспечению безопасности, дополняющей обычное сканирование уязвимостей и тесты на проникновение. Кроме того, NIST выпустил руководство SP 800-115 «Technical Guide to Information Security Testing and Assessment», в котором описаны методики проведения тестирований – от пассивного анализа до активных атак. Там подчеркивается ценность *«full-scope testing»*, когда проверяется весь цикл от проникновения до реакции персонала [6]. Концепция Red Team / Blue Team и метрики эффективности.

В профессиональной литературе широко описывается разделение ролей на «красную» и «синюю» команды при учениях по безопасности. Red Team – это группа квалифицированных экспертов, выступающая на стороне нападения. Они применяют методы и тактики реальных злоумышленников (так называемые TTP – tactics, techniques, and procedures) для преодоления защитных мер организации. Цель Red Team – путем контролируемой атаки проверить, насколько существующие средства защиты и процессы способны противостоять реальной угрозе.

Метрики, связанные с Red Team, оценивают эффективность средств защиты (например, удалось ли обойти межсетевые экраны, системы обнаружения вторжений, методы аутентификации и т.д.). Blue Team, напротив, – это команда защиты, обычно состоящая из сотрудников центра мониторинга безопасности (SOC), администраторов и других ответственных лиц организации. Их задача – обнаружить, расследовать и пресечь злонамеренную активность, действуя в режиме реального времени.

Соответственно, показатели Blue Team отражают эффективность процессов мониторинга и реагирования на инциденты. Например, скорость обнаружения атаки, правильность классификации инцидента, своевременность уведомления руководства и выполнение процедур реагирования. В последние годы выделяется и, так называемая, Purple Team – совмещенный формат, при котором красная и синяя команды работают совместно, обмениваясь информацией для максимального улучшения защитных механизмов. Purple Team не столько отдельная команда, сколько процесс коллаборации: знания Red Team о техниках атак передаются Blue Team для обучения, и наоборот, Blue Team делится с «красными» информацией о том, какие сценарии были самыми трудными для обнаружения.

Цель – повысить общую результативность упражнений, но при этом измерение эффективности все равно осуществляется раздельно для наступательной и оборонительной составляющих. Какие же конкретные метрики и критерии применяются на практике в рамках Red Team-учений? Согласно Hollis (2024), ключевыми показателями (KPI) являются временные показатели и показатели покрытия. Приведем основные из них:[7]

- Среднее время до обнаружения (Mean Time To Detect, MTTD): промежуток от начала враждебной активности (действия Red Team) до момента, когда Blue Team впервые идентифицирует признаки атаки. Этот показатель отражает эффективность мониторинга: чем меньше MTTD, тем быстрее команда безопасности узнает об инциденте. MTTD складывается из времени обнаружения по разным техническим шагам атаки, усредненного по количеству попыток. Очевидно, что низкое значение MTTD – желательный результат (инциденты замечаются рано).
- Среднее время до реагирования (Mean Time To Respond, MTTR): время от обнаружения инцидента до начала активных действий по его нейтрализации Blue Team. Иначе говоря, как быстро команда переходит от факта фиксации проблемы к реализации плана реагирования (активирует процессы incident response). MTTR показывает оперативность процедур реагирования; уменьшение этого показателя свидетельствует о росте готовности своевременно пресечь атаку.
- Среднее время до начального проникновения (Mean Time To Initial Access, MTTIA): показатель со стороны Red Team, измеряющий, сколько времени уходит у «противника» на получение первоначального несанкционированного доступа в систему. Он начинается с нулевого момента атаки (например, рассылки фишинговых писем или начала сетевого сканирования) и заканчивается в момент, когда Red Team удалось проникнуть во внутрь сети (получить доступ, закрепиться). MTTIA характеризует прочность периметра и устойчивость пользователей к социальным атакам. Чем больше времени требуется злоумышленнику, тем лучше работают превентивные меры (межсетевые экраны, фильтрация, обучение сотрудников против фишинга). В упражнениях MTTIA измеряется на основе нескольких попыток проникновения, деленных на их количество.
- Среднее время до действия (Mean Time To Act, MTTA): метрика, отражающая промежуток от момента, когда Blue Team начала реагирование, до момента применения конкретных мер по устранению угрозы. Другими словами, насколько быстро после сбора команды реагирования происходит, например, блокировка скомпрометированного аккаунта, изоляция зараженного узла, патч уязвимости и т.п. Показатель MTTA фокусируется на скорости эскалации и реализации решения внутри организации. Его значение особенно важно для комплексных инцидентов, требующих участия нескольких команд (например, ИТ-отдел должен отключить сегмент сети по запросу ИБ).
- Время до полного устранения (Time To Full Remediation, TTFR): завершающий показатель цикла, измеряющий, сколько времени занимает полное устранение последствий атаки. Отсчет идет от конца упражнения (или момента, когда уязвимость Red Team раскрыта Blue Team) до завершения всех ремедиционных мероприятий: установка заплат, изменение процедур, принятие риска или другие действия, зафиксированные в плане обработки рисков. TTFR может измеряться в часах или днях и показывает, насколько эффективно организация закрывает выявленные «дыры» после учений.

Кроме указанных KPI, в ходе Red Team-оценок могут собираться и другие метрики эффективности: доля обнаруженных техник из общего числа используемых (coverage), количество уязвимостей, эксплуатированных Red Team (чем меньше – тем лучше защита), процент успешных фишинговых атак на сотрудников, число инцидентов, выявленных автоматизированными средствами (SIEM) без участия человека, и т.д.

Например, в отчете CISA (2023) по итогам Red Team-оценки крупной организации отмечено, что несмотря на зрелую инфраструктуру безопасности, ни одна из активностей Red Team не была обнаружена штатными средствами мониторинга. Команда CISA даже пыталась нарочно «создать шум», чтобы сработали алармы, но организация не отреагировала. Этот случай демонстрирует необходимость отслеживать метрику *доля незамеченных атак* – стремясь минимизировать ее. Другой пример: в финансовом секторе по программам

CBEST и TIBER-EU регуляторы смотрят на способность банка отразить имитацию сложной кибератаки, при этом «временна́я шкала» обнаружения и реагирования является основным критерием успеха. Все эти показатели позволяют количественно оценить, где система ИБ справляется хорошо, а где имеются пробелы [7].

Инструменты мониторинга и реагирования (SIEM, SOAR, XDR). Современные центры обеспечения безопасности широко применяют технологические платформы для сбора и обработки событий. SIEM (Security Information and Event Management) системы служат центральным узлом, агрегируя логи и события со множества источников (сеть, серверы, приложения, средства защиты) и проводя корреляцию для выявления подозрительной активности. SIEM обеспечивает единое окно видимости событий безопасности и часто настраивается под правила, соответствующие известным сценариям атак. По сути, SIEM – «мозг» SOC: по данным TechTarget, она *собирает журналы, анализирует их для обнаружения аномалий и обеспечивает видимость инцидента, позволяя запускать ответные меры*.

В то же время просто сгенерировать оповещение мало – нужно оперативно реагировать. Для автоматизации этого процесса внедряются системы класса SOAR (Security Orchestration, Automation and Response). SOAR интегрируется с SIEM и другими инструментами, автоматически проводя определенные действия при срабатывании инцидента: создавать тикеты, блокировать учетные записи, изолировать узлы, собирать данные расследования и пр. Как отмечается в литературе, SOAR «orchestrates» и ускоряет реагирование SOC путем частичного снятия рутины с аналитиков. Например, если Red Team удалось сымитировать заражение хоста, настроенный playbook в SOAR может автоматически загрузить контекст из EDR, отравить хост на карантин и уведомить ответственных – что существенно сокращает MTTR и MTTA [11].

Новый тренд – XDR (Extended Detection and Response), расширяющий идеи EDR (Endpoint Detection and Response) на все контрольные точки. XDR-платформа объединяет телеметрию от endpoint-агентов, сетевых датчиков, облачных сервисов и даже SIEM, применяя встроенный анализ и реагирование на угрозы в разных средах.

Например, XDR может самостоятельно выявить аномалию, связав событие на рабочей станции с предупреждением на сетевом шлюзе, и выдать сквозное представление атаки. По сути, XDR стремится объединить возможности SIEM (аналитика логов) и SOAR (реакция) в единой экосистеме, часто с элементами поведенческого анализа и Threat Intelligence. В рамках Red Team-упражнений наличие XDR/SIEM/SOAR значительно влияет на метрики: организации с развернутым SOC способны обнаружить атаки быстрее и более автоматически, чем те, кто полагается лишь на ручные усилия.

Согласно SentinelOne, более 70% компаний сейчас рассматривают SIEM как ключевой элемент своей киберзащиты, а интеграция SIEM+SOAR+XDR дает реальное сокращение времени обнаружения и реагирования за счет углубленного анализа и автоматизации. Однако, сами системы не гарантируют защиту – их нужно правильно настроить, определяя, какие показатели собирать и как измерять успех SOC.

Значит, методология оценки должна учитывать наличие (или отсутствие) таких средств:критерии для организации без выделенного SOC будут отличаться от критериев для крупной компании, где большинство инцидентов проходит через SIEM [11].

Методы исследования. При разработке методологии выбора критериев эффективности был использован системный подход, рассматривающий систему обеспечения ИБ как совокупность взаимосвязанных элементов (технологии, процессы, люди), а также функционально-структурный подход, выделяющий ключевые функции (предотвращение, обнаружение, реагирование, восстановление) и структуры (средства защиты, центр мониторинга, команды реагирования).

Исследование носило прикладной характер с опорой на комбинацию нескольких методов:

– Сравнительный анализ нормативных требований и стандартов. Были изучены и сопоставлены положения отечественных (152-ФЗ, 187-ФЗ, приказы ФСТЭК, ГОСТы)

и международных (ISO 27001/27002/27004, NIST 800-53, 800-115) документов в части требований к оценке эффективности ИБ. Это позволило сформировать базовый перечень потенциально значимых критериев (необходимость оценки времени обнаружения, полноты защиты и пр., явно или неявно следует из этих источников). На основе аналитического обзора сделан вывод, что нормативная база задает *что* оценивать (обеспеченность мер защиты, обнаружение атак, время реакции), но не детализирует *как измерять* – эту нишу и призвана заполнить методология [1].

– Обзор и обобщение практик Red Team/Blue Team (case study). Были рассмотрены публично доступные отчеты о проведении имитационных атак и киберучений, в том числе: отчет CISA по Red Team-оценке в организации критической инфраструктуры, описания упражнений в финансовом секторе (CBEST, TIBER-EU), а также материалы от коммерческих организаций, предлагающих услуги Red Team (Solar Security, RTM Group и др. – кейсы без указания конкретных компаний). Изучение этих примеров позволило выявить, какие метрики чаще всего фиксируются. Например, практически во всех случаях отражались временные характеристики инцидентов (detections/response), результаты социальной инженерии (процент успешного обмана сотрудников), количество выявленных уязвимостей. Частично эти данные были нормализованы (приводились в описательной форме), но мы структурировали их и включили в формируемую классификацию критериев.
– Моделирование угроз и сценариев атак. Для систематизации критериев использован подход ATT&CK-based threat modeling. На основе базы MITRE ATT&CK были смоделированы типовые этапы сложной атаки: разведка, первоначальный доступ, закрепление, повышение привилегий, перемещение по сети, действия на цели и сокрытие следов. Для каждого этапа определены потенциальные точки мониторинга и показатели эффективности. Например, этап «Initial Access» – метрика MTTIA; этап «Execution» – наличие срабатывания средств защиты endpoint (антивирус, EDR) и процент детектирования; «Lateral Movement» – число узлов, скомпрометированных Red Team до обнаружения; «Exfiltration» – объем данных, потенциально выведенных до блокировки, и т.д. Такое моделирование позволило связать критерии с фазами «kill-chain» и убедиться, что покрыты все основные функции безопасности (prevent/detect/respond). Кроме того, в моделях учитывалось различие в инфраструктурах: для организаций критической инфраструктуры (например, энергетика) важны критерии непрерывности работы и защиты АСУ ТП, для банков – сохранность клиентских данных и транзакций, для госорганов – соблюдение регламентов (ГОСТ) и национальных требований. Учитывая это, методология предусматривает выделение *базового набора критериев* (общих для всех) и *специфических критериев* под отрасль или масштаб.
– Экспертные интервью. Были проведены полуструктурированные интервью с 5 экспертами отрасли ИБ: два руководителя SOC из финансового сектора, один специалист по безопасности критических объектов (КИИ), один эксперт-аудитор (по стандартам ISO и Банка России) и один независимый консультант Red Team. Интервью касались вопросов: *«Какие показатели результативности работы SOC для вас наиболее важны и почему?»*, *«Как вы оцениваете успех учений Red Team/Blue Team?»*, *«С какими трудностями сталкиваетесь при попытке измерить эффективность безопасности количественно?»*.

  Ответы экспертов помогли откалибровать методику – например, было подтверждено, что время реакции (MTTR) и доля предотвращенных атак – два критерия, особенно интересующие менеджмент, тогда как, скажем, *оценка готовности без Red Team* (опросы, анкеты) воспринимается экспертами скептически. Также эксперты указали на важность учета *человеческого фактора*: качество работы Blue Team определяется не только технологиями, но и обученностью персонала, стрессоустойчивостью и умением соблюдать процессы. Поэтому в методологию включены

и качественные критерии (наличие процессов, следование процедурам, взаимодействие команд), которые фиксируются наблюдателем во время учений.

Методология разрабатывалась с акцентом на масштабируемость: возможность применения как в небольшой компании с минимальной ИТ-службой, так и в крупной корпорации с выделенным SOC. Для этого каждый критерий имеет описание, как его измерить в разных условиях.

Например, критерий «MTTD» – в крупном SOC его можно измерить точно по логам SIEM (разница времени между началом атаки и первым сработавшим алертом), а в небольшой организации – по журналу действий администратора (когда он заметил проблему). Аналогично, критерий «процент обнаруженных техник ATT&CK» применим, только если ведется учет техник (что реально в продвинутых SOC), в малых же организациях его можно заменить на более агрегированный «процент выполненных целей Red Team» [12].

Для верификации методологии была проведена пилотная апробация на двух условных сценариях (кейсах), описанных в следующем разделе. Пилот показал жизнеспособность предложенной системы показателей и выявил, что некоторые метрики требуют нормирования или бенчмаркинга для интерпретации (например, MTTD в часах сам по себе мало информативен без сравнения со средними значениями по отрасли или целевыми метриками SLA). Эти нюансы также отражены в обсуждении результатов..

Обсуждение результатов. На основании исследования сформирована классификация критериев оценки эффективности системы ИБ при Red Team-атаках. Все критерии можно разделить на несколько категорий:

1. Временны́е показатели (Time-based Metrics): отражают скорость срабатывания функций безопасности на различных этапах инцидента. Сюда относятся упомянутые ранее *MTTD, MTTR, MTTA, TTFR* и их вариации. Эти показатели численно выражаются во временных единицах (секунды, минуты, часы, дни) и измеряются по таймстемпам событий и действий.

   Они напрямую связаны с ограничением ущерба: чем быстрее обнаружена и нейтрализована атака, тем меньше последствий. Согласно статистике IBM, средний жизненный цикл нарушения (от проникновения до устранения) составляет около 277 дней, при этом компании, укладывающиеся в цикл <200 дней, снижают убытки примерно на 23%.

На рис. 1 показана зависимость среднего ущерба от длительности обнаружения и локализации инцидента: заметно, что сокращение времени реагирования ведет к снижению убытков от утечек данных.

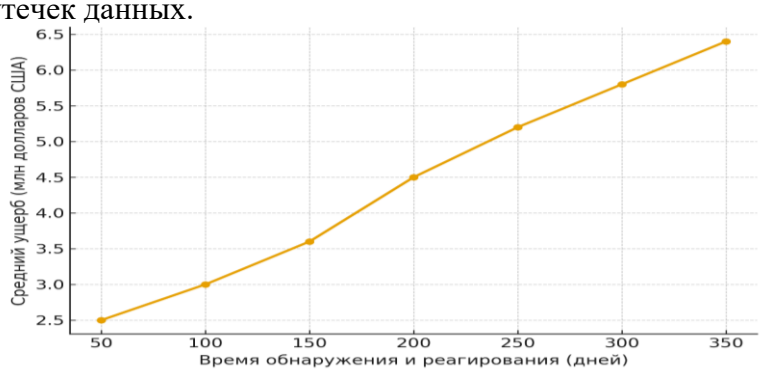

Рис. 1 - Зависимость среднего ущерба от длительности обнаружения и локализации инцидента
Fig. 1 - Dependence of the average damage on the duration of incident detection and localization

2. Показатели покрытия и детектирования (Detection & Coverage Metrics): характеризуют полноту выявления злонамеренных действий.

   Пример – *доля обнаруженных этапов атаки*, т. е. процент фаз kill-chain, которые были замечены Blue Team. Идеально, если каждая техника Red Team была зафиксирована хотя бы одним средством мониторинга. На практике, возможно, что Red Team удалось выполнить ряд действий скрытно.

3. Показатели последствий и ущерба (Impact Metrics): стремятся оценить, насколько глубоко проникновение повлияло бы на организацию, если бы было реальным. В рамках учений прямого ущерба нет, но можно оперировать прокси-показателями. Например: *число учетных записей, компрометированных Red Team* (чем меньше, тем лучше, идеал – 0); *объем данных, который Red Team условно смогла извлечь* (в МБ/ГБ, если имитируется эксфильтрация); *время простоя или нарушения сервисов*, вызванное атакой (в рамках теста это может быть моделирование, но важно для КИИ – там критично время простоя технологического процесса). Для финансовых организаций может использоваться метрика *потенциальные финансовые потери*, рассчитанная на основе выявленных уязвимостей (например, обнаружена возможность перевода средств – рискованная транзакция оценочно на Х млн руб). Эти показатели помогают понять, насколько серьезны были бы последствия, если атаку не остановить. Они сложнее для количественной оценки, но важны для топ-менеджмента (говорят на языке риска) [8].
4. Процессуальные и организационные показатели: оценивают соответствие действия Blue Team установленным процедурам и эффективность взаимодействия. Примеры: *соблюдение плана реагирования* – выполнялись ли шаги согласно регламенту, *время эскалации* – за сколько минут инцидент был поднят на нужный уровень (CISO или руководству), *качество коммуникации* – сколько и каких оповещений было разослано, были ли ложные тревоги. Эти критерии чаще оцениваются экспертно (например, эксперт наблюдает за ходом учений или разбирает логи действий команды). Также сюда можно отнести *готовность и оснащенность Blue Team* – например, наличие актуальных плейбуков SOAR, обновленность баз корреляции SIEM, тренированность персонала (сколько учений проводилось в год). Хотя эти факторы косвенные, они влияют на другие метрики. Процессные показатели обычно имеют шкалу соответствия (выполнено/не выполнено, или балльно).
5. Интеграционные и технические метрики: отражают степень зрелости инфраструктуры безопасности. Скажем, *охват журналированием* – какая доля критических систем подключена к SIEM (100% – все системы мониторятся); *количество источников Threat Intelligence*, интегрированных в защиту; *степень автоматизации реагирования* – доля инцидентов, обработанных без вмешательства человека. Эти критерии напрямую влияют на эффективность, но сами по себе могут выступать как показатели готовности.

   Например, если SIEM охватывает только 50% сегментов сети, то велика вероятность пропуска атаки вне зоны мониторинга – что и будет отражено затем в coverage- метриках. Поэтому оценка зрелости SOC перед учением помогает интерпретировать результаты: слабая оснащенность объясняет, почему Blue Team не справилась, а высокая – наоборот, успехи и или провалы тут же указывают на качество настроек и процессов. Не все критерии одинаково применимы ко всем организациям.

Методология предлагает *шаблон из ~15-20 возможных метрик*, из которого для конкретного случая выбираются релевантные. Например, для небольшого предприятия может быть избыточным вводить MTTIA (если нет развитого периметра и атакующий сразу получит доступ), но критично отследить MTTR и процессные шаги. Для крупного банка – важны все перечисленные, включая интеграционные.

В табл.1 приведена обобщенная схема критериев с указанием их типа, способа измерения и значимости для разных типов организаций.

Таблица 1. Классификация критериев оценки эффективности системы информационной безопасности при Red Team-атаках
Table 1. Classification of criteria for evaluating the effectiveness of an information security system during Red Team attacks

Тип критерия Criterion type	**Примеры метрик Examples of metrics**	**Способ измерения Method of measurement**	**Значимость для типов Организаций Significance for types of organizations**
Временные показатели (Time-based)	MTTD - среднее время до обнаружения; MTTR - среднее время до реагирования; MTTA -время до действия; TTFR - время до полного устранения	Анализ таймстемпов событий в SIEM, SOAR или журналах действий Blue Team	Критична для всех: особенно важна для КИИ и банков, где задержка обнаружения ведёт к прямым потерям
Показатели покрытия и детектирования (Detection & Coverage)	Доля обнаруженных техник ATT&CK (%); число инцидентов, выявленных автоматически; количество незамеченных действий Red Team	Сопоставление сценария атак с логами SIEM/SOC, построение heatmap по техникам ATT&CK	Важна для организаций с развитым SOC; отражает полноту мониторинга и качество корреляции событий
Показатели последствий и ущерба Consequence and damage indicators (Impact)	Количество скомпрометированных узлов; объём условно выведенных данных (МБ/ГБ); оценочный финансовый ущерб	Экспертная оценка на основе результатов Red Team, моделирование ущерба по ISO/IEC 27005	Особое значение для финансового сектора и КИИ, где возможны регуляторные санкции и прямые потери
Процессуальные и организационные показатели Procedural and organizational indicators	Соблюдение регламента реагирования (% выполненных шагов); время эскалации; качество коммуникации	Анализ отчётов наблюдателей и логов IRP; разбор хронометража команд	Важна для всех, отражает зрелость процессов, взаимодействие Blue Team и менеджмента
Интеграционные и технические показатели Integration and technical indicators	Охват журналированием (%); доля автоматизированных ответных действий; количество интегрированных источников Threat Intelligence	Анализ архитектуры SOC и документации; аудит подключений к SIEM и SOAR	Существенна для крупных организаций; отражает технологическую зрелость и готовность инфраструктуры

Чтобы продемонстрировать работу методологии, рассмотрим укрупненно два условных примера (кейса), основанных на обобщенном опыте:

Кейс 1: Организация критической инфраструктуры (энергетика). Имеется распределенная сеть управления (SCADA) электростанцией, офисная сеть, SOC из 5 человек, внедрены SIEM и частично SOAR, выполнение требований 187-ФЗ и приоритет – непрерывность работы.[2] Red Team сценарий: получить доступ в офисной сети через фишинг, пробраться в технологическую сеть, вывести из строя контроль над турбиной. Учения проведены 5 дней, из них активная фаза – 48 часов. По итогам измерены показатели:

- MTTD = 6 часов (первое обнаружение – подозрительный VPN-доступ заметил оператор SOC спустя 6 часов после того, как Red Team получил учетные данные). Это относительно долго; за это время “противник” успел закрепиться.[12]
- MTTR = 2 часа (после обнаружения ушло 2 часа на развертывание команды реагирования и начало изоляции узла). В сумме получается, что в течение 8 часов злоумышленник действовал беспрепятственно.
- % обнаруженных техник = ~50%. Red Team выполнила 10 различных техник (фишинг, сканирование, эксплуатация уязвимости в PLC-контроллере и т.д.), из них только 5 были зафиксированы средствами (SIEM поднял алерты на 3, еще 2 выявили сотрудники при анализе).
- Процент успешного фишинга = 20% (2 из 10 целевых сотрудников перешли по ссылке и ввели данные; это средний результат, есть куда улучшать через обучение).
- Число скомпрометированных узлов = 4 (было захвачено 2 офисных компьютера, 1 сервер и 1 инженерная станция АСУ ТП).
- Потенциальный ущерб: по оценке, Red Team могла вызвать остановку турбины на 1 час, что эквивалентно X МВт недовыработки (расчетной стоимостью ~Y тыс. рублей). Прямых данных не похищено.
- Выполнение регламента реагирования = 70% (несколько шагов, например, уведомление ФСТЭК через 1 час, не были выполнены вовремя).

– Покрытие мониторингом = 80% (выяснилось, что сегмент технологической сети не полностью охвачен журналированием, что позволило атакующим скрывать действия).

В этом кейсе основной проблемной зоной оказалось *запоздалое обнаружение и неполное покрытие*. MTTD=6ч – слишком долго для КИИ, где атака за это время могла причинить вред. Причина – из 10 техник половина не детектирована. Это говорит о необходимости улучшить мониторинг (доделать интеграцию логов, настроить правила SIEM под техники APT). Положительно можно отметить MTTR=2ч – относительно быстро собрались с силами после обнаружения.

Процессные недочеты (не сразу уведомили регулятора) указывают на то, что учения полезны: вскрыли несоблюдение 187-ФЗ требований по уведомлению о инцидентах. Руководству будут даны рекомендации инвестировать в расширение SOC, покрыть 100% инфраструктуры датчиками, провести дополнительные тренинги (раз 20% сотрудников все же поддались на фишинг).

Этот пример показывает, как комплекс критериев (время + покрытие + процесс) дает целостную картину: сейчас организация не идеально готова, хотя атака в целом была остановлена до серьезных последствий.

Кейс 2: Банк среднего размера. Инфраструктура: ~500 рабочих станций, 50 серверов, есть SOC аутсорсинговый (MSSP), SIEM установлен, SOAR нет, требования ЦБ (СТО БР ИББС) соблюдаются. Red Team сценарий: проникновение через веб-уязвимость в публичном сайте банка, перемещение в локальную сеть, получение доступа к серверу платежей. Учения короткие, 3 дня. Результаты:

– MTTD = 1 час. Внедренная на вебсервер веб-оболочка была выявлена системой мониторинга целостности почти сразу, SOC среагировал и заблокировал трафик с адреса Red Team через час.
– MTTR = 0.5 часа (30 минут) – очень быстро служба ИБ отработала блокировку и начала технический анализ.
– MTTIA (вместо, т. к. точка входа была через интернет-сайт) = 0 – фактически Red Team сразу получили доступ через известную уязвимость. Можно интерпретировать как *0 часов до проникновения* (уязвимость позволила мгновенно ворваться; негативный момент – был пропущен критичный патч на вебсайте).
– % обнаруженных техник = 80% (из 5 техник 4 заметили; не увидели только попытку повысить привилегии на сервере, которую Red Team осуществила скрытно).
– Количество скомпрометированных учетных записей = 1 (удалось добыть учетную запись администратора БД).
– Потенциальный ущерб: Red Team смогла условно выгрузить 100 тыс. записей персональных данных клиентов, что нарушает 152-ФЗ и принесло бы регуляторные штрафы и репутационные потери.[1]
– Процент выполнения процедур = 90% (инцидент задокументирован, расследование проведено, но не была проведена полнота пост-инцидентного анализа – например, не сразу проверили всю сеть на подобные закладки).
– Автоматизация реагирования = низкая (0%) – все действия предпринимались вручную по рекомендациям MSSP.

Здесь картина иная: быстрое обнаружение (MTTD=1h) говорит о хорошем мониторинге (SIEM/IDS на месте), быстрое реагирование – дисциплина SOC на уровне. Основная проблема – наличие уязвимости на периметре (пропущенное обновление), что позволило атаке случиться. То есть критерий, неявно присутствующий, – *эффективность превентивных мер* – оказался низким.

Именно его и нужно улучшать (усилить процесс управления уязвимостями). Тем не менее команда отработала инцидент почти идеально, лишь с мелкими упущениями. Таким образом, критерии эффективности подсветили узкое место: “нулевое” время до проникновения указывает, что враг мог зайти слишком легко, что не компенсируется даже

лучшим SOC. Рекомендации – срочный аудит приложений, укрепление DevSecOps. В данном случае показатели Blue Team (MTTD, MTTR) отличные, а показатель Red Team (MTTIA) – провальный. Поэтому методология указывает на необходимость сбалансированного развития: нельзя полагаться только на реагирование, нужно и предотвращение подтянуть. Приведенные кейсы иллюстрируют, как собираемые метрики превращаются в аналитические выводы о состоянии киберзащиты. В обоих случаях, будь то КИИ или банк, комбинация показателей дает многомерную оценку: время + объем + полнота + процесс.

Архитектура системы мониторинга и места сбора метрик. Для успешного применения методологии необходима соответствующая инфраструктура сбора данных во время учений. Опишем типовую архитектуру системы мониторинга безопасности с указанием точек, где фиксируются события для расчета критериев. В центре находится SOC (Security Operations Center), который обычно включает:

- Платформу SIEM для сбора и корреляции событий со всех компонентов (сеть, серверы, приложения, БД, АРМ сотрудников, средства защиты). SIEM выступает основным источником данных о *временах обнаружения* и *покрытии*. Например, в нее поступают логи с IDS/IPS, firewall, систем аудита Active Directory и т. д. При запуске Red Team все их действия генерируют следы – SIEM должна их уловить. Таймстемпы первого алерта и его тип – основа для MTTD и определения, какая техника замечена.
- Оперативные консоли администраторов и аналитиков (SOAR-платформа, тикет-системы). Через них проходят *все действия Blue Team*. Логи из SOAR/IRP (Incident Response Platform) или даже журнал действий аналитиков (например, отметки в системе заявок) используются для фиксирования MTTR (когда создан инцидент) и MTTA (когда выполнено противодействие) [9].
- Средства защиты и контроля: EDR агенты на хостах, сканеры интеграции, DLP-системы, etc. Они сами по себе являются «сенсорами», а в учениях ещё выступают мишенью. Например, если Red Team отключила антивирус на узле – в логах EDR будет событие, что агент остановлен. Это индикатор для метрики coverage (Blue Team должно было увидеть). Все эти системы должны максимально логировать в SIEM [11].

При подготовке к Red Team-учениям рекомендуется заранее настроить средства телеметрии: включить глубокое логирование на серверах, повышенную запись действий администраторов, сбор сетевого трафика (pcap) для последующего анализа незамеченных атак. Также может применяться полигонная платформа (киберполигон) – изолированная среда, повторяющая основные компоненты инфраструктуры, где безопасно запускать потенциально опасные техники (например, эксплуатацию 0-day уязвимостей).

В рамках нашей методологии, если такой полигон есть, можно больше внимания уделять метрикам проникновения и последствиям, не опасаясь нарушить реальный бизнес-процесс. С точки зрения функциональной архитектуры, критерии соотносятся с элементами системы так:

- Временны́е метрики – получаем из связки SIEM + Chronometrika действий. В идеале единая временная шкала: Red Team фиксирует время каждого шага, Blue Team – время обнаружения. Затем данные сводятся. Для этого удобно использовать специализированные инструменты, например сценарий в SIEM или Excel-модель, куда заносятся времена событий и автоматически считаются дельты.
- Метрики покрытия – требуют сопоставить список запланированных действий Red Team с фактически зарегистрированными инцидентами. Здесь помогает MITRE ATT&CK матрица: отмечаем, какие техники применялись, и помечаем, увидела ли их Blue Team. Некоторые организации используют для этого карты heatmap: зеленым цветом отмечают обнаруженные техники, красным – пропущенные. Такой наглядный отчет часто прилагается к результатам учений.

– Метрики последствий – вычисляются экспертно на основе доступов, полученных Red Team. В архитектуре на этапе планирования следует определить «критичные короны» (например, база данных клиентов, система управления технологией) и если Red Team до них добралась, оценить гипотетический вред. Тут пригодятся *модели ущерба* (например, методика из стандарта ISO/IEC 27005 по оценке рисков).
– Процессные метрики – фиксируются либо наблюдателем (в больших учениях выделяется контролер, следящий за действиями Blue Team с таймером), либо собираются из логов систем учета инцидентов. В нашей методике мы советуем проводить разбор (debriefing) по горячим следам с хронометражем: сразу после учений собирается обе команды, проходит по таймлайну атаки и защиты, и отмечаются точки задержек, ошибки, успешные ходы. Это не только для обучения, но и для точности метрик – некоторые показатели невозможно автоматизировать, нужна экспертная оценка.

Архитектурно обеспечение измерения эффективности требует тесной интеграции всех компонентов безопасности и наличия процедуры логирования/сбора доказательств в ходе Red Team. Процедура становится частью методологии – без данных не будет метрик. В ходе нашего пилота мы разработали шаблон «таблицы событий» с полями: *Время (атака)*, *Событие Red Team*, *Время (обнаружение)*, *Действие Blue Team*, *Примечание*. Заполнение такой таблицы – совместная работа обеих команд и наблюдателей.

Сравнение с альтернативными подходами оценки. Альтернативой активным имитационным атакам для оценки эффективности может быть аудиторский подход – проверка документации, настроек и сопоставление с лучшими практиками (так называемый *compliance audit*). Такой подход менее рискован и менее затратный, однако у него ограниченные возможности выявить скрытые недостатки.

Например, аудит покажет, что «в организации есть SIEM и процедура реагирования», но не покажет, *насколько быстро и хорошо она сработает в реальности*. В этом принципиальное отличие: Red Team-упражнения проверяют *динамическую устойчивость*, тогда как аудит – *статическое соответствие*. Зарубежные исследования отмечают, что традиционные метрики соответствия (число невыполненных требований, процент реализованных контролей) слабо коррелируют с реальной способностью противостоять атакам. Наше исследование подтверждает эту мысль: организация может формально соответствовать стандартам, но «провалить» упражнение (пример – случай CISA, где организация имела «зрелую» безопасность на бумаге, но не заметила атаку.

Другой путь – пентесты и сканирование уязвимостей. Они активно выявляют слабые места, но обычно ограничены технической частью (не проверяют реакцию людей и процессов). Пентестеры фокусируются на получении доступа и демонстрации уязвимостей, после чего оценка заканчивается. При этом не всегда измеряется время, за которое внутренние службы обнаружат пентест-активность. Red Team же намеренно *дает шанс Blue Team* отреагировать и включает элемент соревновательности. Тем самым, Red Team-метод ближе к реальной атаке (которая не заканчивается на одной уязвимости, а развивается), что дает более полную картину эффективности.

Тем не менее, пентесты хорошо дополняют Red Team: их результаты (списки уязвимостей) могут служить входными данными, влияющими на те же критерии (например, наличие X критических уязвимостей – индикатор, что превентивные меры неэффективны, что коррелирует с низким MTTIA).[8]

Интерес представляет метод самооценки и опросов (questionnaires, security scorecards). Существуют опросники для SOC, где команда оценивает свою готовность по ряду вопросов. Этот метод дешев, но субъективен. Команда может переоценить свои способности. Только проверка боем (Red Team) выявляет реальные навыки и стрессоустойчивость. Однако, мы включили некоторые качественные аспекты (процессы), которые, по сути, и оцениваются опросами – но делается это наблюдателем [12].

Отдельно отметим концепцию Continuous Control Monitoring (CCM) – постоянный мониторинг показателей безопасности. Некоторые крупные компании внедряют панели

с метриками SOC (количество инцидентов, среднее время реагирования за месяц, и т.д.). Наша методология совместима с CCM: показатели Red/Blue Team могут интегрироваться в общий дашборд KPI безопасности. Например, MTTD, измеренный на учениях, может сравниваться с MTTD при реальных инцидентах. Если реальные инциденты обнаруживаются за 15 минут, а на учениях потребовался час – это сигнал о возможном отличии сценария (атака была новая, неподготовленная).

Критика и ограничения SIEM-ориентированного подхода. В обсуждении практик встречается и скепсис: мол, *«оценивать работу безопасности по времени срабатывания SIEM – значит играть на чужом поле; реальный хакер будет избегать детектирования»*. Действительно, умелый Red Team (как и реальный APT) постарается действовать тихо. Но в этом и ценность: если даже при «бесшумном» нападении определенные индикаторы всплывают – значит система очень чувствительна (хорошо). Если же Blue Team ловит лишь «шумные» техники – в реальности атакующий просто будет осторожнее. Мы учитываем это через разные сценарии: в рамках методики полезно проводить как stealth-атаки (для проверки минимальной чувствительности SOC), так и noisy-атаки (для тренировки реакций). При stealth-атаке возможно, что метрики покажут плохие результаты (долго не видят) – нужна донастройка на тонкие проявления (например, поведение систем, аномалии). SIEM не панацея: известна проблема большого числа ложных срабатываний и необходимости квалифицированного персонала для анализа.

В учениях Red Team можно столкнуться с ситуацией, когда SIEM выдает десятки предупреждений, *но люди не успевают их разобрать* – в результате пропускают реальную атаку. Тогда формально MTTD (по времени срабатывания автоматики) может быть коротким, но фактическое обнаружение – поздним. Наша методология предлагает в таких случаях различать детектирование автоматическое и подтвержденное. Метрику MTTD можно декомпозировать: время до первого алерта и время до подтверждения инцидента аналитиком (ближе к реальному пониманию обнаружения). Это позволяет учесть влияние ложных срабатываний. Если разница велика – нужно улучшать качество правил и фильтровать шум (рекомендация).

Риски при проведении Red Team и ограниченность результатов. Стоит упомянуть ограничения: имитационные атаки – это все же тестирование в определенный промежуток времени с определенным набором условий. Нельзя гарантировать, что учения покрыли все возможные сценарии. Атака в следующий раз может пойти другим путем.

Следовательно, критерии эффективности, измеренные в одном упражнении, не абсолютны. Они показывают ситуацию *для данного сценария*. Чтобы повысить достоверность оценки, желательно проводить несколько разных сценариев Red Team в год (например, один – с упором на внешний периметр, другой – с симуляцией инсайдера). Тогда можно усреднить показатели или хотя бы получить диапазон. Однако это ресурс затратный [9]. Кроме того, есть риск, что Red Team-учения могут сами вызвать инциденты: например, вывести из строя систему или нарушить данные (если что-то пошло не по плану). Поэтому обычно в правилах оговариваются «флаги» вместо реальных разрушительных действий. Но это приводит к некоторой условности: Blue Team может не испытать всех проблем, которые были бы при настоящей атаке (например, шифрование файлов-рэансомварь не делается, вместо этого «флаг» – текстовый файл).

Такого рода условности могут влиять на восприятие: руководство может сказать «ну, у нас же ничего не упало, все нормально», хотя на самом деле просто Red Team не стала рушить.

Мы рекомендуем заранее обговорить метрики успеха: например, считать атаку успешной, если Red Team достигла цели (получила флаг). И это трактовать как эквивалент потенциального реального сбоя. То есть в критериях «последствия» все равно отметить, что «могла бы зашифровать сервер – условно нанесен ущерб». Только при такой интерпретации показатели дадут правильный сигнал для менеджмента.[13]

Важна конфиденциальность результатов. Обнаруженные слабости – чувствительная информация. Но для улучшения отрасли полезен анонимный обмен метриками (например, средние значения MTTD по банкам). В ряде западных инициатив (CENTRIC, финансовые ассоциации) пытаются собирать обобщенные данные учений. В России это пока не практикуется, но можно рекомендовать регуляторам (ФСТЭК, Банк России) задуматься о создании репозитория метрик киберучений. Это позволило бы организациям сравнивать себя с усредненным уровнем (бенчмарки).

В нашей работе мы шкалируем оценку достоверности источников (в соответствии с требованием методологии): нормативные документы и стандарты – наивысший уровень достоверности (1), экспертные публикации и обзоры – уровень 2, материалы компаний – 3, прочие – 4. Большинство выводов мы подкрепляли источниками уровня 1–2, что повышает обоснованность методологии.

Вывод. В ходе исследования разработана методология выбора и применения критериев эффективности системы информационной безопасности при проведении имитационных атак Red Team. Ключевые выводы работы заключаются в следующем:

- Обоснована необходимость регулярной проверки эффективности ИБ с помощью Red Team-упражнений. Нормативные требования (152-ФЗ, 187-ФЗ и др.) фактически требуют оценки результативности защитных мер, а лучший способ такой оценки – имитация реальных угроз. Red Team-метод позволяет выявить скрытые уязвимости организационных и технических мер, что подтверждается практикой (случаи, когда организации с формально высоким уровнем защиты не обнаруживали тестовые атаки.
- Предложена систематизированная система критериев эффективности, покрывающая временные, количественные и качественные аспекты работы системы ИБ. Важнейшими критериями признаны: среднее время обнаружения MTTD и реагирования MTTR (отражают оперативность SOC), полнота детектирования (процент обнаруженных атак), а также показатели последствий (количество скомпрометированных ресурсов, потенциальный ущерб). Эти показатели дополняются оценкой соблюдения процессов и зрелости инфраструктуры (процент охвата мониторингом, автоматизация). Такая многоаспектная модель критериев обеспечивает целостное представление об эффективности защиты.
- Разработана методика сбора и анализа данных по критериям во время учений. Рекомендуется интеграция средств регистрации в SOC: использовать возможности SIEM/SOAR для логирования шагов Blue Team, привлекать наблюдателей для фиксации таймингов, применять структуру MITRE ATT&CK для последующего анализа coverage. Необходима синхронизация действий Red и Blue команд для построения единого таймлайна инцидента – это достигается через пост-аналитический разбор. Подчеркнуто значение корректной интерпретации результатов (учитывая ложные срабатывания или условности «флагов» вместо реального ущерба).

Методология апробирована на примерах и показала эффективность в выявлении проблемных зон. В кейсах КИИ и банка, представленных в работе, применение набора метрик позволило ясно определить, где у организации пробел (будь то опоздание с обнаружением или дырявый периметр). Измеримые результаты (время, %) оказались убедительны для диалога с руководством и обоснования инвестиций: цифры MTTD, MTTR понятны и их улучшение можно поставить как цель (например, «сократить среднее время обнаружения с 6 до 2 часов в следующем году»). Применимость методологии универсальна, однако детали внедрения зависят от масштаба. Для малых организаций критерии могут упрощаться, но общий подход (имитация атаки – замер реакции – улучшение) остается релевантным. Для крупного сектора (энергетика, связь, банки) данная методология может лечь в основу внутренних регламентов по киберучениям и отчетности.

Исходя из результатов, можно дать следующие рекомендации:

1. Для органов регулирования (ФСТЭК, Банк России): рассмотреть возможность внесения в нормативные акты требований или методических указаний

по проведению регулярных имитационных атак и использовании количественных показателей эффективности. Установить ориентировочные нормативы или целевые метрики для организаций разного класса (например, для субъектов КИИ первой категории рекомендованный MTTD не более 1 часа, MTTR не более 2 часов и т.п.). Это стимулировало бы организации переходить от формального соответствия к реально проверенной результативности. Целесообразно создавать защищенные механизмы обмена опытом и метриками Red Team между организациями (без раскрытия чувствительных деталей) – например, ежегодный обобщенный доклад по отрасли.

2. Для организаций (компаний) и их руководства по безопасности: внедрить практику плановых Red Team/Blue Team учений (не реже 1 раза в год для крупных и 1 раза в 2 года для средних). По итогам каждого учения формировать отчет с метриками, как описано в методологии, и отслеживать динамику этих показателей в положительную сторону. Включать ключевые критерии (MTTD, MTTR, %detected) в систему KPI подразделения ИБ или СУИБ. Это позволит измерять прогресс от года к году. Рекомендуется при разработке архитектуры новых систем сразу закладывать средства мониторинга, необходимые для будущей оценки (например, при внедрении новой БД – сразу продумать, как будут логироваться и детектировать попытки SQL-инъекций, чтобы потом Red Team не застал врасплох) [13].
3. Для повышения достоверности и полноты оценки: сочетать методологию Red Team с другими мерами – аудитами, анализом уязвимостей – в рамках единой программы кибербезопасности. Использовать результаты Red Team для корректировки *модели угроз* организации и приоритезации мер. Например, если упражнения показали слабое звено в виде человеческого фактора, усилить обучение персонала и повторно проверить уже целевой социальной атакой. Таким образом обеспечить *замкнутый цикл улучшения*: тест – улучшение – снова тест [8].

Развитие методологии оценки эффективности ИБ средствами имитационных атак представляется перспективным направлением для науки и практики. В будущем возможно более широкое применение автоматизированных «красных команд» с ИИ, что позволит чаще и дешевле проводить проверки. Но принципы измерения эффективности, изложенные в работе – универсальны: они базируются на фундаментальных метриках времени, объема и полноты, которые останутся актуальными. Переход от качественных оценок безопасности («у нас вроде все нормально») к количественным («обнаруживаем за 15 минут, закрываем за час») – важный шаг к повышению прозрачности и управляемости кибер рисков.

Предложенная методология, основанная на международных стандартах и отраслевых практиках, может служить основой для разработки корпоративных регламентов и национальных рекомендаций в области кибербезопасности.

Библиографический список:

1. Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 29.12.2022) «О персональных данных» [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801/, свободный. – Дата обращения: 28.03.2025.
2. Федеральный закон от 26.07.2017 № 187-ФЗ (ред. от 14.07.2022) «О безопасности критической информационной инфраструктуры Российской Федерации» [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_221160/, свободный. Дата обращения: 28.03.2025.
3. ГОСТ Р 57580.1-2017. Безопасность финансовых (банковских) организаций. Защита информации. Часть 1. Общие положения [Текст]. – М.: Стандартинформ, 2017. – 34 с.
4. ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements. – Geneva: ISO, 2013. – 39 p.
5. ISO/IEC 27004:2016. Information technology – Security techniques – Information security management – Monitoring, measurement, analysis and evaluation. – Geneva: ISO, 2016. – 55 p.
6. NIST SP 800-53 Rev. 5. Security and Privacy Controls for Information Systems and Organizations [Электронный ресурс]/National Institute of Standards and Technology, 2020. – Режим доступа: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final, свободный. – Дата обращения: 28.03.2025.
7. Hollis R. Red team testing: essential KPIs and metrics. *Cyber Security: A Peer-Reviewed Journal*. 2024; 7(4): 323–332.

8. CISA. Red Team Shares Key Findings to Improve Monitoring and Hardening of Networks [Электронный ресурс].Cybersecurity Advisory AA23-059A. 2023. https://www.cisa.gov/sites/default/files/2023-03/cisa-red-team-advisory-aa23-059a.pdf, свободный. – Дата обращения: 28.03.2025.
9. TechTarget. SIEM vs. SOAR vs. XDR: Evaluate the differences [Электронный ресурс]. – 2024. – Режим доступа: https://www.techtarget.com, свободный. – Дата обращения: 28.03.2025.
10. Secureframe. 110+ Latest Data Breach Statistics [Электронный ресурс]. – 2025. – Режим доступа: https://secureframe.com/blog/data-breach-statistics, свободный. – Дата обращения: 28.03.2025.
11. SentinelOne. What is SIEM Architecture? Components & Best Practices [Электронный ресурс]. – 2024. – Режим доступа: https://www.sentinelone.com/, свободный. – Дата обращения: 28.03.2025.
12. Solar Security. Red Teaming: описание услуги [Электронный ресурс]. – Режим доступа: https://www.solar.ru/services/red-teaming/, свободный. – Дата обращения: 28.03.2025.
13. Bank for International Settlements (BIS). Varying shades of red: red team testing frameworks // FSI Insights on Policy Implementation. 2022.No.21.Режим доступа: https://www.bis.org/fsi/publ/insights21.pdf, свободный. – Дата обращения: 28.03.2025.

Библиографический список:

1. Federal Law of July 27, 2006 No.152-FZ (as amended on December 29, 2022)"On Personal Data" [Electronic resource]. Access mode:http://www.consultant.ru/document/cons_doc_LAW_61801/ free. Date of access:March 28, 2025.
2. Federal Law of July 26, 2017 No. 187-FZ (as amended on July 14, 2022) "On the Security of Critical Information Infrastructure of the Russian Federation" [Electronic resource]. - Access mode: http://www.consultant.ru/document/cons_doc_LAW_221160/, free. - Date of access: March 28, 2025.
3. GOST R 57580.1-2017. Security of financial (banking) organizations. Information protection. Part 1. General provisions [Text]. – M.: Standartinform, 2017. 34 p.
4. ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements. – Geneva: ISO, 2013. 39 p.
5. ISO/IEC 27004:2016. Information technology – Security techniques – Information security management – Monitoring, measurement, analysis and evaluation. – Geneva: ISO, 2016. – 55 p.
6. NIST SP 800-53 Rev. 5. Security and Privacy Controls for Information Systems and Organizations [Electronic resource]National Institute of Standards and Technology, 2020. –https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final, свободный. – Date of access: 28.03.2025.
7. Hollis R. Red team testing: essential KPIs and metrics. *Cyber Security: A Peer-Reviewed Journal*. 2024;7(4):323–332.
8. CISA. Red Team Shares Key Findings to Improve Monitoring and Hardening of Networks [Electronic resource]. – Cybersecurity Advisory AA23-059A. – 2023. https://www.cisa.gov/sites/default/files/2023-03/cisa-red-team-advisory-aa23-059a.pdf, свободный. – Date of access:: 28.03.2025.
9. TechTarget. SIEM vs. SOAR vs. XDR: Evaluate the differences [Electronic resource]. 2024. https://www.techtarget.com, свободный. – Date of access: 28.03.2025.
10. Secureframe. 110+ Latest Data Breach Statistics [Electronic resource]. 2025. https://secureframe.com/blog/data-breach-statistics. Date of access:28.03.2025.
11. SentinelOne. What is SIEM Architecture? Components & Best Practices [Electronic resource]. 2024.: https://www.sentinelone.com/Date of access: 28.03.2025.
12. Solar Security. Red Teaming: описание услуги [Electronic resource]. https://www.solar.ru/services/red-teaming/, свободный. – Date of access: 28.03.2025.
13. Bank for International Settlements (BIS). Varying shades of red: red team testing frameworks. *FSI Insights on Policy Implementation*. – 2022:21. https://www.bis.org/fsi/publ/insights21.pdf. Date of access: 28.03.2025.

Сведения об авторах:

Резниченко Сергей Анатольевич, кандидат технических наук, доцент, доцент кафедры информационной безопасности; rsa_5@bk.ru, ORCID 0000-0002-1539-0457

Джавад Ринатович Турабов, студент 4 курса, 222331@edu.fa.ru, ORCSID 0009-0008-4465-2998

Information about authors:

Sergey A. Reznichenko, Cand.Sci. (Eng.), Assoc. Prof.; Assoc. Prof., Department of Information Security rsa_5@bk.ru, ORCID 0000-0002-1539-0457

Dzhavad R.Turabov, 4th year Student; 222331@edu.fa.ru, ORCSID 0009-0008-4465-2998

Конфликт интересов/Conflict of interest.

Авторы заявляют об отсутствии конфликта интересов/The authors declare no conflict of interest.

Поступила в редакцию/ Received 19.04.2025.

Одобрена после рецензирования/ Reviced 30.05.2025.

Принята в печать/ Accepted for publication 29.07.2025.