

ПРИЛОЖЕНИЕ НА МЕТОДОЛОГИЯТА PURPLE TEAM ЗА ОЦЕНЯВАНЕ НА КИБЕРУСТОЙЧИВОСТТА НА ИНДУСТРИАЛНИ КОНТРОЛНИ СИСТЕМИ

гл. ас. д-р Димитър Иванов Николов

Висше военноморско училище „Н. Й. Вапцаров“ – Варна

E-mail: d.nikolov@naval-acad.bg

Резюме: *Настоящата статия изследва приложението на методологията Purple Team при оценяване и усъвършенстване на защитните способности на индустриалните системи за управление, с акцент върху електроенергийната инфраструктура. Разгледани са особеностите на взаимодействието между Red Team и Blue Team, ограниченията при симулиране на кибератаки в оперативни технологии и необходимостта от съчетаване на мрежова, системна и технологична телеметрия. Предложен е методологичен модел за организиране на Purple Team упражнения, основан на определяне на защитни цели, избор на релевантни техники, събиране на доказателства, анализ на резултатите и повторна проверка. Формулирани са показатели за оценяване на откриваемостта, диагностиката, реагирането и технологичната безопасност. Изследването има аналитичен и методологичен характер, като предложените показатели подлежат на последващо експериментално валидиране.*

Ключови думи: *Purple Team, Red Team, Blue Team, индустриални системи за управление, ICS, SCADA, киберустойчивост, откриване на кибератаки, MITRE ATT&CK.*

APPLICATION OF PURPLE TEAM METHODOLOGY FOR ASSESSING THE CYBER RESILIENCE OF INDUSTRIAL CONTROL SYSTEMS

chief assist. professor Dimitar I. Nikolov, PhD

Nikola Vaptsarov Naval Academy – Varna

E-mail: d.nikolov@naval-acad.bg

Abstract: *This article examines the application of Purple Team methodology to the assessment and improvement of defensive capabilities in industrial control systems, with particular emphasis on electric power infrastructure. It analyzes collaboration between Red Team and Blue Team specialists, the constraints of controlled cyberattack simulation in operational technology environments, and the importance of combining network, system, and process telemetry. A methodological model is proposed for organizing Purple Team exercises*

through defensive objective definition, relevant technique selection, evidence collection, result analysis, and repeated validation. Evaluation indicators are introduced for detection, diagnosis, response, and operational safety. The study is analytical and methodological in nature, and the proposed indicators require subsequent experimental validation.

Keywords: *Purple Team, Red Team, Blue Team, industrial control systems, ICS, SCADA, cyber resilience, cyberattack detection, MITRE ATT&CK.*

1. ВЪВЕДЕНИЕ

Цифровата трансформация на енергетиката, промишлеността и транспортната инфраструктура води до разширяване на комуникационните връзки между информационните технологии и системите, управляващи физически процеси. Съвременните индустриални системи за управление включват програмируеми логически контролери, отдалечени терминални устройства, операторски станции, системи за диспечерско управление и специализирани комуникационни компоненти. Тяхната функционалност зависи от непрекъснатия обмен на информация и правилното изпълнение на управляващите алгоритми. Същевременно интеграцията с корпоративни мрежи, системи за дистанционна поддръжка и външни цифрови услуги създава допълнителни възможности за кибервъздействие. Според NIST сигурността на оперативните технологии трябва да бъде разглеждана в контекста на специфичните изисквания към надеждността, производителността и безопасността на технологичните процеси (STOUFFER et al., 2023).

При традиционните оценки на информационната сигурност основното внимание често се насочва към наличието на уязвимости, неправилни конфигурации и възможности за неоторизиран достъп. Подобни проверки са необходими, но не предоставят достатъчна информация за действителната способност на организацията да открива и анализира действията на противника. Установяването на техническа слабост не доказва, че тя може да бъде използвана при конкретни оперативни условия, както и че съществуващите защитни механизми няма да разпознаят опита за експлоатация. Ръководството NIST SP 800-115 разглежда техническото тестване като последователен процес на планиране, изпълнение, анализ и разработване на мерки за ограничаване на установените проблеми (SCARFONE et al., 2008). При индустриалните системи този процес изисква допълнително отчитане на технологичните зависимости.

Методологията Purple Team предоставя възможност за преодоляване на част от ограниченията на самостоятелните офанзивни и дефанзивни проверки. Нейната същност се изразява в организирано взаимодействие между специалистите, възпроизвеждащи поведението на противника, и екипите, отговорни за защитното наблюдение и реагирането. В рамките на подобно взаимодействие определена техника може да бъде изпълнена при контролирани условия, анализирана чрез наличните източници на телеметрия и повторно проверена след въвеждането на коригиращи действия. Purple Team Exercise Framework разглежда този подход като средство за систематично усъвършенстване на защитните способности, а не единствено като форма на проникващо тестване (SCYTHE, б. г.).

Целта на настоящото изследване е да се разработи методологична рамка за приложение на Purple Team упражнения при оценяване на киберустойчивостта на индустриални системи за управление. Обект на анализа са защитните механизми и организационните процеси в ICS/SCADA среди, а предмет — възможностите за тяхното проверяване чрез съвместно изпълнение на контролирани сценарии и последваща оценка на резултатите. Изследователският подход включва анализ на специализирани нормативни и методологични публикации, сравнително разглеждане на защитните функции и разработване на система от оценъчни показатели. Предложеният модел е предназначен за бъдещо експериментално прилагане, без да се претендира за извършена емпирична валидация.

2. МЕТОДОЛОГИЧНИ ОСНОВИ НА PURPLE TEAM ПОДХОДА

Разграничението между Red Team и Blue Team произтича от различните им функционални задачи. Red Team възпроизвежда предварително определени модели на атакуващо поведение с цел проверка на защитата, докато Blue Team осъществява наблюдение, идентифициране на подозрителни събития, анализ и реагиране. Purple Team не представлява задължително самостоятелно организационно звено, а може да се реализира като координирана форма на работа между двата екипа. Неговата отличителна характеристика е наличието на обща цел за подобряване на защитните способности, при която действията на атакуващата страна служат като контролирани тестови стимули. В този смисъл сътрудничеството заменя съревнователния елемент като основен механизъм за извличане на практически резултати (SCYTHE, б. г.).

Съществено методологично изискване е изборът на сценарии да бъде основан на действителни модели на заплахи, а не единствено на функционалните възможности на използваните инструменти. Разузнавателната информация за киберзаплахи позволява да бъдат идентифицирани техники, които имат отношение към конкретната технологична архитектура, критичните активи и потенциалните последици от компрометиране. NIST SP 800-150 разглежда обмена на информация за киберзаплахи като средство за подпомагане на идентифицирането, оценяването, наблюдението и противодействието на заплахи (JOHNSON et al., 2016). При Purple Team упражненията тези сведения могат да бъдат преобразувани в проверими защитни хипотези, обвързани с очаквани събития и предварително определени критерии за успех.

За систематизиране на атакуващото поведение е приложима базата от знания MITRE ATT&CK, включително специализираната матрица за индустриални системи. ATT&CK for ICS описва тактики и техники, свързани с достъп до индустриални мрежи, придвижване между системи, събиране на информация, въздействие върху управляващи функции и нарушаване на технологични процеси (MITRE, б. г.-а). Нейното използване предоставя общ терминологичен модел, чрез който действията на Red Team могат да бъдат съпоставени с наблюденията на Blue Team. Допълнително значение имат ресурсите за емуляция на противник, разработени от MITRE, които демонстрират как сведенията за реални кампании могат да бъдат организирани в последователни сценарии за проверка на защитата (MITRE, б. г.-b).

Повторяемостта представлява друг основен принцип на Purple Team оценяването. След установяване на недостатъчна видимост или неправилна класификация се разработва коригиращо действие, което трябва да бъде проверено чрез повторно изпълнение на същия сценарий. Тази логика съответства на концепцията за непрекъснато наблюдение на сигурността, при която организацията поддържа актуална информация за състоянието на активите, заплахите и ефективността на защитните механизми (DEMPSEY et al., 2011). Автоматизираните платформи за емуляция, включително MITRE CALDERA, могат да подпомагат възпроизводимостта на отделни тестови действия, но тяхното използване трябва да бъде ограничено до техники и среди, за които е установена безопасна приложимост (MITRE, 2025).

3. СПЕЦИФИКА НА ТЕСТВАНЕТО НА ИНДУСТРИАЛНИ КОНТРОЛНИ СИСТЕМИ

Индустриалните системи се отличават от стандартните корпоративни информационни среди по непосредствената връзка между цифровите операции и физическите процеси. Изпълнението на управляваща команда може да доведе до изменение на налягане, температура, електрически товар или състояние на комутационно оборудване. Поради това определени техники, допустими при лабораторно тестване на обикновени информационни системи, могат да бъдат неприемливи в действаща технологична инфраструктура. Ръководството NIST SP 800-82 Rev. 3 поставя специален акцент върху съвместното управление на киберсигурността, надеждността и безопасността, като отчита ограниченията на индустриалните компоненти и техния продължителен експлоатационен цикъл (STOUFFER et al., 2023).

За електроенергийната инфраструктура особено значение има разграничаването между киберсъбитие и технологично нарушение. Необичайна последователност от мрежови съобщения може да представлява резултат от легитимна промяна в режима на работа, техническа неизправност или целенасочено въздействие. От друга страна, протоколно валидна заявка може да бъде несъвместима с текущото състояние на електрическата система. Изследването на Zografopoulos et al. (2021) разглежда взаимовръзките между киберфизическите заплахи, оценяването на риска и защитните показатели в енергийните системи. Тази специфика обосновава необходимостта от съчетаване на информационна и инженерна експертиза при интерпретиране на резултатите от Purple Team упражнения.

Допълнително ограничение произтича от разнородността на индустриалното оборудване. В една технологична среда могат да функционират устройства с различни операционни системи, ограничени изчислителни ресурси и специфични комуникационни протоколи. Не всички компоненти поддържат инсталиране на агенти за наблюдение, централизирано събиране на логове или подробна регистрация на административните действия. В резултат на това защитната видимост зависи от комбинирането на мрежова телеметрия, събития от операторските станции, данни от SCADA и измервания на физическия процес. Наличието на множество източници обаче не гарантира тяхната аналитична съвместимост, ако липсват надеждна времева синхронизация и единна идентификация на участващите активи.

Оперативната безопасност следва да бъде включена още при определяне на обхвата на упражнението. Сценариите трябва да се съгласуват с инженерния персонал, като предварително се определят допустимите действия, условията за прекратяване и необходимите средства за възстановяване. Подходът към оценяване на риска, представен в NIST SP 800-30 Rev. 1, позволява разглеждане на заплахите и последствията в контекста на организационните цели (JOINT TASK FORCE TRANSFORMATION INITIATIVE, 2012). Когато определено действие може да предизвика неприемливо технологично въздействие, неговото възпроизвеждане следва да се ограничи до изолирана лабораторна среда или симулационен модел. Така се запазва аналитичната стойност на проверката, без да се допуска неоправдан риск за производствения процес.

4. МЕТОДОЛОГИЧЕН МОДЕЛ ЗА ПРОВЕЖДАНЕ НА PURPLE TEAM УПРАЖНЕНИЯ

Предложеният методологичен модел включва шест взаимосвързани етапа, които осигуряват последователност и проследимост при провеждането на Purple Team упражнения. Първоначално се определя конкретна защитна цел, формулирана като проверима хипотеза относно способността за откриване или реагиране на определено атакуващо поведение. Следва избор на релевантен сценарий, основан на MITRE ATT&CK for ICS и съобразен с архитектурните характеристики на изследваната среда. Третият етап обхваща подготовката на защитното наблюдение чрез идентифициране на необходимите източници на телеметрия и определяне на очакваните доказателства. Впоследствие се извършва контролирано изпълнение на сценария, при което се регистрират техническите действия и съответните защитни събития. Получените резултати се анализират съвместно от участниците, като установените пропуски се използват за разработване на конкретни коригиращи мерки. Заключителният етап включва повторно изпълнение при съпоставими условия с цел установяване на ефективността на предприетите подобрения. По този начин методологията осигурява преход от еднократна проверка към цикличен процес за усъвършенстване на защитните способности.

При практическото приложение на модела е необходимо да се осигури разграничение между изпълнението на тестовото действие и неговото защитно интерпретиране. Red Team документира фактически извършените операции и времевите им характеристики, докато Blue Team установява дали съответните събития

са били наблюдавани, класифицирани и ескалирани по подходящ начин. Координаторът на упражнението съпоставя двата набора от данни и идентифицира несъответствията. Този процес позволява да бъдат разграничени липсата на телеметрия, недостатъчната аналитична информация и организационните затруднения при реагиране. Съвременните препоръки на NIST за управление на киберинциденти подчертават необходимостта от интегриране на откриването, реагирането и възстановяването в цялостния процес за управление на киберриска (NELSON et al., 2025).

Особено важно е коригиращите действия да бъдат насочени към причините за установения пропуск. При липса на наблюдение може да се наложи добавяне на нов източник на данни или промяна в архитектурата на събирането им. Когато събитието е регистрирано, но не е разпознато, подходящата мярка може да включва усъвършенстване на аналитичните правила и контекстната информация. Ако заплахата е правилно класифицирана, но реакцията е неадекватна, проблемът може да се намира в процедурите, разпределението на отговорностите или липсата на инженерно одобрени защитни действия. Подобно разграничаване съответства на функционалния подход на NIST SP 800-53 Rev. 5, при който защитните контроли се разглеждат както според тяхното предназначение, така и според необходимостта от оценяване на тяхната ефективност (JOINT TASK FORCE, 2020).

Възможността за автоматизация следва да се разглежда като средство за повишаване на повторемостта, а не като заместител на експертната оценка. Изследването на Miller et al. (2018) разглежда автоматизираната емуляция като проблем на планиране и изпълнение при непълна информация. За индустриалните системи това обстоятелство има допълнително значение, тъй като технически успешното изпълнение на дадена операция не е достатъчно основание тя да бъде допустима в конкретен технологичен режим. Поради това автоматизирани сценарии могат да бъдат използвани за предварително одобрени проверки в лабораторна среда, докато интерпретацията на процесните последиствия и разрешаването на потенциално рискови действия остават отговорност на компетентните специалисти.

5. ОЦЕНЯВАНЕ НА ЗАЩИТНИТЕ СПОСОБНОСТИ И ПРИЛОЖЕНИЕ В ЕНЕРГЕТИКАТА

Оценяването на защитните способности при Purple Team упражнения се основава на съвкупност от количествени и качествени показатели, позволяващи

разграничаване на различните аспекти на киберустойчивостта. Откриваемостта се определя чрез съотношението между правилно идентифицираните тестови действия и общия брой предварително определени действия, за които се очаква защитен сигнал. Времето за откриване характеризира интервала между началото на тестовото действие и генерирането на валидно предупреждение, докато диагностичната точност отразява способността на анализаторите да определят характера на събитието, засегнатите компоненти и потенциалните последствия. Адекватността на реагирането се оценява чрез съответствието между предприетите защитни действия и предварително одобрените оперативни процедури. Допълнителен показател е повторяемостта, която позволява да се установи дали резултатите остават устойчиви при последователни изпълнения на идентични сценарии. За индустриалните системи особено значение има технологичната безопасност, изразена чрез отсъствие на неприемливи отклонения от допустимите работни режими. Предложената система от показатели има методологичен характер и изисква последващо експериментално валидиране, преди да бъде използвана като стандартизирана количествена оценка.

При количествено сравняване на последователни упражнения може да се използва изменението на дела на откритите действия, представено чрез зависимостта

$$\Delta D = D_2 - D_1$$

, където D_1 обозначава откриваемостта преди коригиращите действия, а D_2 — стойността след тяхното прилагане. Положителната разлика показва подобрене единствено в рамките на проверените сценарии и конкретните експериментални условия. За надеждна интерпретация е необходимо да се осигури съпоставимост на използваните тестови действия, системни конфигурации, източници на телеметрия и критерии за успех. При многократни изпълнения следва да се анализира и вариацията на резултатите, тъй като нестабилното откриване може да бъде скрито зад приемлива средна стойност. Предложените показатели са съвместими с общия принцип за измерими защитни резултати, заложен в Cybersecurity Performance Goals на CISA (CISA, б. г.).

В електроенергийните системи Purple Team упражненията могат да бъдат организирани около три основни групи защитни задачи. Първата е свързана с достоверността на технологичните измервания и разпознаването на несъответствия между предаваните стойности и очакваното състояние на електрическия процес. Втората обхваща контрола върху достъпа до операторски станции, инженерни работни

места и системи за дистанционно управление. Третата е насочена към комуникационната устойчивост и идентифицирането на необичайни промени в индустриалния трафик. За всяка група е необходимо да се определят допустимите отклонения, очакваните защитни доказателства и условията, при които дадено събитие следва да бъде разглеждано като потенциален индикатор за кибервъздействие.

Процесно ориентираното откриване представлява перспективно направление, тъй като позволява комуникационните наблюдения да бъдат съпоставени с физическите зависимости на управляваната система. При електроенергийни процеси това може да включва напрежение, ток, активна и реактивна мощност, състояние на комутационни устройства и последователност на управляващи операции. Нарушаването на определени зависимости може да бъде основание за допълнителен анализ, но не следва автоматично да се интерпретира като доказателство за атака. Технологични неизправности, преходни режими и планирани операторски действия също могат да предизвикат отклонения. Ето защо аналитичната достоверност зависи от интегрирането на мрежовата телеметрия с инженерни модели, експлоатационни данни и информация за текущото състояние на съоръженията (ZOGRAFOPOULOS et al., 2021).

Управлението на резултатите от Purple Team упражненията следва да бъде обвързано с по-широката организационна рамка за киберсигурност. NIST Cybersecurity Framework 2.0 предоставя структура за разглеждане на управлението, идентифицирането, защитата, откриването, реагирането и възстановяването като взаимосвързани функции (NIST, 2024). В този контекст отделните упражнения могат да бъдат използвани за проверка на конкретни защитни способности и за определяне на приоритетите за подобрене. Разузнавателните оценки на ENISA допълват този процес чрез информация за развитието на заплахите и характерните модели на кибероперации (ENISA, 2024). Съчетаването на техническите резултати с актуалния профил на заплахите позволява ограничените ресурси за тестване да бъдат насочвани към области с най-голяма оперативна значимост.

6. ЗАКЛЮЧЕНИЕ

Предложеният модел разглежда Purple Team като средство за последователно валидиране на защитните способности, а не като изолирана демонстрация на атакуващи

техники. Неговата основна методологична стойност произтича от проследимата връзка между избрания сценарий, наблюдаваните защитни събития, установените пропуски и предприетите коригиращи действия. За индустриалните системи тази връзка трябва да бъде допълнена с оценка на физическите последствия и с инженерно обосновани ограничения върху изпълнението. Основните ограничения на подхода са свързани с непълнотата на телеметрията, различията между лабораторните и производствените среди, предварителната осведоменост на защитния екип и зависимостта на резултатите от избора на тестови сценарии. Поради това положителният резултат от отделно упражнение не може да бъде интерпретиран като доказателство за цялостна устойчивост срещу всички възможни противници.

В заключение, приложението на Purple Team методологията създава предпоставки за преминаване от периодично установяване на технически слабости към систематично подобряване на откриването, диагностиката и реагирането при киберзаплахи срещу ICS/SCADA среди. Предложената шестетапна рамка съчетава разузнавателно обоснован избор на сценарии, контролирано изпълнение, събиране на защитни доказателства и повторна проверка. За електроенергийната инфраструктура нейното прилагане изисква интегриране на мрежова и процесна телеметрия, както и участие на инженерните специалисти. Бъдещото експериментално валидиране следва да се осъществи в изолирани лабораторни среди, включващи симулирани електрически процеси, реалистична индустриална комуникация и защитно наблюдение, с цел установяване на измерими промени в защитните способности при запазване на оперативната безопасност.

ИЗПОЛЗВАНА ЛИТЕРАТУРА

CISA. Cross-Sector Cybersecurity Performance Goals. Cybersecurity and Infrastructure Security Agency. [Електронен ресурс]. Достъпно на: <https://www.cisa.gov/cybersecurity-performance-goals> (посетен на 11.10.2026).

DEMPSEY, Kelley; CHAWLA, Nirali; JOHNSON, L. A.; et al. Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. NIST Special Publication 800-137. Gaithersburg: National Institute of Standards and Technology, 2011. DOI: <https://doi.org/10.6028/NIST.SP.800-137>.

ENISA. ENISA Threat Landscape 2024. European Union Agency for Cybersecurity, 2024. [Електронен ресурс]. Достъпно на: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024> (посетен на 11.10.2026).

JOHNSON, Christopher; BADGER, Mark; WALTERMIRE, David; SNYDER, Julie; SKORUPKA, Clem. Guide to Cyber Threat Information Sharing. NIST Special Publication 800-150. Gaithersburg: National Institute of Standards and Technology, 2016. DOI: <https://doi.org/10.6028/NIST.SP.800-150>.

JOINT TASK FORCE. Security and Privacy Controls for Information Systems and Organizations. NIST Special Publication 800-53, Revision 5. Gaithersburg: National Institute of Standards and Technology, 2020. DOI: <https://doi.org/10.6028/NIST.SP.800-53r5>.

JOINT TASK FORCE TRANSFORMATION INITIATIVE. Guide for Conducting Risk Assessments. NIST Special Publication 800-30, Revision 1. Gaithersburg: National Institute of Standards and Technology, 2012. DOI: <https://doi.org/10.6028/NIST.SP.800-30r1>.

MILLER, Douglas; ALFORD, Ron; APPLEBAUM, Andy; FOSTER, Henry; LITTLE, Caleb; STROM, Blake. Automated Adversary Emulation: A Case for Planning and Acting with Unknowns. MITRE, 2018. [Електронен ресурс]. Достъпно на: <https://www.mitre.org/news-insights/publication/automated-adversary-emulation-case-planning-and-acting-unknowns> (посетен на 11.10.2026).

MITRE. ATT&CK for ICS. MITRE ATT&CK. [Електронен ресурс]. Достъпно на: <https://attack.mitre.org/matrices/ics/> (посетен на 11.10.2026).

MITRE. Adversary Emulation and Red Teaming. MITRE ATT&CK. [Електронен ресурс]. Достъпно на: <https://attack.mitre.org/resources/get-started/adversary-emulation-and-red-teaming/> (посетен на 11.10.2026).

MITRE. CALDERA. MITRE Corporation. [Електронен ресурс]. Достъпно на: <https://www.mitre.org/our-impact/intellectual-property/caldera> (посетен на 11.10.2026).

NELSON, Alexander; REKHI, Sanjay; SOUPPAYA, Murugiah; SCARFONE, Karen. Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile. NIST Special Publication 800-61, Revision 3. Gaithersburg: National Institute of Standards and Technology, 2025. DOI: <https://doi.org/10.6028/NIST.SP.800-61r3>.

NIST. The NIST Cybersecurity Framework (CSF) 2.0. NIST Cybersecurity White Paper 29. Gaithersburg: National Institute of Standards and Technology, 2024. DOI: <https://doi.org/10.6028/NIST.CSWP.29>.

SCARFONE, Karen; SOUPPAYA, Murugiah; CODY, Amanda; OREBAUGH, Angela. Technical Guide to Information Security Testing and Assessment. NIST Special Publication 800-115. Gaithersburg: National Institute of Standards and Technology, 2008. DOI: <https://doi.org/10.6028/NIST.SP.800-115>.

SCYTHER. Purple Team Exercise Framework. [Електронен ресурс]. Достъпно на: <https://github.com/scythe-io/purple-team-exercise-framework> (посетен на 11.10.2026).

STOUFFER, Keith; PEASE, Michael; TANG, CheeYee; et al. Guide to Operational Technology (OT) Security. NIST Special Publication 800-82, Revision 3. Gaithersburg:

National Institute of Standards and Technology, 2023. DOI:
<https://doi.org/10.6028/NIST.SP.800-82r3>.

ZOGRAFOPOULOS, Ioannis; OSPINA, Juan; LIU, Xue; KONSTANTINOU, Charalambos.
Cyber-Physical Energy Systems Security: Threat Modeling, Risk Assessment, Resources,
Metrics, and Case Studies. IEEE Access, 2021, Vol. 9, pp. 29775–29818. DOI:
<https://doi.org/10.1109/ACCESS.2021.3058403>.