# КИБЕРПОЛИГОНЪТ НА ЕЦИХ ТРАКИЯ ПО ПРОЕКТ „CYBER4ALLSTAR“ КАТО СРЕДА ЗА РАЗВИТИЕ НА ЕКСПЕРТИ В СФЕРАТА НА МРЕЖОВАТА И ИНФОРМАЦИОННА СИГУРНОСТ В ЮЖЕН ЦЕНТРАЛЕН РЕГИОН“

Д-Р ХРИСТИАН ДАСКАЛОВ, СТАНИСЛАВ АТАНАСОВ

*Цифров иновационен хъб „Тракия“, Пловдивски университет „Паисий Хилендарски“*
*h.daskalov@edihtrakia.org, s.atanasov@edihtrakia.org*

***Резюме:*** *Цифровият иновационен хъб „Тракия“ (ЦИХ Тракия) обединява представители на академичните среди, МСП, институции и браншови асоциации, за да осигури безвъзмезден достъп до услуги в сферата на киберсигурността както чрез капацитета на членовете и експертите на ЦИХ Тракия, така и чрез установените партньорски отношения в рамките на Европейския коридор на цифровите хъбове в киберсигурността (ECCE) и Европейската организация по киберсигурност (ECSO). По опита на ECCE и ECSO се изгражда и първият в България киберполигон с отворен достъп за развитие на експерти в сферата на мрежовата и информационна сигурност, който през 2024 г. стартира на територията на Южен Централен Регион. Неговата архитектура от гледна точка на съвременните технологични, бизнес и академични добри практики е представена и анализирана в настоящия доклад.*

**Ключови думи:** *киберполигон, цифров иновационен хъб, киберсигурност*

# THE CYBER RANGE OF EDIH TRAKIA UNDER THE "CYBER4ALLSTAR" PROJECT AS AN ENVIRONMENT FOR THE DEVELOPMENT OF EXPERTS IN THE FIELD OF NETWORK AND INFORMATION SECURITY IN BULGARIA’S SOUTH-CENTRAL REGION

DR. HRISTIAN DASKALOV, STANISLAV ATANASOV

*Digital Innovation Hub Trakia, Plovdiv University „Paisii Hilendarski“*
*h.daskalov@edihtrakia.org, s.atanasov@edihtrakia.org*

***Abstract:*** *The Digital Innovation Hub „Trakia“ (DIH Trakia) brings together representatives of academia, SMEs, institutions and industry associations to provide free access to cybersecurity services on a regional, national and European levels through the capacity of the DIH members and experts, as well as through the established relationships with the European Corridor of Digital Hubs in Cyber Security (ECCE) and the European Cyber Security Organization (ECSO). Following the successful experience of ECCE and ECSO members, Bulgaria's first open-access cyber-range for the development of experts in the field of network and information security is being launched on the territory of the South-Central Region. The architecture of the system from the perspective of the current technological, business and academic best practices, is analyzed within the article.*

**Key words:** *cyber-range, digital innovation hub, cybersecurity*

## 1. Въведение

С оглед на нуждата да изясним някои ключови понятия от сферата на киберсигурността, в контекста, в който са използвани те в настоящия доклад, „Киберпространство“ или „Киберполигон“ (което ще използваме като превод на „Cyber-Range“ като кибер-физична система) следва да бъде разбирано, както е представено в цитирания тук документ на „European Cyber Security Organization“ – Европейската организация по киберсигурност (ESCO), а именно:

*„Киберполигон е платформа за разработване, предоставяне и използване на интерактивни симулационни среди. Симулационната среда представлява представяне на информационната и телекомуникационна инфраструктура на дадена организация, индустриалната и мрежа, мобилни и физически системи, приложения и инфраструктури, включително симулация на атаки, потребители и техните дейности, както и на всякакви други интернет, публични услуги или услуги на трети страни, от които симулираната среда може да зависи. Киберполигонът включва комбинация от основни технологии за реализиране и използване на симулационната среда и на допълнителни технологии за компоненти, които от своя страна са желателни или необходими за постигане на цели, свързани със специфична употреба на киберпространството.“* [1] [2]

За да може да се изпълнят целите на научния доклад за гарантиране на ясното разбиране от страна на изследователите и доставчиците на подобни решения за нуждите на Цифрови иновационни хъбове в цяла Европа, би следвало в увода към доклада да бъдат посочени още и целите, които си поставя екипът зад проекта „Cyber4AllSTAR“ при употребата на решението на територията на Южен Централен Регион (ЮЦР), и които трябва да изпълнява разработеният и позициониран в ЮЦР киберполигон:

1. Киберполигонът следва да функционира като Емулирана виртуална среда (Emulated virtual environment), която е способна да емулира различни компютърни и мрежови архитектури, като по този начин улеснява експериментирането, тестването и възпроизвеждането на реални сценарии и случаи на употреба.

Средата трябва да може да бъде мигрирана в различни центрове за данни и да се използва повторно, за да се подпомогне обучението, решаването на проблеми, тестване и сертифициране на софтуерни решения; изследвания по различни теми и проблеми, свързани с киберсигурността.

Емулираната виртуална среда позволява да се създават виртуални мрежи от напълно функционални възли, в които работят различни операционни системи, мрежови стекове и приложения.

2. Киберполигонът следва да опосредства провеждането на игри / симулации за киберсигурност, в които:

a. Екипите от обучаващи се участници могат да се състезават помежду си в защита / компрометиране на сигурността на предварително определени мрежови възли и схеми;

b. Самостоятелни обучения, при които екипи от отделни лица могат да се състезават срещу предварително инсталирани софтуерни решения за защита / атака, за да постигнат определени цели и да придобият практически опит;

c. Предварително дефинирани индивидуални обучения за повишаване на осведомеността и уменията на участниците в областта на киберсигурността, както и за проверка на знанията и уменията на специалисти по мрежова и информационна сигурност с цел валидиране на същите и сертификация.

## 2. Проект – инициатори и цели

Цифровата трансформация и киберсигурността са основен приоритет на Европейския съюз през настоящия програмен период, който Европейската Комисия изпълнява посредством програма „Цифрова Европа“ 2021-2027 г. Ключов момент в тази програма е изграждането на мрежа от Европейски цифрови иновационни хъбове (European Digital Innovation Hubs – EDIHs), които да ускорят широкото използване на новите технологии (изкуствен интелект, високопроизводителни изчисления, блокчейн и др.), благоприятстващи разработването и въвеждането на иновациите сред малките и средни предприятия и публичните организации на принципа „тествай преди да инвестираш“. [3]

Европейски цифров иновационен хъб „Тракия“, познат още и под наименованието Cyber4AllSTAR е част от тази пан-европейска мрежа и по същество представлява съвместен проект между Съюза за стопанска инициатива, Българска асоциация по киберсигурност, Община Пловдив, Българска академия на науките и др. партньори, обединени в сдружение „Цифров иновационен хъб Тракия“.

Цифров иновационен хъб „Тракия“, позициониран в гр. Пловдив, е избран на Европейско ниво да промотира и предоставя услуги по цифровизация и киберсигурност в Южен централен район – гр. Пловдив, гр. Пазарджик, гр. Смолян, гр. Хасково и гр. Кърджали, както и на територията на цялата страна, доколкото предизвикателствата пред киберсигурността в България нямат регионален характер или обхват.

Ролята на Хъба (понятието е идентично на „координационен център“) е да предоставя на бизнеса и местната администрация иновативни цифрови решения, за да ги интегрират те в ежедневната си дейност. ЕЦИХ Тракия служи като точка за контакт, която предоставя цифров капацитет и предлага възможността за експериментиране и тестване на нови технологии според специфичните нужди и дейността на бизнеса и местните власти в региона с фокус върху решенията в сферата на киберсигурността.

Дейностите в обхвата на ЕЦИХ „Тракия“ допринасят за осигуряването на киберустойчива среда в Южен-централен регион, както и за привличането на чуждестранни и национални инвестиции в индустриите с висока добавена стойност, доколкото същите могат да претендират за съответствие с новите европейски регулации в сферата на киберсигурността като European Cybersecurity Act & Certification Framework, European Cyber Resilience Act, European Cyber Solidarity Act, Dora, NIS, NIS2, AI Act, Chips Act и др.

Позиционирането на хъба на територията на Южен централен район (по-специално на територията на Община Пловдив) е свързано с особеностите на индустриалното развитие на региона, с потребностите на бизнеса и местните власти в него, и с експертизата на местната академична общност.

Както бе споменато, ЕЦИХ „Тракия“ е част от европейската мрежа от ЕЦИХ съсредоточени в сферата на киберсигурността, която се координира от Европейската организация по киберсигурност (ECSO), договорен партньор на Европейската комисия и нейния European Cybersecurity Coordination Center (ECCC) по въпросите на киберсигурността. Експертите по мрежова и информационна сигурност от ЮЦР получват достъп до най-добрите практики и технологии в целия Европейски съюз, благодарение на интеракцията с ЕЦИХ Тракия. По-конкретно, Хъбът може да им бъде полезен със следното:

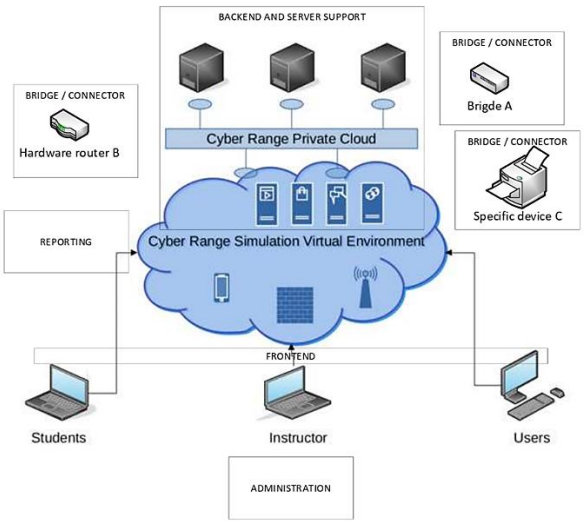
1. Възможност за безплатно базово обучение на специалистите и на настоящи и бъдещи техни клиенти и партньори по теми, свързани с киберсигурността – кибер хигиена, общи правила за спазване и придобиване на базови умения във връзка с цифровата трансформация и нови технологии;
2. Възможност за възползване от безплатни услуги за киберсигурност, свързани с проверка и подобряване на киберсигурността в съответните фирми и институции – близо 30 са услугите по каталог;
3. Възможност за безплатна консултация за осигуряване на европейско и национално финансиране на проекти, свързани с нови информационни технологии;
4. Възможност за участие в тематични конференции и семинари;
5. Възможност за включване в общността от експерти по киберсигурност, независимо от индивидуалното ниво и позиция.

### 3. Киберполигон – ключови компоненти

При изграждането на решението на ЕЦИХ Тракия за киберполигон е взет предвид и реализиран подходът, описан като CRAI (Cyber Range Advanced Implementation, не по-ранна версия от Version 3.0). Този подход, измежду други подобни [4], дава възможност на инструкторите да създават структурирани сценарии за обучение, а на обучаемите - да участват в обучителни сесии, включващи:

1. напълно емулирана виртуална среда;
2. физически налични мрежови среди;
3. хибридни среди, които използват както виртуални, така и физически устройства и възли.

По този начин решението може да обслужи голям брой услуги от портфолиото на хъба. За да представим примерната архитектура и подход за реализиране на Киберполигона, ще приложим следната диаграма като Фиг. 1, последвана от описание на нейните компоненти:




***Фиг. 1.*** *Базова архитектура на киберполигона*

- Front-End: Този компонент е отговорен за осигуряването на реалистичен и адаптивен интерфейс за различните групи потребители на киберполигона. Той е базиран на съвременен уеб базиран UX със централизирано съхранение на историята на действията и активностите, резултатите от тестването и обучението, напредъка по различните сценарии и т.н. Последната, но не и по важност функция на фронтенда, е да показва на живо отчитане и състояние на използваните виртуални среди;

- Backend: Това е ядрото на киберполигона, което отговаря за управлението на виртуални среди и техния пълен жизнен цикъл (създаване, използване, унищожаване), действията на потребителите, наблюдението (мониторинга) и оркестрацията на всички останали системни компоненти;

- Bridge/connector (мостове): Този компонент отговаря за свързването на физическите устройства с виртуална среда/мрежа. В зависимост от конкретния случай на използване, мостовете може да не бъдат активирани, ако всички мрежови елементи могат да бъдат емулирани и липсва връзка с физическа или отдалечена виртуална среда;

- Reporting (отчети): Този компонент отговаря за събирането на съответните системни и потребителски събития и създаване на отчети за дейността, инциденти, свързани с киберсигурността, или всякакви други данни, които се генерират от използването на киберполигона, или когато той е в състояние на покой или поддръжка;

- Administration: Този компонент е отговорен за осигуряване на специализиран административен интерфейс за привилегированите системни потребители. Тези специални функции включват опции за проектиране, модифициране или добавяне на нови сценарии, конфигуриране на други потребителски характеристики, контрол върху използването на виртуални среди и др.;

При реализиране на решението за киберполигон са приложени както ключовите компоненти, така и концептуалните принципи, описани в CRAI а именно:

- Обектно-ориентиран подход с повторно използване на съществуващи компоненти, когато са възможни такива с отворен код тип „permissive licensing terms“. Дизайнът на системата и компонентите е съвместим и се придържа към съвременните принципи за разработване на Agile софтуер (или сходен подход с подобна гъвкавост и контрол над процеса и качеството).

При реализиране на системата са взети предвид следните изисквания, които са включени и в оценка на изначално предложените решения:

1. Отворен достъп до изходния код, прозрачност на продукта и липса на компоненти, насочващи към определен доставчик. Това е особено важно, за да се гарантират редовни актуализации на компонентите на системата, контрол при извършване на промените, свързани със сигурността и функционалностите, възможност за извършване на одити и прегледи на кода. Това изискване е важно и за гарантиране на самостоятелността на проекта след изтичане на гаранционния период. Дизайнът, архитектурата и съпътстващата документация трябва да бъдат предадени на възложителя, като се прехвърли интелектуалната им собственост върху продукта, на всички компоненти които са разработени и уникални и по задание на възложителя. Изпълнителят трябва да се ангажира, че няма да може да използва компоненти, архитектура и функционалности и други части от проекта, станали собственост на възложителя без негово писмено разрешение.

2. Активна общност и поддръжка на избраните решения за реализация на киберполигона. Поради планирания дълъг хоризонт на проекта, тези характеристики са изключително важни, за да се гарантира стабилност и бърза реакция в случай на проблеми или необходимост от въвеждане на промени. Общностите са важен компонент и в стратегията на ЕЦИХ „Тракия“ и комуникацията с тях е стратегическа.

3. Мащабируемост и подобрения. Планираните разширения и подобрения на киберполигона трябва да бъдат поддържани и улеснявани от избора на технологии, продукти и реализация.

Имайки предвид, че архитектурата на полигона е разпределена и може да се налага балансиране на натоварването и трафика, както и че е изключително важно да се поддържа високо ниво на потребителска удовлетвореност и оперативна съвместимост, следните минимални комуникационни протоколи също са заложени и поддържани в имплементацията на съответните зони:

А. Вътрешна зона (недостъпна директно от интернет) поддържа следните протоколи :

- SSH: Този протокол е основният протокол за отдалечен достъп до системите в ядрото и виртуалните среди, както и до мрежите, и техните възли. SSH поддържа методите за идентификация чрез потребителско име, парола и ключове. Всички системи, достъпни от публичен интернет и използвани за дейности,

свързани с конфигурация или администрация, както и достъпа до VPN използван за такава цел, са минимум с двуфакторна идентификация.

- Remote desktop (RDP): Протоколът е необходим за случаи, в които се достъпват в обучения или администриране машини с Windows операционна система. Употребата на този протокол е сведена до минимум и не се препоръчва, нито има практика да бъде прилаган в среда извън учебната.

- HTTPS REST: е протокол, използван за комуникация между системните модули, модулите за обучение и отчетите с потребителите на киберполигона. Целта му е да извлича данни или да предава конфигурации, с което реализира част от функциите по интеграция. Минималната допустима версия на SSL към датата на инициирането на полигона е TLS 1.3.

- AMQP: Смисълът на този протокол е да реализира RPC и междукомпонентните комуникационни канали (най-често в контекста на комуникация „module-to-module“).

- Други необходими TCP/IP и UDP протоколи: Това са всички други протоколи, необходими за пълна симулация на мрежовата среда, различна топология и постигане на поставените цели на киберполигона.

Б. Външна зона (достъпна от интернет):

- VPN: За да може потребителят на полигона да достъпи средата на виртуалната симулация за обучения, да наблюдава или администрира компоненти на системата, е необходимо да изгради защитена връзка през VPN (Virtual private network).

- Потребителски web базиран интерфейс за достъп: Част от компонентите, които са свързани с информационна, подготвителна или административна дейност към киберполигона и не са част от административния интерфейс или стимулационните компоненти са достъпни директно през HTTPS TLS 1.3 (или по-нова). Тази функционалност е предвидена с цел намаляване на административната и оперативна тежест за достъп до компоненти от средата, ползването преди реалното обучение и отговаря изцяло на принципа за достъпност и прозрачност.

При така описаното проектиране на киберполигона са взети предвид и следните принципи за производителност, устойчивост и управление на риск, посочени по-долу, които са съществена част от неговата архитектура:

- Модулност - дизайнът на киберполигона предполага използването на модули, които се изграждат и разгръщат самостоятелно, но могат да работят заедно, за да осигурят желаната функционалност и потребителско изживяване. Макар че модулите зависят един от друг, те могат да бъдат конфигурирани на различни сървъри, облачни доставчици на услуги и просто на отделни машини. Това дава възможност за по-голяма гъвкавост, предотвратява не загуба на оперативност и загубата на данни. При разрастване на системата или необходимост от промяна на архитектурата, модулността осигурява гъвкавост и преносимост.

- Мащабируемост – киберполигонът следва да е мащабируем и внедряването му следва да позволява увеличаване на броя на участващите физически или виртуални сървъри, както и на свързаните подсистеми. В зависимост от сценария и нуждите на потребителите, компонентите на киберполигона могат да бъдат инсталирани в частния облак на Хъба, на сървъри на компанията ползвател или на мобилен сървър, стандартни сървъри в облака или специализиран собствен облак. В съответствие с необходимата изчислителна мощност и броя на потребителите се използва стандартно балансиране на натоварването и методите за обединяване могат да бъдат използвани за обслужване на голям брой заявки и да позволяват голям обем на едновременни сесии.

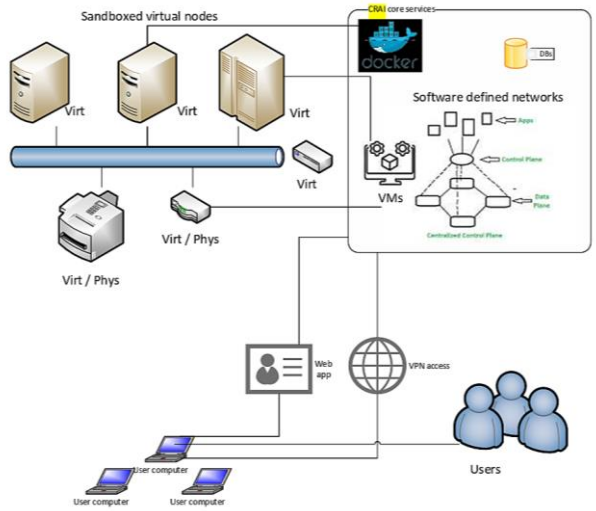
- Непрекъсваемост, резервираност и мониторинг – киберполигонът трябва да предостави качествена услуга и добро потребителско преживяване. За целта, при проектирането е важно да се направи анализ на непрекъсваемостта и факторите, оказващи влияние и да се планира дублиране на критичните компоненти. Качеството на процесите в полигона са обект на постоянното наблюдение за производителност, аларми, срив или събития, свързани с киберсигурността във всичките му компоненти. За целта, като неразделна част от реализацията му, са предвидени и системи за регистриране на натоварване и грешки, системи за регистриране на събития в контекста на киберсигурността, системи за управление на конфигурациите и агрегатор на логове.

- Управление на риска – при проектирането на киберполигона са предоставени предварителни оценки на риска на предложеното решение, съгласно ISO 27005, или аналогичен подход (според практиката на изпълнителите). Анализът на риска се прави с цел да се удостовери познаване на принципите за сигурно проектиране и сигурност по дизайн. За референция към подходите от участниците информацията е структурирана съгласно добрите практики в ISO 27005.

Следва да се отбележи, че като част от оценката на риска е предоставена и методология, която се използва за проверка на слабостите на

решението и реализирания подход за извършване на тестове. При приемането на решението са извършени тестове съгласно използваната методология, прилагана от ЕЦИХ „Тракия“ при предоставяне на услугите от портфолиото на Хъба, като тя в най-общи линии може да бъде определена като сходна на NIST SP 800-115.

Като обобщение по тази точка представяме във Фиг. 2 детайлната логическа архитектура на мултифункционалното кибер-физично решение, без да навлизаме в дълбочината на детайлите, описани по-горе:




***Фиг. 2.*** *Детайлна архитектура на полигона*

## 5. Заключение

Настоящият доклад постига своята цел да представи аналитично киберполигона на ЕЦИХ Тракия, изграден по проект „Cyber4AllSTAR“, като среда за развитие на експерти в сферата на мрежовата и информационна сигурност в Южен Централен регион“, фокусирайки се върху техническите характеристики на полигона.

Ограниченията в обхвата на доклада не позволяват да се навлезе в детайлите на съществени за общността на специалистите по киберсигурност въпроси като изискванията към сигурността на реализацията на полигона; създаването и активирането на сценарии върху полигона; проблемите при управлението на отношенията между стейкхолдърите по иновационни проекти и програми [5]. Това са въпроси, които биха могли да се разгледат в последващи научни статии, особено когато бъдат генерирани достатъчно данни, които да валидират съответните изследователски хипотези от страна на екипа зад киберполигона.

Конкретната изследователска препоръка е да се постави акцент върху разглеждането на сценариите като ключов компонент от един съвременен киберполигон, тъй като бурното развитие на генеративния изкуствен интелект в последните години значително промени процесите по тяхното създаване и активиране:

- Сценариите са последователност от събития във виртуалната и реалната среда, като част от компонентите могат да бъдат предварително зададени и програмирани, а други са част от причинно-следствената връзка, породена от влиянието на средата, от участниците в нея или нейните компоненти.
- Създаването на сценария е процес, в който се описват всички компоненти на средата – физически или виртуални, по начин, по който да могат да бъдат повторяеми и споделяни.
- Сценариите имат ясна цел и носят възможност за придобиване или потвърждаване на умения и знания.
- Сценариите могат да имат и характер на тест за системи и устройства в случаите, когато говорим за сценарии, свързани с цифрови близнаци или ясно обособени системи и цели.

Поради всичко по-горе изброено, темата за създаването и активирането на сценарии за обучение, валидация на знания и умения и сертификация на софтуерни и хардуерни продукти чрез киберполигон се превръща в централна тема. Нейното разглеждане се предхожда задължително от постигането на общо разбиране за начина на функциониране на съответните кибер-физични системи – цел, което настоящият доклад изпълнява успешно.

## ЛИТЕРАТУРА


1. European Cyber Security Organization, Cyber range features checklist, ECSO WG5 Report, 2022.
2. European Cyber Security Organization, Understanding Cyber Ranges: From Hype to Reality, ECSO WG5 Report, 2020.
3. European Commission Joint Research Center, „Digital innovation hubs as policy instruments to boost digitalization of SMEs“ Science for Policy Report, 2020.
4. Lates, I. Cyber Ranges Implementation Methodology, Proceedings of the 16th International Conference on Business Excellence, 2022.
5. Даскалов, Х. Стейкхолдър мениджмънт по проекти, програми и стратегии в образованието, науката и иновациите, Военно издателство, 2014.