

ИНОВАТИВНИ ПРЕВАНТИВНИ И ОПЕРАТИВНИ СТРАТЕГИИ ЗА КИБЕРЗАЩИТА И ОТБРАНА НА КОМУНИКАЦИОННИ И ИНФОРМАЦИОННИ МРЕЖИ В РЕАЛНО ВРЕМЕ

Петър Манев

Университет по библиотекознание и информационни технологии

Резюме: В съвременния свят, където мрежовите и ИТ устройства са част от ежедневието ни, съществува голямо разнообразие от операционни системи, доставчици и потребители, което от своя страна въвежда много точки на непреднамерено излагане на злонамерени и нежелани дейности. Поради това разнообразието, структурата и сложността на подобни нежелани атаки представляват сериозно предизвикателство по отношение на създаване на мерки за киберзащита и отбранителни мерки за много различни и разнообразни инфраструктури, които непрекъснато се развиват. Има много предизвикателства пред изготвянето на единна стратегия за защита, като тези предизвикателства варират от инсталационни, хардуерни и инфраструктурни изисквания до търговски и доставни специфики и способност за правилно обучение на персонала.

Това изследване разглежда и обобщава предложение за иновативни превантивни и оперативни стратегии за киберзащита и отбрана на комуникационни и информационни мрежи в реално време, главно чрез фокусиране върху мониторинг на мрежовата сигурност, който не зависи от операционните системи и инфраструктурата, може да бъде разпръснат и същевременно има контейнеризиран модел на работа, разделен по основни функционалности, за да се осигури максимална защита на самата система. Въз основа на практическия опит на авторите в индустрията за киберсигурност при разработването на подобни системи, това е постижимо чрез използване на иновативни подходи както за самото проектиране и внедряване, така и за обучение.

Ключови думи: киберотбрана; киберстратегия; информационни мрежи; оперативни стратегии

ВЪВЕДЕНИЕ

Киберзаплахите продължават да се увеличават с постоянното развитие на ИТ технологиите. Организацията често се затрудняват да се справят с обема и сложността на кибератаките. Киберстратегии за защита също трябва да поддържат темпа и постоянно да се развиват със заплахите. Като част от мерките, които се прилагат, Европейският съюз разширява обхвата на приложение на стратегията за киберсигурност, като се включват дигитални доставчици, публични администрации, производство на критични продукти и същевременно има изискване за докладване на по-големи инциденти в рамките на 24 часа (Директива (ЕС) 2022/2555). Има по-голяма нужда от по-ранно предупреждение, по-широки оценки на риска и разширено наблюдение на сигурността.

Агенцията за киберсигурност и сигурност на инфраструктурата (АКСИ)

(Cybersecurity and Infrastructure Security Agency 2020) очертава в своята рамка за киберсигурност постоянното наблюдение за мрежова сигурност като критична категория от функциите за ранно оповестяване и откриване на нарушители (Cybersecurity Framework Implementation Guidance 2020, р. 9). Има нужда от постоянно обновяване в подхода, мерките и инструментите за киберсигурност и съответно тяхното приложение.

Много от настоящите предизвикателства пред стратегиите за киберзащита произтичат главно от различията в хардуера, операционните системи и зависимостите на търговските доставчици при инсталирането, поддръжката и обучението на персонала за мониторинг на сигурността на комуникационните мрежи. Разнообразието от електронни устройства и комуникационни мрежи създава предизвикателства при избора на най-важните точки за мониторинг. Това изследване предлага нов модел за мониторинг и операции на мрежовата сигурност, който адресира проблемите и елиминира единичните точки на отказ, включително по отношение на инсталирането, вътрешната сигурност на системата, експлоатацията и поддръжката.

МЕТОДОЛОГИЯ НА ИЗСЛЕДВАНЕТО

Освен общите методологии, произлизащи от теорията на системите, анализ и синтез, са използвани частни научно-практически методологии за контрол и наблюдение, а именно:

▷ „Методология за секторни оценки на киберсигурност“ (European Union Agency for Cybersecurity 2021, р. 13) с цел осигуряване на координирано прилагане на контроли за сигурност;

▷ „Методология за киберзащита за организация“ (National Cyber Security Authority, 2017, р. 59) за изследване на възможностите за прилагане на иновации в мрежовата сигурност (наблюдение). На базата на анализ на критичните системни компоненти на комуникационната инфраструктура са изведени предложения за иновативни решения на оперативно стратегическо ниво на управление.

РЕЗУЛТАТИ

Изведени са предизвикателствата пред съвременните сложни информационни и комуникационни мрежи от гледна точка на киберсигурност, сложност и нехомогенност на инфраструктурата и софтуерните приложения. Основните изследователски въпроси, разгледани в този доклад, са:

▷ важни съвременни предизвикателства пред системите за киберсигурност (наблюдение) на инфраструктурите в съвременните комуникационни мрежи;

▷ иновативни стратегии за системи за превантивна киберзащита и отбрана на комуникационни и информационни мрежи в реално време, като децентрализиран мениджмънт на операция, портативност, компонентна сигурност, агностична архитектура, операционна система и хардуер независимост на функционалността.

ДИСКУСИЯ

От методологическа гледна точка е необходимо да се анализират същността и съдържанието на използваните основни понятия, произлизащи от темата.

Значението на понятието *иновация* се определя от неговия корен, а именно „нов“. Понятието означава процес на създаване на идеи, концепции и стратегии с цел внедряването им в алгоритмите на функциониране на системите за киберзащита и отбрана, като нови подходи, алгоритми, методологии и методи, водещи до по-ефективна адаптация към вътрешната и външната среда, в която функционира държавната (организационна) система за защита на комуникационната и информационна система (КИС).

Следователно семантиката на понятието *иновация* означава нещо ново в КИС, което не е прилагано (правено) до момента при анализите в организацията или технологичната система.

За да се анализират иновациите в КИС, които оперират в киберпространството, следва да се дефинира ясно какво представлява то. Според National Institute of Standards and Technology (NIST 2012) киберпространството е:

„Глобален домейн в информационната среда, състоящ се от взаимозависима мрежа от инфраструктури на информационни системи, включително интернет, телекомуникационни мрежи, компютърни системи и вградени процесори и контролери“.

От определението става ясно какво е съдържанието на киберпространството, т.е. елементите, от които се състои. А същността му, т.е. закономерностите, на които се основава функционирането на елементите от съдържанието, е концептуално и технологично дефинирана в проекта на системата и реализирана на практика.

За генериране на определение на понятието *киберсигурност* на концептуално ниво, се прилага подходът, при който е изградено определението на концептуално ниво на по-общото понятие *сигурност* (Manev 2016, p. 274). В този контекст, на концептуално ниво, даваме следното определение:

Киберсигурността е динамично състояние, при което електронната комуникационна (информационна) система функционира съгласно плановия алгоритъм и правила, в рамките на допуските на стойностите на нейните, на външната и на вътрешната среда параметри, и ако по някакви причини излезе извън рамките на плановото функциониране и работа, то тя разполага с ресурси (сили и средства) да го възстанови.

На концептуално ниво динамиката в режимите на функциониране на системите може да се анализира в обхвата на трите характерни зони и нива на сигурност, а именно номинална, аварийна и катастрофална (Manev 2019).

Независимо че приемаме по-горе посоченото определение на понятието *киберсигурност*, посочваме и виждането на стандарта ISO/IEC

27032:2012, който определя: „Киберсигурност е осигуряване на конфиденциалност, цялостност и достъпност на информацията в киберпространството“ (ISO/IEC 27032:2012).

Налага се изводът, че това определение има по-скоро технократски подход, отколкото научен, на концептуално ниво, каквато е темата на изследването. Това е основанието да се използва посоченото по-горе определение на понятието *киберсигурност*.

NIST определя мрежата като: „Информационна(и) система(и), внедрена(и) с набор от взаимно свързани компоненти. Такива компоненти могат да включват рутери, хъбове, кабели, телекомуникационни контролери, ключови разпределителни центрове и устройства за технически контрол“.

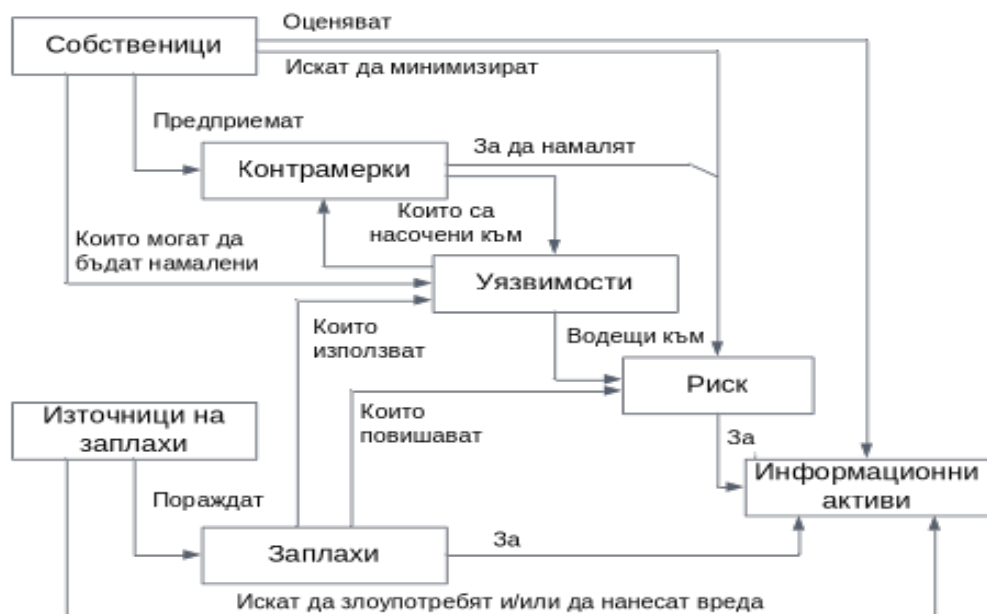
Определение на понятието *електронна комуникационна мрежа* е дадено в „Европейски кодекс за електронни съобщения“ по следния начин:

„Преносните системи, независимо дали са базирани на постоянна инфраструктура или централизиран административен капацитет, и, където е приложимо, комутационно или маршрутизиращо оборудване и други ресурси, включително мрежови елементи, които не са активни, които позволяват преноса на сигнали по кабел, радио, оптични или други електромагнитни средства, включително сателитни мрежи, фиксирани (с комутация на канали и пакети, включително интернет) и мобилни мрежи, електрически кабелни системи, доколкото те се използват за предаване на сигнали, мрежи, използвани за радио и телевизионно излъчване, и кабелни телевизионни мрежи, независимо от вида на пренасяната информация“ (Direktiva (ES) 2018/1972).

Съгласно ISO/IEC 27000 определението на понятието *инцидент с информационната сигурност* е:

„Единични или поредица от нежелани или неочаквани събития със сигурността на информацията, за които има значителна вероятност да компрометират бизнес операциите и да застрашат информационната сигурност“ (ISO/IEC 27000:2018).

Според въздействието и потенциалните вреди за организациите инцидентите може да бъдат класифицирани като: *критични* – в резултат на атаки, които трудно може да бъдат спрени или ограничени, предизвикващи инциденти, при които може да бъде изложен човек или критична инфраструктура на риск от физическо увреждане; *предизвикващи пълно или частично прекратяване на бизнес процеси*, операции, услуги, чието възстановяване изисква големи усилия, ресурси и време; *увреждащи* – засягат само отделни ресурси, операции или услуги; *тривиални* – предизвикващи незначително или краткотрайно вредно въздействие, при което не е задължително да се предприемат незабавни действия, но което е наложително да бъде наблюдавано. От изключително важно значение е да се създават и прилагат на практика иновативни и превантивни оперативни стратегии за киберзащита и отбрана на комуникационни и информационни мрежи в реално време (фиг. 1).



Фиг. 1. Общи понятия за сигурност и тяхната взаимовръзка
(Mitev, Denchev 2023, pp. 483 – 491)

Превенцията е дейност в организацията, която се планира, организира и провежда, преди да се случат инциденти. За тази цел следва да са анализирани възможно най-добре същността и съдържанието на уязвимостите, рисковете на защитаваната информационна система, както и възможните източници на видовете заплахи. Анализите на рисковете се отнасят към защитаваната система и организацията, която е собственик, докато изследването на заплахите се отнася към външната среда, в която оперират организацията и нейната информационна система.

Стратегията е дългосрочно проектирана дейност чрез изпълнение на ключови основни задачи, при което изпълнението на следващата е възможно само след изпълнение на предходната. В този контекст е необходимо да се адресират основни съвременни кибероперации и съответно предизвикателствата по отношение на иновативни превантивни и оперативни стратегии:

- ▷ Създаване на нов модел за мониторинг на комуникационната информационна мрежа (КИМ), който гарантирано да се внедрява независимо от софтуерните изисквания на всяка операционна система.

- ▷ Системата за мониторинг на КИМ да е независима от наличието на интернет – да може да работи в затворени среди. Това изисква тя да има всички необходими компоненти, като управление, откриване и предупреждение, готови и достъпни за употреба в автономен режим.

- ▷ Да може да работи в разпръснат режим. От оперативна гледна точка самата система не трябва да има централна точка на управление на повреда. Тя

трябва да може да се внедрява на толкова места, колкото е необходимо, и процесът на оперативно внедряване не трябва да зависи от наличието на централно място за управление.

▷ Мобилност на системата за мониторинг. Да е портативна – не трябва да зависи от никакъв вид инсталационен носител, като виртуална инфраструктура, DVD/CD и/или съществуващи софтуерни изисквания.

▷ Системата за мониторинг на сигурността да бъде хардуерно независима. Това позволява по-бързо внедряване и/или операции за реагиране в киберпространството в реално време. По този начин се отговаря на изискването за възможност за мониторинг в КИМ, функциониращи в аварийен режим, при изпадане в такава ситуация.

▷ Да бъде контейнеризирана, за да се осигури максимална сигурност за собствените ѝ операции, за да не бъдат прекъсвани от зловреден софтуер или нежелана и неоторизирана активност. Всяка система за мониторинг на мрежовата сигурност трябва да има своите основни компоненти, като данни, визуализация, управление, откриване и оповестяване – разделени и изолирани, за да се осигури максимална защита срещу атака или нарушение на цялата система.

▷ Агностичната архитектура – инсталацията на системата, с нейната компонентна архитектура, може да се извърши на всякаква операционна система.

▷ Моделът за мониторинг на КИМ да е без единична точка на отказ, системно-мрежов. С други думи, моделът за мониторинг е нужно да осигурява и анализира много възли за мониторинг на различните елементи и структури на мрежата. Повреда в един възел за мониторинг или възел с по-централизирана функционалност за управление не трябва да има забранителен ефект върху цялостната способност за мониторинг.

Ако има разпръсната мрежа с много точки на присъствие в различна инфраструктура или географски местоположения, всеки субконтинент на тази мрежа трябва да може да бъде наблюдаван, независимо от софтуерните или операционните изисквания на системата за мониторинг на мрежовата сигурност. Осигуряването на това ниво на гъвкавост позволява преодоляване на много често срещани проблеми и изисквания в съвременните внедрявания. Те могат да варират в зависимост от внедрената инфраструктура или инфраструктурата, която трябва да бъде наблюдавана.

Най-често срещаният проблем е внедряването на хардуер. Това изисква както физическа доставка, присъствие, така и хардуерна връзка на системата, което невинаги е възможно в информационните мрежи, когато работят в аварийен режим. Друг проблем за хардуерно базираните системи за мониторинг е, че те просто изискват физически персонал на място, за да се свържат, което в много случаи е или времево невъзможно, или финансово скъпо.

По този начин е възможно внедряване на система за мониторинг на мрежовата сигурност, която е независима от инфраструктурата и позволява преодоляване на проблема с физическото присъствие на хардуера и персонала. Друг важен аспект е лекотата на обучение на крайните потребители, анализаторите

по сигурността или ИТ управленския персонал, за да работят и внедряват системата, тъй като не се изисква специфична инфраструктура, което улеснява ад хос тестването, внедряването и инсталирането ѝ в повечето съвременни мрежи.

▷ Сигурност и защита на системата за мониторинг на сигурността на КИМ. Тя обикновено се състои от много функционални компоненти, като всеки компонент трябва да бъде изолиран и да може да гарантира собствения си обхват на сигурност. Пробив в генерираните данни за сигурност на компонента не трябва да дава достъп до управлението на системата. С други думи, пробив в един функционален компонент на системата не трябва да води до пробив или достъп до системата като цяло.

Формирането и създаването на такива иновативни системи за мониторинг на сигурността подобряват наличните отбранителни възможности за превантивни и оперативни стратегии за киберзащита. Такива системи може да бъдат проектирани, прототипирани и произведени (SELKS is now Clear NDR – Community 2025), особено като се има предвид наличието на съвременни софтуерни компоненти и езици за програмиране, като статично компилирани езици за общо предназначение, позволяващи създаването на един изпълним двоичен файл, който няма други софтуерни изисквания освен операционна система, налична за функциониране, тъй като той съдържа всички необходими компоненти за внедряване. По този начин се елиминират всякакви софтуерни нужди и изисквания, налични за операционната система.

ЗАКЛЮЧЕНИЕ

Изключително динамичното развитие на съвременните интелигентни технологии, комуникации и мрежи представя естествени предизвикателства пред операциите по сигурност в различните състояния на системите, като обучение на персонала и операторите в диапазона от нормален режим на работа на системата до аварийни ситуации, които изискват изключително бърза реакция и внедряване.

Необходими са иновативни превантивни и оперативни стратегии за киберзащита и отбрана на комуникационните и информационните мрежи в реално време, които разчитат на гъвкав и независим подход за мониторинг на сигурността, независимо от хардуера, операционната система, местоположението или управлението. Такива киберзащитни системи, благодарение на своята гъвкавост и сигурност на операциите, осигуряват необходимата стабилност на функциониране, спестяване на време за обучение, внедряване и експлоатация.

Независимостта от хардуера дава допълнителна възможност и предимство на системата за мониторинг на сигурността, работеща във всяка среда, тъй като тя може лесно да бъде инсталирана и управлявана на всякакъв хардуер от тип сървър с общо предназначение. Комбинирани, всички тези качества осигуряват ефективни, бързи и гъвкави възможности при справяне с предизвикателствата на съвременните информационно-комуникационни системи.

Благодарности: Тази публикация е финансирана от Министерството на образованието и науката в изпълнение на Национална научна програма „Сигурност и отбрана“, приета с ПМС № 731 от 21.10.2021 г., и съгласно Споразумение № Д01-74/19.05.2022 г.

ЛИТЕРАТУРА

- ДИРЕКТИВА (ЕС) 2022/2555. [viewed 05 March 2025]. Available from: https://www.nis-2-directive.com/NIS_2_Directive_Article_23.html
- CYBERSECURITY and Infrastructure Security Agency, May 2020. *Cybersecurity Framework Implementation Guidance*, p. 9. [viewed 05 March 2025]. Available from: https://www.cisa.gov/sites/default/files/publications/Commercial_Facilities_Sector_Cybersecurity_Framework_Implementation_Guidance_FINAL_508.pdf
- EUROPEAN Union Agency for Cybersecurity, September 2021. *Methodology for Sectoral Cybersecurity Assessments*, p. 13. [viewed 05 May 2025]. Available from: <https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20SCSA%20Methodology.pdf>
- NATIONAL Cyber Security Authority, June 2017. *Cyber Defence Methodology for an Organization*, p. 59. [viewed 02 March 2025]. Available from: https://www.gov.il/BlobFolder/policy/cyber_security_methodology_for_organizations/he/Cyber1.0_english_617_A4.pdf
- МАНЕВ, Е., 2016. Определение за сигурност – организационнокултурен подход. *Юридически сборник*, том XXIII, с. 262 – 274.
- МАНЕВ, Е., 2019. Зони и нива на сигурност – хипотези. *Сборник с доклади „Четвъртата промишлена революция и Балканите“*, кн. 36, серия „Юридически науки и обществена сигурност“, с. 7 – 13. ISSN 1313-7263
- МИТЕВ, Н.; ДЕНЧЕВ, С., 2023. Заплахи, уязвимости, рискове и инциденти с киберсигурността. *Сборник доклади от Национална научна конференция с международно участие „Сигурност и отбрана“*. София: За буквите – О писменехъ, 2023, с. 483 – 491. ISBN 978-619-185-593-3
- СЕМЕРДЖИЕВ, Цв.; МИТЕВ, Н., 2015. *Информационна сигурност*. София: Софттрейд, 315 с. ISBN 978-954-334-173-3
- ЗАКОН за киберсигурност. Обн. ДВ, бр. 94 от 13 ноември 2018 г., изм. ДВ, бр. 69 от 4 август 2020 г., изм. и доп. ДВ, бр. 85 от 2 октомври 2020 г., изм. и доп. ДВ, бр. 15 от 22 февруари 2022 г., изм. ДВ, бр. 25 от 29 март 2022 г. [viewed 09.04.2025]. Available from: <https://lex.bg/bg/mobile/ldoc/2137188253>
- ЕВРОПЕЙСКА сметна палата. *Предизвикателства пред ефективното прилагане на политиката за киберсигурност на ЕС*. Информационно-аналитичен документ, март 2019 г. [viewed 12.04.2025]. Available from: https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_BG.pdf
- ISO/IEC 27032:2012. *Information technology – Security techniques – Guidelines for cybersecurity*. [viewed 13 March 2025]. Available from: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en>

НАЦИОНАЛЕН институт за стандарти и технологии. *Информационно-аналитичен документ – речник*, март 2025 г. [viewed 11.04.2025]. Available from: <https://csrc.nist.gov/glossary/term/network>

ISO/IEC 27000:2018. *Information technology – Security techniques – Information security management systems – Overview and vocabulary*. [viewed 13 March 2025]. Available from: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en>

SELKS is now Clear NDR – Community. [viewed 07 March 2025]. Available from: <https://www.stamus-networks.com/clear-ndr-community>

ДИРЕКТИВА (ЕС) 2018/1972 на Европейския парламент и на Съвета от 11 декември 2018 г. за установяване на Европейски кодекс за електронни съобщения (преработена) (Текст от значение за ЕИП).

REFERENCES

DIREKTIVA (ES) 2022/2555. [viewed 05 March 2025]. Available from: https://www.nis-2-directive.com/NIS_2_Directive_Article_23.html

CYBERSECURITY and Infrastructure Security Agency, May 2020. *Cybersecurity Framework Implementation Guidance*, p. 9. [viewed 05 March 2025]. Available from: https://www.cisa.gov/sites/default/files/publications/Commercial_Facilities_Sector_Cybersecurity_Framework_Implementation_Guidance_FINAL_508.pdf

EUROPEAN Union Agency for Cybersecurity, September 2021. *Methodology for Sectoral Cybersecurity Assessments*, p. 13. [viewed 05 May 2025]. Available from: <https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20SCSA%20Methodology.pdf>

NATIONAL Cyber Security Authority, June 2017. *Cyber Defence Methodology for an Organization*, p. 59. [viewed 07 May 2025]. Available from: https://www.gov.il/BlobFolder/policy/cyber_security_methodology_for_organizations/he/Cyber1.0_english_617_A4.pdf

MANEV, E., 2016. Opređenje za sigurnost – organizacionnokulturen podhod. *Yuridicheski sbornik*, tom XXIII, s. 262 – 274.

MANEV, E., 2019. Zoni i niva na sigurnost – hipotezi. *Sbornik s dokladi „Chetvartata promishlena revolyutsia i Balkanite“*, kn. 36, seria „Yuridicheski nauki i obshtestvena sigurnost“, s. 7 – 13. ISSN 1313-7263

MITEV, Nikolay; DENChEV, Stoyan, 2023. Zaplahi, uyazvimosti, riskove i intsidenti s kibersigurnostta. *Sbornik dokladi ot Natsionalnata nauchna konferentsia s mezhdunarodno uchastie „Sigurnost i otbrana“*. Sofia: Za bukvite – O pismeneh, 2023, s. 483 – 491. ISBN 978-619-185-593-3

SEMERDZHIEV, Tsv.; MITEV, N., 2015. *Informatsionna sigurnost*. Sofia: Softtrejd, 315 s. ISBN 978-954-334-173-3

ZAKON za kibersigurnost. Obn. DV, br. 94 ot 13 noemvri 2018 g., izm. DV, br. 69 ot 4 avgust 2020 g., izm. i dop. DV, br. 85 ot 2 oktombri 2020 g., izm. i dop. DV, br. 15 ot 22 februar 2022 g., izm. DV, br. 25 ot 29 mart 2022 g. [viewed 09.04.2025]. Available from: <https://lex.bg/bg/mobile/ldoc/2137188253>

EVROPEYSKA smetna palata. *Predizvikatelstva pred efektivnoto prilagane na*

politikata za kibersigurnost na ES. Informatisionno-analitichen dokument, mart 2019 g. [viewed 12.04.2025]. Available from: https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_BG.pdf

ISO/IEC 27032:2012. *Information technology – Security techniques – Guidelines for cybersecurity*. [viewed 13 March 2025]. Available from: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en>

NATIONAL Institute of Standards and Technology. *Information analytics document – Glossary*. [viewed 13 March 2025]. Available from: <https://csrc.nist.gov/glossary/term/network>

ISO/IEC 27000:2018. *Information technology – Security techniques – Information security management systems – Overview and vocabulary*. [viewed 13 March 2025]. Available from: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en>

SELKS is now Clear NDR – Community. 2025. Available from: <https://www.stamus-networks.com/clear-ndr-community>

DIREKTIVA (ES) 2018/1972 na Evropeyskia parlament i na Saveta ot 11 dekemvri 2018 g. za ustanovyavane na Evropeyski kodeks za elektronni saobshtenia (prerabotena) (Tekst ot znachenie za EIP).

INNOVATIVE PREVENTIVE AND OPERATIONAL STRATEGIES FOR CYBER PROTECTION AND DEFENSE OF COMMUNICATION AND INFORMATION NETWORKS IN REAL TIME

Abstract: *In today's world, where network and IT devices are part of our daily lives, there is a wide variety of operating systems, vendors and users, which in turn introduces many points of unintended exposure to malicious and unwanted activities. Therefore, the diversity, structure and complexity of such unwanted attacks pose a serious challenge in terms of creating cyber protection measures and defense measures for many different and diverse infrastructures that are constantly evolving. There are many challenges to developing a unified protection strategy, and these challenges range from installation, hardware and infrastructure requirements to commercial and delivery specifics and the ability to properly train personnel.*

This report examines and summarizes a proposal for innovative preventive and operational strategies for cyber protection and defense of communication and information networks in real time, mainly by focusing on network security monitoring that is independent of operating systems and infrastructure, can be dispersed and at the same time has a containerized operation model, separated by core functionalities, to ensure maximum protection of the system itself. Based on the authors' practical experience in the cybersecurity industry in developing such systems, this is achievable by using innovative approaches to both the design and implementation itself, as well as training.

Keywords: *cyber defense; cyber strategy; information networks; operational strategies*

Petar Manev, IT Expert

ORCID ID: 0009-0007-7968-1716

University of Library Studies and Information Technologies

Sofia, Bulgaria

E-mail: petermanev@gmail.com