IT4Sec Reports 152
http://dx.doi.org/10.11610/it4sec.0152

Приложение на стратегически подход при противодействие срещу киберпрестъпността

Георги Видев, Бориславa Дойчинова, Ивана Гюрова, Виктория Събчева, Стефан Стефанов

Институт по информационни и комуникационни технологии – БАН
секция “Информационни технологии в сигурността”
www.IT4Sec.org

София, юли 2026

Георги Видев, Бориславa Дойчинова, Ивана Гюрова, Виктория Събчева, Стефан Стефанов, Приложение на стратегически подход при противодействие срещу киберпрестъпността**,** *IT4Sec Reports 152* (юли 2026), http://dx.doi.org/10.11610/it4sec.0152

IT4Sec Reports 152 „Приложение на стратегически подход при противодействие срещу киберпрестъпността". Киберсигурността отдавна даде да се разбере, че не може да бъде проблем и отговорност само на отделните потребители в киберпространството. Огромният брой потребители, различните нива на тяхното знание как да защитят своите активи, модерните технологии и подчертано международният характер на киберпрестъпленията правят неизбежна намесата на държавата по пътя на използване на стратегически подход. Дали обаче съществуват и какви могат да бъдат предизвикателствата пред създаване на една достатъчно ефективна стратегия за противодействие срещу киберпрестъпността? Целта на изследването, резултатите от което са представени в разработката, не е създаване на стратегически документ, а дискутиране и извеждане на основни характеристики на една стратегия за противодействие срещу киберпрестъпността. Авторите използват комбинация от теоретични знания, добри практики и собствени идеи в опита да намерят отговори на тези предизвикателства.

Ключови думи: киберпространство, киберсигурност, киберпрестъпност, стратегически подход, стратегия

IT4SecReports 152 "Application of a strategic approach to countering cybercrime". It has long been evident that cybersecurity cannot be solely the problem or responsibility of individual users in cyberspace. The vast number of users, the varying levels of knowledge regarding asset protection, modern technologies, and the distinctly international nature of cybercrime make state intervention—through a strategic approach—inevitable. However, what challenges arise in formulating a sufficiently effective strategy to counter cybercrime? The aim of the study presented here is not to draft a strategic document, but rather to discuss and outline the key characteristics of a cybercrime counter-strategy. The authors draw upon a combination of theoretical knowledge, best practices, and their own insights in an effort to address these challenges.

Keywords: cyberspace, cybersecurity, cybercrime, strategic approach, strategy

Редакционен съвет

Председател: акад. Кирил Боянов

Редактори: д-р Стоян Аврамов, проф. Генадий Агре, доц. Кирил Алексиев, проф. Даниела Борисова, проф. Венелин Георгиев, проф. Величка Милина, доц. Златогор Минчев, доц. Георги Павлов, проф. Тодор Тагарев, доц. Велизар Шаламанов

Отговорен редактор: Наталия Иванова

© Георги Видев, Бориславa Дойчинова, Ивана Гюрова, Виктория Събчева, Стефан Стефанов, 2026 г.

ISSN 1314-2119

ВЪВЕДЕНИЕ

Дискусиите в полето на киберсигурността могат да се развиват в различни посоки и на различни плоскости. Възможен вариант е дискусия по проблемите на противодействието срещу киберпрестъпността и приложимостта на стратегически подход в тази ключова за сигурността област. На тази база възниква въпросът доколко полезен и необходим е стратегическия подход когато се търси решение на проблемите с превенцията, разкриването, разследването, правоприлагането и международното сътрудничество при противодействието срещу един значим сектор на престъпността, какъвто е киберпрестъпността. Ако трябва да бъде посочен един основен аргумент за това трябва ли да се използва стратегически подход може да се оцени огромния брой на потребителите в киберпространството, всеки от които се явява потенциална жертва на киберпрестъпления и невъзможността да бъдат създадени и прилагани индивидуални стратегии за защита на всеки от тези потребители. На тази база може да се каже, че използването на стратегически подход при противодействието срещу киберпрестъпността не е само възможност, а необходимост и може единствен избор, даващ необходимата ефективност на това противодействие.[1]

На следващи място възниква въпросът какво представлява стратегията за противодействие срещу киберпрестъпността и какво включва технологията за нейното разработване. Световният опит показва, че една подобна стратегия се среща при не малък брой страни, които са оценили нейните предимства. Като стратегически документ тя може да бъде част от стратегията за киберсигурност, но може да има своята самостоятелност. Съществуват също така различни технологии за разработване на подобна стратегия. Възможен вариант за разработване на стратегия за противодействие срещу киберпрестъпността, който е избран за основа на изследването в настоящата публикация, включва последователно изследване и намиране на отговори на логически подредени и структурирани въпроси.

Защо е важно да бъде разработвана и прилагана стратегия за противодействие срещу киберпрестъпността?

Не са рядкост оценките за това, че киберпрестъпността представлява една от най-бързо развиващите се форми на международна престъпност, както и за това, че последствията от киберпрестъпността за значими и се реализират в различни социални и икономически области и аспекти. Причините за тези оценки са различни, сред които като пример разрастването на глобалната свързаност и големият брой международни киберпрестъпления, изискващи създаване и използване на стратегически способности за сътрудничество между отделните държави при разкриване, разследване и правоприлагане при киберпрестъпления. Други съществени характеристики на киберпрестъпленията, доказващи тяхната значимост са високата икономическа деструктивност, съпричастност към други видове престъпност, в това число и тероризъм и т.н.

- определяне на ролите и отговорностите на институциите в процедурите за противодействие срещу киберпрестъпленията;

[1] Изследванията в разработката са направени като част от научноизследователски проект „Актуални проблеми на сигурността в силно динамична и рискова среда“ към Лабораторията за стратегически изследвания на рисковете и сигурността на НБУ.

- постигане на достатъчно задълбочено разбиране на заплахите, уязвимостите и рисковете, водещи до киберпрестъпления;
- доказване на напредъка в противодействието срещу киберпрестъпността или разкриване на т.нар. „бели полета“ в плоскостта на това противодействие;
- повишава осведомеността на различните групи заинтересовани лица;
- осигурява рамка за превенция, разкриване и отговор на киберпрестъпността.

Кое прави трудно разработването и прилагането на достатъчно ефективна стратегия за противодействие срещу киберпрестъпността?

Разработването и прилагането на работеща стратегия за противодействие срещу киберпрестъпността е изправено пред редица трудности, имащи разнороден характер. Една част от тях имат локален характер и са свързани с културата и традициите на дадена държава, готовност на потребителите да следват подобни стратегически решения, капацитет на управляващите да използват стратегически подход към киберпрестъпността и т.н. Друга група трудности имат връзка с изучаването и разбирането на киберпрестъпността. Към тази група попада липсата на единно, общоприето определение за това какво представлява киберпрестъпността. Практиката показва, че при дефиниране на киберпрестъпността съществуват различни подходи. Един от често използваните подходи е чрез изброяване на деянията, които се определят като киберпрестъпления. Трета група трудности са свързани с особеностите на домейна, в рамките на който се извършват киберпрестъпленията. За киберпространството е характерно нарастващо ниво на глобална свързаност, от което като следствие се увеличава броя на потребителите в това пространството, съпроводено със снижаване на средното ниво за тяхната осведоменост и подготовка по въпросите за противодействие срещу киберпрестъпността. На следващи място може да се посочи разширяване на on-line процесите (в бизнеса, образованието, администрацията и т.н.) при използване на недостатъчно сигурни мрежи и недостатъчно подготвени потребители. Не са за пренебрегване причините, свързани с развитие на технологиите на изкуствения интелект, концепциите за „умни градове“, „умни домове“ и т.н. (IoT) което води увеличаване на повърхността от уязвимости и вектори за атака, използвани от киберпрестъпниците. Новите технологии водят до повишаване на комплесността и сложността на атаките от една страна на базата на нарастване на уменията, опита и мотивацията на киберпрестъпниците и от друга страна за сметка на разширяване на кръга на киберпрестъпниците, една част от които са облекчени откъм необходимост за притежаване на специфични знания. Четвъртата група трудности пред използване на стратегическия подход при противодействието срещу киберпрестъпността е свързана с нормативни особености. Тук попадат съществуващите проблеми при докладване на киберпрестъпленията и недостатъчен капацитет за тяхното разкриване и разследване; съществуващи проблеми при законодателството и юрисдикцията, особено при киберпрестъпления с международен характер и т.н.

Как да бъде формулирана целта пред стратегията за противодействие срещу киберпрестъпността?

Целта пред една стратегия за противодействие срещу киберпрестъпността следва да бъде достатъчно комплексна и изчерпателна. В тази връзка същата може да бъде формулирана в няколко направления:

- гарантиране на националната киберсигурност, чрез защита на критичната информационна инфраструктура, държавните информационни системи, критични сектори и цифровите активи на Република България от злонамерени действия в киберпространството;
- повишаване на киберустойчивостта по пътя на изграждане на институционален, технически и оперативен капацитет за превенция, ранно предупреждение, реакция, съхранение на информация и възстановяване след киберинциденти;
- осигуряване на достатъчно ефективна правна и регулаторна рамка чрез хармонизиране на националното законодателство с изискванията на NIS2, Акта за киберсигурност на ЕС (EU Cybersecurity Act) и другите приложими европейски регулации и добри практики както и допълнение и подобрения в наказателния кодекс;
- развитие на киберкултура и кадрови потенциал с възможности за насърчаване на осведомеността по киберсигурност сред широката общественост и училищата;
- разширяване на мащаба и повишаване на ефективността на международното сътрудничество чрез инициативи за задълбочаване на партньорството в рамките на НАТО, ЕС и двустранните отношения в полето на колективната киберзащита.

Какъв да бъде обхватът на стратегията предвид многообразието от киберпрестъпления?

Практическата полза от една стратегия за противодействие срещу киберпрестъпността в значителна степен зависи от нейния обхват. Измерители за този обхват могат да бъдат търсени в различни направления.

На първо място следва да се определи обхвата по отношение на престъпленията, които попадат в класификацията на киберпрестъпленията като част от общия мащаб на престъпленията, за които се цели противодействие. Като цяло, в българския Наказателен кодекс, съгласно член девети от глава втора, престъплението представлява обществено опасно деяние (действие или бездействие), извършено виновно и обявено от закона за наказуемо. За дигиталната среда, киберпрестъпността се дефинира като съвкупност от действия и поведения в киберпространството, които противоречат на установените законови норми. Киберпрестъпността може да бъде разглеждана в рамките на различни модели за класифициране, като пример моделът на Furnell от 2001 г. или моделът на Gordon и Ford от 2006 г. Тези модели използват различни критерии за класифициране на киберпрестъпленията:

- активни киберпрестъпления (като пример, неправомерен достъп до защитена среда) и пасивни киберпрестъпления (при които компютърът е средство, подпомагащо незаконна дейност);

- компютърът като цел (мишена), разработване и разпространение на зловреден софтуер (вируси), DDoS атаки (отказ на услуга), нерегламентирано модифициране или изтриване на информация.;
- компютърът като средство (дигиталните технологии като помощно средство за извършване на различни киберпрестъпления като финансови или крипто измами, фишинг и др.)
- компютърът без съществена роля в киберпрестъплението;
- разпространение на пиратски софтуер и т.н.

Възможен подход при определяне на обхвата на стратегията за противодействие срещу киберпрестъпността е изброяване на покриваните видове киберпрестъпления:

- неправомерен достъп (хакерство), което включва проникване в дигитални системи, нерегламентирана промяна или унищожаване на файлове и информация, кражба и злоупотреба с лична информация.
- информационен шпионаж, представляващ следващата стъпка след неправомерния достъп, която включва придобиването и използването на информация, защитена по определен ред или до която интернет потребителите нямат законен достъп;
- спам, разбира като изпращане на съобщения, имейли, SMS или друг тип дигитална комуникация, която има най-често търговска цел, но може също така да бъде свързана със злонамерени действия;
- разпространение на материали, съдържащи детска порнография, включващо създаване, разпространение, предлагане, притежание и всички свързани дейности с материали, изобразяващи сексуално насилие върху деца.

От начина, по който се определя обхвата на стратегията зависят резултатите от измерването на мащабите на киберпрестъпността. По статистика на Евростат [2] за 2025 година, България е една от европейските страни с най-нисък дял на населението (38%), което притежава основни дигитални умения. Този показател играе важна роля при формирането и измерването на мащабите на киберпрестъпността, защото предразполага и за по-голям процент жертви на кибератаки. Според проучване на Mediapool [3] за 2023 година, 70% от българските компании са били подложени на кибератаки със злонамерен софтуер. Най-честите престъпления са: фишинг атаки - 47%; злонамерен софтуер - 17%; атаки с вируси - 12%; кражба на идентичност - 10%.

В рамките на Европейския съюз, ransomware атаките остават водеща заплаха за бизнеса по статистика на Агенцията на Европейския съюз за киберсигурност (ENISA), чийто доклад за 2025 година[4] показва, че 81% от кибератаките са от такъв тип. Малките компании са най-голямата таргет група на киберпрестъпниците, защото създаването и развитието на дигитална система за сигурност е задача, която много често е финансово непосилна за работодателите.

---

[2] Digitalisation in Europe – 2025 edition, https://ec.europa.eu/eurostat/web/interactive-publications/digitalisation-2025

[3] Дара Сапунджиева (2023) - 70% от българските компании са били подложени на кибератаки със зловреден софтуер https://www.mediapool.bg/70-ot-balgarskite-kompanii-sa-bili-podlozheni-na-kiberataki-sas-zlovreden-softuer-news352903.html

[4] ENISA (European Union Agency for Cybersecurity) Thread Landscape (2025) https://www.enisa.europa.eu/sites/default/files/2025-10/ENISA%20Threat%20Landscape%202025%20Booklet.pdf

На следващи място обхватът на стратегията за противодействие срещу киберпрестъпността се определя на базата на ангажираните субекти и институции.

Като обща констатация може да се каже, че България не разполага с добре изградена и развита система за взаимодействие между институциите, занимаващи се с противодействието срещу киберпрестъпността. Като институции с ангажименти в областта на стратегията могат да бъда посочени Съветът за киберсигурност към Министерски съвет, Секторните екипи за реагиране на инциденти (CERT); Национален екип за реагиране при инциденти с компютърната сигурност; Главна дирекция "Борба с организираната престъпност" (ГДБОП) - Отдел "Киберпрестъпност", играещо ролята на оперативно звено на МВР за разкриване и разследване на киберпрестъпления; Държавна агенция „Технически операции" (ДАТО), специализирана при прилагане на специални разузнавателни средства; Национален институт по криминалистика към МВР, занимаващ се с изследвания в областта на криминалистиката и веществените доказателства.

Мащабът на една стратегия за противодействие срещу киберпрестъпността зависи от нормативната база, върху която тя се изгражда и прилага

От гледна точка на националната законодателна система като пример за подоблни документи могат да бъдат посочени:

- Закон за киберсигурност, приет през 2018 година, целящ да уреди дейностите по организацията, контрола и другите процеси, свързани с киберсигурността и киберпрестъпленията.
- Глава девета „а" от Наказателния кодекс на Република България "Компютърни престъпления - чл. 319а - 319е, инкриминираща престъпления, свързани с нерегламентиран достъп (хакерство), заразяване на устройства със злонамерен софтуер и финансови измами.
- Закон за защита на личните данни (ЗЗЛД), касаещ защитата на правата на физическите лица при обработването на личните им данни.
- Закон за защита на класифицираната информация (ЗЗКИ), който има за цел да подобри защитата и управлението на класифицираната информация.

Разширявайки мащаба, като примери за документи в областта на стратегията, влизащи в европейската законова рамка могат да бъдат посочени:

- Конвенция за киберпрестъпност на Съвета на Европа (Будапещенска конвенция), в сила от 2004 година, задължаваща европейските държави да криминализират определени киберпрестъпления като детска порнография, незаконен достъп, шпионаж, измами и др. България е подписала конвенцията през 2005 година.
- Общ регламент относно защитата на данните (GDPR), в сила от 2018 година, имащ за цел унифициране на правилата за боравене с лични данни и тяхното използване в дигиталното пространство.
- Директива 2013/40/ЕС, свързана с кибератаките срещу информационни системи и тяхното значение и засилваща се опасност на ниво ЕС и глобално.
- Директива (ЕС) 2022/2555 (NIS2), представляваща рамка, която има за цел да развие мерките за киберсигурност и управлението на риска.

До каква дълбочина за бъде анализа на моментното състояние на противодействието срещу киберпрестъпността?

За да бъдат адекватни и успешни стратегическите решения в полето на противодействието срещу киберпрестъпността, същите следва да се основават на достатъчно задълбочен анализ на външната и вътрешната среда, в която стратегията се прилага. Подобен анализ дава възможност да бъдат определени основните проблемни области, необходимите стратегически цели и оперативни дейности на базата на влиянието на съвкупност от фактори. Като инструменти на тези анализи се използват два от широко прилаганите методи - SWOT и PESTLE анализ, които позволяват да бъдат идентифицирани основните силни и слаби страни на съществуващата система, външните възможности и заплахи, които влияят върху способността за противодействие срещу киберпрестъпността, както и влиянието на различни групи от фактори на външната среда.

Резултатите от извършения SWOT анализ могат да бъдат представени по следния начин:

Силни страни (Strengths)

- членството на България в ЕС и НАТО осигурява възможности за международно сътрудничество, обмен на информация и добри практики;
- наличие на нормативна база, свързана с киберсигурността и киберпрестъпленията;
- изградени са специализирани структури като ГДБОП, CERT България и секторни екипи за реагиране при инциденти;
- нараства интересът към обучението и развитието на специалисти в областта на киберсигурността;
- все повече организации започват да инвестират в мерки за защита на информационните си системи

Слаби страни (Weaknesses)

- недостатъчна осведоменост и дигитална култура сред голяма част от населението;
- липса на достатъчно квалифицирани кадри и експерти в областта на киберсигурността и дигиталните разследвания;
- недостатъчна степен на координация между отделните заинтересовани институции;
- остарели информационни системи и технологии в част от държавните администрации;
- недостатъчно ефективно законодателство при някои видове киберпрестъпления;
- ниско ниво на киберсигурност при малките и средните предприятия;
- недостатъчно развити канали и възможности за докладване на киберинциденти и киберпрестъпления.

Възможности (Opportunities)

- по-нататъшно развитие на обучения и програми за киберосведоменост;
- използване на изкуствен интелект за откриване и анализ на киберзаплахи, както и разкриване и разследване на киберпрестъпления;

- използване на европейско финансиране на програми за киберсигурност и участие в международни проекти;
- развитие на публично-частни партньорства в проблеми области;
- усъвършенстване на законодателството и адаптирането му към новите видове престъпления;
- създаване и развитие на специализирани програми за обучение в училища и университети.

Заплахи (Threats)

- нарастване на броя и сложността на ransomware, phishing и AI-базирани атаки;
- преобладаващ трансграничен характер на киберпрестъпността;
- развитие на deepfake технологии и дезинформация;
- атаки срещу критична инфраструктура и държавни институции;
- изтичане на чувствителни лични и финансови данни;
- използване на криптовалути за прикриване на престъпна дейност.

На базата на резултатите от анализа на вътрешната среда може да се обобщи, че България разполага с базова институционална и нормативна рамка за противодействие срещу киберпрестъпността, но съществуват сериозни затруднения при нейното практическо прилагане и развитие.

Наблюдава се значително изоставане по отношение на дигиталната култура, подготовката на потребителите и наличието на достатъчно квалифицирани специалисти. В голяма част от случаите човешкият фактор остава основна предпоставка за успешното реализиране на киберпрестъпления, особено при ransomware и атаки чрез социално инженерство.

Успоредно с това, бързото развитие на технологиите, изкуствения интелект и трансграничния характер на киберпрестъпността поставят сериозни предизвикателства пред съществуващото законодателство и способностите на институциите за ефективно разследване и правоприлагане.

Всичко това показва необходимостта стратегията да бъде насочена приоритетно към:

- повишаване на киберосведомеността и обучението;
- изграждане на устойчив кадрови капацитет;
- модернизиране и адаптиране на законовата рамка към новите видове киберпрестъпления;
- подобряване на координацията между заинтересованите институции.

Анализът на влиянието на фактори от външната среда върху способностите за противодействие срещу киберпрестъпността се извършва в следните основни области:

Политически фактори (Political)

- налице е нарастваща необходимост от национални политики за противодействие срещу киберпрестъпността;
- от решаващо значение е засилването международно сътрудничество в рамките на ЕС и НАТО;

- ясно видима е необходимостта от повишена координация между институциите.

Икономически фактори (Economic)

- ежегодно се отчитат значителни финансови загуби вследствие на киберизмами и ransomware атаки;
- като недостатъчни се оценяват инвестициите в киберсигурност при малките и средните фирми;
- осезаем недостиг на квалифицирани специалисти по киберсигурност на пазара на труда.

Социални фактори (Social)

- ниско ниво на дигитална грамотност и недостатъчна осведоменост на различните групи потребители в киберпространството;
- повишена зависимост на различните социални дейности от дигитални услуги и социални мрежи;
- повишен до неприемливи нива риск от социално инженерство и онлайн измами.

Технологични фактори (Technological)

- бързо развитие на AI технологии и автоматизирани атаки, които разширяват плоскостта на заплахите и възможните атаки.
- разпространение на cloud услуги и IoT устройства.
- нарастване на степента на сложност, комплексност и скорост за реализиране на кибератаките.

Правни фактори (Legal)

- необходимост от актуализиране и допълване на законодателството;
- търсене на достатъчно ефективни начини за решаване на проблеми с международната юрисдикция при трансгранични престъпления;
- необходимост от механизми за по-бързо адаптиране на националното законодателство към европейските регулации.

Екологични фактори (Environmental)

- засилена зависимост на критичната инфраструктура от дигитални системи и тяхната сигурност;
- завишени нива на риск от кибератаки срещу различни сектори на критичната инфраструктура, каквито са енергетиката, транспорта и здравеопазването;
- търсена от потребителите устойчивост и непрекъсваемост на услугите, използващи информационни системи, мрежи и технологии.

Резултатите от PESTLE анализа показват, че противодействието срещу киберпрестъпността е силно повлияно от бързо променящата се международна и технологична среда. Нарастващата дигитализация, развитието на изкуствения интелект и увеличаващата се зависимост от онлайн услуги създават нови възможности за киберпрестъпниците и затрудняват институциите при разкриването, разследването и превенцията на престъпленията. В същото време ниската дигитална грамотност и недостатъчната подготовка на потребителите създават предпоставки за успешното реализиране на phishing атаки, онлайн измами и атаки чрез социално инженерство. Сериозно предизвикателство представлява и

необходимостта от по-гъвкава и модерна законодателна рамка, която да може своевременно да отговаря на развитието на новите технологии и появата на нови форми на киберпрестъпност.

Резултатите от SWOT и PESTLE анализите показват, че основните предизвикателства пред противодействието срещу киберпрестъпността в България са свързани не само с технологичните рискове, но и с недостатъчната подготовка на обществото, бизнеса и институциите. Липсата на киберкултура, ограничените обучения и недостигът на квалифицирани кадри създават условия за повишаване на броя и мащаба на киберпрестъпленията. Наред с това се наблюдава необходимост от по-гъвкаво и модерно законодателство, способно да отговори на динамично развиващите се технологии и новите форми на киберпрестъпност.

Като извод следва факта, че основните проблемни области по отношение на противодействието срещу киберпрестъпността са свързани с информираността и обучението на потребителите, както и с ефективността на законодателната рамка, регламентираща това противодействие в полето на материалното и процесуалното наказателно право.

Как да изглежда бъдещото състояние на противодействието срещу киберпрестъпността и визия за неговото достигане?

Свързаността, която днес предоставят дигиталните технологии, е довела до толкова изменения в ежедневието на потребителите, че огромен набор от социалните и икономическите процеси оперират основно в киберпространството. Това води, от една страна, до изключително много възможности за развитие във всички обществени сфери, но от друга страна създава сериозни рискове от киберпрестъпност на национално и международно ниво.

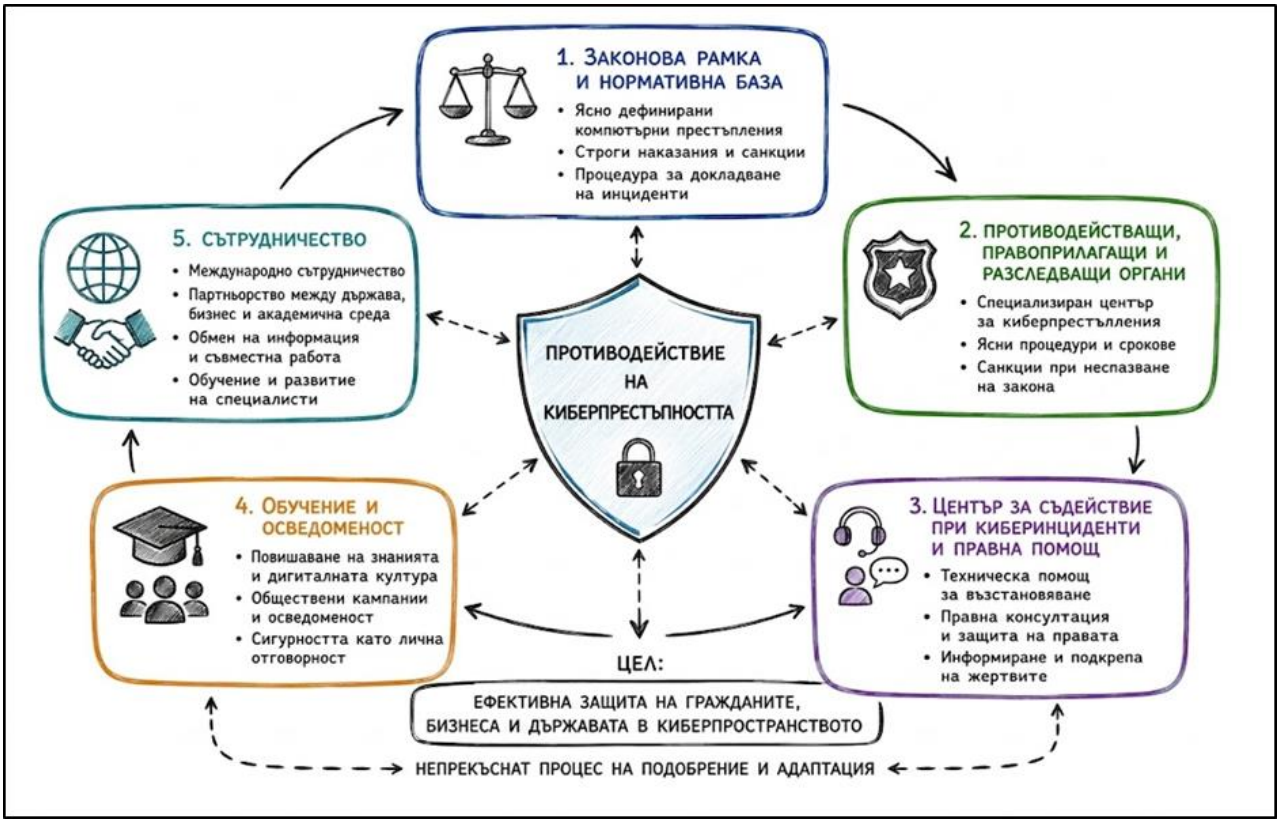
В тази насока, в следващите години България трябва да постигне киберустойчивост чрез надеждна и сигурна мрежова инфраструктура с висока наличност, която да отключи пълния потенциал на технологиите, като гарантира интегритета и конфиденциалността на данните, предавани по интернет мрежата както и личната неприкосновеност на гражданите.

Постигането на тази визия в перспектива е осъществимо и изисква стратегически и управленски подход, фокусиран върху актуализация на законодателната рамка и развитието и регулярното обучение. Този процес следва да бъде изграден в тясно сътрудничество на международно ниво и в синхрон междудържавни институции, бизнес и академична общност.

Развитието на противодействието срещу киберпрестъпността в бъдеще следва да засегне и изгради следните ключови компоненти (виж фиг. 1):

- законова рамка и нормативна база, в която следва ясно и без двусмислие да бъдат установени и разписани всички компютърни престъпления, така че да няма възможност дадено компютърно престъпление да остане извън обхвата на закона. Същевременно, предвидените наказания и санкция да бъдат достатъчно значими, че потенциалните ползи да бъдат в пъти по-малки от последствията от извършеното престъпление, което да действа като възпиращ фактор и да демотивира потенциалните извършители. Важна част представлява и включването на ясна процедура по докладване на инциденти, свързани с киберпространството.

- повишаване на капацитета на противодействащи, правоприлагащи и разследващи органи, в това число създаване на специализиран център за обработване на случаи, чиято дейност да е насочена към борбата с киберпрестъпленията, извършени от организирани групи или отделни лица. Тези органи следва да стъпят на ясните процедури, конкретните времеви периоди и изричните изисквания, зададени в закона. В допълнение, санкциите при неспазване на утвърдените закони за докладване на инциденти да бъдат съизмерими с конкретните субекти и техните организационни обороти.



Фиг. 1. Примерна взаимовръзка между основните компоненти на визията за изграждането на ефективно противодейства срещу киберпрестъпността

- създаване на Център за съдействие при киберинциденти и правна помощ, занимаващ се със съдействие и правна помощ за жертвите, имащ за цел да минимизира щетите от киберпрестъпленията и да информира жертвите от подобни деяния. Центърът трябва да предоставя както експертна техническа подкрепа за възстановяване на дигитални активи, така и специализирана правна консултация относно правата на засегнатите субекти в киберсредата.
- обучение и осведоменост в полето на противодействието срещу киберпрестъпността с особено внимание върху социалното инженерство. Това позволява да се прилагат както експериментални методи, така и иновации за повишаване на осведомеността в личен и обществен план. Провеждането на регулярни обществени кампании за киберсигурност би довело до такова ниво на осведоменост, че сигурността да бъде възприета като персонална отговорност.

- в сферата на сътрудничеството следва да се преследва визията за това, че нито една държава, в това число и нито една компания, не би могла сама да се справи с предизвикателствата в киберпространството. Затова е много важно международното сътрудничество и пряката взаимопомощ между държавата, бизнеса и академичната среда. Такова партньорство би донесло големи ползи, свързани с обмена на информация и съвместната работа по киберслучаи. Същевременно не бива да се подценява и обучението на специалисти в сферата, които да отговорят на предизвикателствата пред противодействието срещу киберпрестъпления. Специалистите трябва да бъдат поощрявани и лесно да могат да се реализират в държавни или частни компании. Тяхното развитие следва да бъде поставено на първо място и за това могат да се използват инструменти като стимулиране и поощряване..

За да бъде една стратегия за противодействие срещу киберпрестъпността устойчива и ефективна във времето, същата трябва да се основава на следните принципи:

- осигуряване на свободен и равен достъп до интернет;
- защита на основните права и свободи на хората онлайн и неприкосновеността на личния живот;
- неделимост на киберсигурността от националната и международната сигурност;
- съгласуваност между ангажиментите и принципите на сътрудничеството и взаимодействието с други държави;
- активно участие в създаването на общ капацитет и способности;
- откритост, прозрачност и споделена отговорност;
- ефективно използване на опита и добрите практики;
- непрекъснат процес по подобрение, адаптация и контрол;
- използване на метрики за измерване на ефективността на резултатите от прилагане на стратегията.

Реализацията на описаната визия следва да бъде национален ангажимент в следващите години на дигитално развитие на страната. С помощта на целенасочени усилия в полето на законодателството, обучението, активното сътрудничество и непрекъснатото подобрение е възможно да се изгради киберпространство, което да стимулира иновациите, подкрепя развитието и гарантира спокойствието на гражданите и бизнеса.

Кой да бъдат главните области, стратегическите цели и оперативните дейности в стратегията за противодействие срещу киберпрестъпността?

На базата на резултатите от SWOT и PESTLE анализите са изведени две основни проблеми области, които пряко оказват влияние върху способностите за ефективно противодействие върху киберпрестъпността. В основата на тези области стоят проблеми, свързани с подготовката на потребителите, нивото на тяхната осведоменост, адаптацията на законодателството към новите престъпления и координацията между институциите в национален и международен аспект. Нарастващият брой кибератаки, използването на изкуствен интелект и

трансграничният характер на киберпрестъпността налагат изграждане на устойчив стратегически модел в изведените две области.

Област 1. Развитие на обучението, осведомеността и кадровия капацитет

Една от най-значимите слабости в българската среда за киберсигурност е недостатъчната и незадълбочена подготовка както на обикновените потребители, така и на част от институциите и бизнеса по отношение на съвременните киберзаплахи. Голяма част от киберинцидентите са вследствие на човешка грешка, липса на подготовка и познания относно рисковете в дигитална среда. Съществува и сериозен недостиг на квалифицирани специалисти по киберсигурност, дигитална криминалистика и разследване на киберпрестъпления. Това поражда затруднения както за превенцията и защитата, така и за разследването и правоприлагането при случаи на киберпрестъпност. Ограниченото присъствие на специализирано обучение по киберсигурност в училищата, университетите и програмите за професионална квалификация също представлява допълнителен проблем. Поради тези причини изграждането на устойчива система за обучение, повишаване на киберосведомеността и развитието на кадровия потенциал се определя като едно от основните стратегически решения.

Област 2 Усъвършенстване на законодателната и регулаторната рамка

Развитието на дигиталните технологии и динамичното изменение на киберзаплахите поставят сериозни предизвикателства пред националното законодателство. Действащите нормативни актове се оказват недостатъчно адаптирани към съвременните форми на киберпрестъпност. Налични са затруднения при процесите по събиране, анализ и използване на електронни доказателства, както и при координацията между различните институции, които са ангажирани с противодействието срещу киберпрестъпността. Необходимостта от по-бързо адаптиране към европейските регулации и международните стандарти изисква създаването на по-гъвкава и модерна нормативна рамка. Хармонизирането на българското законодателства с изискванията на NIS2, GDPR и останалите европейски механизми за защита на информационните системи е от ключово значение. Усъвършенстването на законодателството и регулаторната среда се определя като ключова стратегическа област за повишаване на ефективността при противодействие срещу киберпрестъпността.

Подобряване на способностите за противодействие срещу киберпрестъпността в посочените по-горе две проблемни области изисква формулиране на конкретни стратегически цели, които да осигурят устойчиво развитие на националната система за киберсигурност. Тези цели могат да бъдат определени по следния начин:

Стратегически цели за главната област 1 „Развитие на обучението, осведомеността и кадровия капацитет“:

- развитие на партньорствата между държавните институции, академични среди и частния сектор по отношение на обмен на знания, добри практики и технологии;
- повишаване на нивото на киберосведоменост сред населението, държавната администрация и бизнеса чрез достатъчно ефективни форми за обучения, информационни кампании и практически насоки за безопасност в дигиталната среда;

- изграждане на устойчив кадрови капацитет от специалисти по киберсигурност, дигитални разследвания и защита на информационните системи;
- интегриране на обучението по киберсигурност в училищното и университетското образование чрез специализирани програми и практически лабораторни занятия.

Стратегически цели за главната област 2 „Усъвършенстване на законодателната и регулаторната рамка“:

- хармонизиране на националната нормативна база с европейските и между- родните стандарти и регулации;
- актуализиране на националното законодателство спрямо съвременните форми на киберпрестъпност и технологични заплахи;
- повишаване на ефективността на координацията между институциите в национален и международен мащаб;
- подобряване на механизмите за разследване и събиране на електронни доказателства.

Постигането на формулираните стратегически цели изисква определяне и изпълнение на конкретни оперативни дейности, структурирани в три нива с постепенно нарастваща степен на сложност.

Оперативни дейности за главна област 1. „Развитие на обучението, осведомеността и кадровия капацитет“ [5]

Таблица 1. Обобщение на оперативните дейности за основна област 1 „Развитие на обучението, осведомеността и кадровия капацитет“

Ниво	Насоченост	Очакван резултат	Срок до:	Изпълнител	Контр. орган
1	Повишаване на базовата осведоменост сред населението и бизнеса	Изградена базова култура и намаляване на рисковете, породени от човешка грешка	12 м.	МЕУ, МОН, CERT	Министерски съвет
2	Изграждане на експертен капацитет и практически способности за реакция	Повишаване броя на подготвените специалисти и подобряване на междуинституционалната координация	36 м.	МОН, университети, ГДБОП, МЕУ	Съвет по киберсигурност
3	Създаване на устойчива система за подготовка и международно сътрудничество	Изградена национална система за развитие и сертифициране на експерти по киберсигурност	48 м.	МОН, МЕУ, научни и бизнес организации	Министерски съвет и Съвета по киберсигурност

Ниво 1. Основно организационно и обучително изграждане

[5] Виж таблица 1

На първо място усилията следва да бъдат насочени към изграждане на киберхигиена, базова култура, свързана с киберсигурността и повишаване на информираността сред населението и администрацията. Предвижда се организиране на национални информационни кампании относно основните видове киберзаплахи. Ще бъдат разработени базови обучения за държавната администрация и служителите в критичните сектори, като е за цел повишаването на уменията за разпознаване и предотвратяване на киберинциденти. Срокът за изпълнение на тези дейности е до 12 месеца, като за основни метрики за оценка на успеха ще бъдат броят проведени обучения, обучените служители и нивото на обществена информираност. Изпълнението дейностите от това ниво се възлага на Министерството на образованието и науката, Министерството на електронното управление, CERT. Контролиращият орган е Министерски съвет.

Ниво 2. Развитие на специализирани способности

На второ ниво се предвижда създаването на устойчиви образователни и професионални механизми за подготовка на специалисти по киберсигурност. Ще бъдат разработени специализирани програми в университетите и гимназиите, както и националните центрове за обучение и симулации на киберинциденти. Това ще се постигне посредством организиране на практически кибер обучения и симулации между държавните институции, бизнеса и академичните среди. Срокът за изпълнение е до 36 месеца, а успехът ще се измерва чрез броя на новосъздадените програми, обучени специалисти и проведени учения. Изпълнение: Министерството на образованието и науката, Министерството на електронното управление, университети, ГДБОП, CERT. Контролиращ орган: Съвет по киберсигурност.

Ниво 3. Дългосрочно устойчиво развитие

На трето място стратегията предвижда изграждането на дългосрочна национална система за развитие на експертен капацитет. Ще бъдат създадени програми за сертифициране на специалисти и киберсигурност, специализирани кибер лаборатории и центрове за научноизследователска дейност. Насърчаване на развитието на публично-частни партньорства с международни организации и технологични компании, което цели внедряване на нови технологии и обмен на експертиза. До 48 месеца е срокът за изпълнение. Основни показатели за успехът са броят на сертифицираните специалисти, международни партньорства и изградени лаборатории. Изпълнение: Министерството на образованието и науката, Министерството на електронното управление, университети, бизнес организации. Контролиращ орган: Съвет по киберсигурност, Министерски съвет.

Оперативни дейности за главна област 2. „Усъвършенстване на законодателната и регулаторната рамка“[6]

Ниво 1. Анализ и идентифициране на законодателни пропуски

Първото ниво включва извършване на цялостен анализ на действащата нормативна уредба, свързана с киберсигурността и киберпрестъпността. Това включва идентифициране на слабостите в Наказателния кодекс, Закона за киберсигурност и процедурите по събиране на електронни доказателства. Срокът за изпълнение е до 12 месеца. Резултатът ще бъде изготвянето на официален доклад с предложения за нормативни промени. Изпълнение: Министерство на правосъдието, МВР, прокуратурата. Контролиращ орган: Народно събрание.

[6] Виж таблица 2

Ниво 2. Актуализация и хармонизация на нормативната база

Предвижда се подготовка и приемане на законодателни изменения, които са свързани с новите форми на киберпрестъпност и европейски регулации. Акцентът ще бъде поставен върху транспонирането на NIS2, подобряване на процедурите за международен обмен на информация и създаване на стандарти за работа с електронни доказателства. Изпълнението е до 36 месеца. Успехът ще се измерва чрез броя на приети нормативни промени и нивото на съответствие с европейските стандарти. Изпълнение: Министерството на правосъдието, Министерството на електронното управление, Министерството на вътрешните работи и Министерството на външните работи. Контролиращ орган: Народно събрание и Висшия съдебен съвет.

Таблица 2. Обобщение на оперативните дейности за основна област 2 „Усъвършенстване на законодателната и регулаторната рамка“

Ниво	Насоченост	Очакван резултат	Срок до:	Изпълнител	Контр. орган
1	Анализ на действащата нормативна база и установяване на пропуски	Изготвени предложения за подобряване на законодателството	12 м.	МП, МВР, прокуратура	Народно събрание
2	Хармонизиране с европейските регулации и подобряване на механизмите за разследване	Подобрена нормативна рамка и по-ефективно противодействие срещу киберпрестъпност	36 м.	МП, МЕУ, МВР, МВнР	Народно събрание и ВСС
3	Изграждане на механизми за постоянна адаптация към новите киберзаплахи	Създадена устойчива система за актуализация на законодателството и институционална координация	48 м.	МП, МВР, ВСС, МЕУ	Министерски съвет и Съвета по киберсигурност

Ниво 3. Изграждане на устойчива правна и институционална среда

На трето ниво предвижда изграждане на устойчив механизъм за периодична актуализация на законодателството и специализация на институциите. Ще бъдат разработени програми за обучение и механизми за постоянен мониторинг на рисковете и тяхното отражение върху нормативната рамка. До 48 месеца е срокът за изпълнение, като успехът ще се измерва чрез повишаване ефективността на разследванията, намаляване на времето за обработка на случаи и подобряване на международното сътрудничество. Изпълнение: Министерството на правосъдието, Министерството на вътрешните работи, Висшия съдебен съвет и Министерството на електронното управление. Контролиращ орган: Министерския съвет и Съвета по киберсигурност.

ЗАКЛЮЧЕНИЕ

Направеното изследване позволява да бъдат направени изводи в няколко направления. Стратегията за противодействие срещу киберпрестъпността действително се оказва инструмент с големи възможности, но ефективността на този инструмент зависи от качествата на създадения документ. Това се оказва не толкова лесен въпрос на базата на посочените в разработката аргументи.

Избраната технология за дискусия по стратегическите проблеми на противодействието срещу киберпрестъпността на базата на търсене на отговори на логически структурирани въпроси предоставя възможности за креативност и комбиниране на теоретични знания, добри практики и нови идеи на анализаторите.

В крайна сметка целта пред изследването е постигната чрез извеждане на основните характеристики на една стратегия за противодействие срещу киберпрестъпността.

ИЗПОЛЗВАНА ЛИТЕРАТУРА

[1] Digitalisation in Europe – 2025 edition, https://ec.europa.eu/eurostat/web/interactive-publications/digitalisation-2025

[2] Дара Сапунджиева (2023) - 70% от българските компании са били подложени на кибератаки със зловреден софтуер https://www.mediapool.bg/70-ot-balgarskite-kompanii-sa-bili-podlozheni-na-kiberataki-sas-zlovreden-softuer-news352903.html

[3] ENISA (European Union Agency for Cybersecurity) Thread Landscape (2025) https://www.enisa.europa.eu/sites/default/files/2025-10/ENISA%20Threat%20Landscape%202025%20Booklet.pdf

[4] https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

[5] https://insight.scmagazineuk.com/dwell-time-reduced-further-as-attackers-infect-in-four-hours

[6] https://www.strategy.bg/bg/public-consultations/10433

[7] https://specopssoft.com/blog/european-countries-cyber-crime/

[8] https://www.segabg.com/hot/category-bulgaria/200-firmi-sa-zagubili-nad-20-mln-evro-sled-kiberizmami

[9] https://e-security.bg/zhiznenovazhni-danni-za-sigurnostta-prez-2024-g/

[10] https://www.svobodnaevropa.bg/a/30057714.html