IT4Sec Reports 149
https://doi.org/10.11610/it4sec.0149

СТРАТЕГИЯ ЗА ПРОТИВОДЕЙСТВИЕ СРЕЩУ КИБЕРПРЕСТЪПНОСТТА

(примерен модел)

Гергана Антонова, Ния Присадашка, Радослав Димитров,
Йоан Йонков, Даниел Радев, Христо Павлов,
Марио Младенов, Илиан Григоров

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

София, октомври 2023

Гергана Антонова, Ния Присадашка, Радослав Димитров, Йоан Йонков, Даниел Радев, Христо Павлов, Марио Младенов, Илиан Григоров, Стратегия за противодействие срещу киберпрестъпността (примерен модел)**,** *IT4Sec Reports 149* (октомври 2023), https://doi.org/10.11610/it4sec.0149

IT4Sec Reports 149 „Стратегия за противодействие срещу киберпрестъпността (примерен модел)“. Навлизането на технологиите и мрежите в професионалния и личния живот на хората извежда на преден план предизвикателствата пред киберсигурността в съвременното общество. Кибератаките и киберпрестъпленията съпътстват ежедневието на съвременните потребители в Интернет като щетите от тях са достатъчно значими, за да бъдат изведени като основен компонент на киберсигурността. Разнообразието на престъпни действия, на извършителите и на последствията налага противодействието срещу киберпрестъпността да се планира и осъществява на базата на стратегически подход. Част от страните конкретизират своите стратегии за киберсигурност с отделни стратегии за противодействие срещу киберпрестъпността, което се оказва правилен подход. В изследването се акцентира върху идеята за необходимостта и полезността от разработването и прилагането на стратегия за противодействие срещу киберпрестъпността. На базата на добри практики, авторски идеи и изследвания се предлага модел за такава стратегия, съобразена със средата в България. Целта е да се предизвика дискусия в посока към оценяване на необходимостта от създаване на национална стратегия за противодействие срещу киберпрестъпността.

Ключови думи: киберсигурност, киберпрестъпност, стратегия, способности, PESTLE – анализ, SWOT - анализ

IT4Sec Reports 149 “Cybercrime Strategy (modeling example)”. The widespread penetration of technology and networks into people’s professional and personal lives brings cyber security challenges to the front line of our society. Cyberattacks and cybercrimes are accompanying the daily lives of modern Internet users, and the damages caused by them are significant enough to be considered as a major component of modern cybersecurity. The diversity of criminal acts, perpetrators, and consequences requires a countering cybercrimes solution that has to be planned and implemented based on a strategic approach. Part of the countries are specifying their cyber security strategies with separate strategies for countering cybercrimes, and this turns out to be the right approach. The study defends the idea of the need and usefulness of developing and implementing a cybercrime strategy. Based on international good practices, authors’ ideas and research, a model for such a strategy, tailored to the Bulgarian environment is proposed. The aim is to provoke a discussion in the direction of assessing the need to create a national cybercrime strategy.

Keywords: cybersecurity, cybercrime, strategy, capabilities, PESTLE - analysis, SWOT - analysis

ISSN 1314-2119

УВОД*

Необратимото навлизане на технологиите в професионалния и личния живот на хората е факт, който не може да бъде отречен. Друг факт е, че степента за използване на тези технологии е функция на тяхната сигурност, като зависимостта е правопропорционална. Трети неоспорим факт е непрекъснато нарастващия мащаб на киберпрестъпността измерен както по броя на кибератаките, така и по размера на щетите от тези престъпления. Характерна особеност на киберпрестъпленията е тяхното разнообразие като вид престъпни действия, адресираност към различни групи потребители, специфични инструменти за постигане на целта и т.н.

При тези обстоятелства, противодействието срещу киберпрестъпността като елемент от създаване на киберсигурност като цяло изисква прилагането на стратегически подход, който следва да бъде достатъчно комплексен и всеобхватен. Следвайки този ред на мисли авторите на настоящия модел стигат да идеята за необходимостта от разработване на стратегия за противодействие срещу киберпрестъпността. Идеята е подкрепена от факта, че една част от страните разполагат с подобни стратегии, които конкретизират общите стратегии за киберсигурност в посоката към ефективното противодействие срещу киберпрестъпността.

В модела се обединени добри практики, достъпни в публикувана литература[1], както и лични идеи, разбирания и резултати от изследвания на авторския колектив. Моделът е адресиран към специалистите по киберсигурност, както и към академичните среди с цел предизвикване на дискусия по проблемите на противодействието срещу киберпрестъпността.

Преглед на опита на различни държави в областта на стратегическия подход при противодействие срещу киберпрестъпността

Прегледът на стратегиите за киберсигурност на различни държави дава възможност за изграждане на обща представа за мястото и ролята на противодействието срещу киберпрестъпността в общата картина на киберсигурността и за възможностите от прилагане на стратегически подход в тази област.

През 2023 г. Съединените щати публикуват актуализиран вариант на националната си стратегия за киберсигурност[2]. В стратегията се отбелязва, че интернет трансформира света като само в рамките на едно поколение се извърши революционализиране в начините, по които хората комуникират и споделят информация в глобален мащаб. Това от своя страна създава възможност за безпрецедентен напредък в човешкия просперитет. В същото време е налице тенденция за нарастване на интензивността и мащаба на зловредните действия в киберпространството, които се характеризират със сложност, комплексност, висока технологичност и огромен мащаб, вариращи от кражба на интелектуална собственост и шпионаж, през атаки на управляващите системи на обекти от критичната инфраструктура до мащабни кампании, засягащи общественото доверие в ценностите на демокрацията. В стратегията се споменават страни като Китай, Русия, Северна Кория, Иран и други, които изграждат и използват офанзивни способности за кибератаки срещу интересите на други държави. На тази база, изграждането и поддържането на дефанзивни способности за противодействие срещу киберпрестъпността се приема за национален приоритет. В процеса на изграждане на подобен тип способности се залага на стратегически подход, в основата на който се поставят сътрудничеството между всички групи заинтересовани лица, изграждано на базата на пет колони: защита на обектите от критичната инфраструктура и критичната

* Моделът е разработен от екип студенти в магистърска програма „Киберсигурност“ на НБУ, под ръководството на проф. Венелин Георгиев.

[1] Seger, A. Cybercrime strategies, Discussion paper, 2012, https://rm.coe.int/16802fa3e1

[2] National Cybersecurity Strategy, The White House, Washington, 2023.

информационна инфраструктура; разкриване и справяне със заплахите и злонамерените действия; формиране на среда за киберсигурност и киберустойчивост; инвестиране в устойчиво бъдеще; укрепване и разширяване на международното сътрудничество. Постигането на посочените по-горе цели изискват сътрудничество между публичния сектор, частния бизнес, гражданското общество, партньорите и международните организации. Успехът на стратегическия подход в противодействието срещу киберпрестъпността зависи от начина, по който се разпределят и адресират ролите, отговорностите и ресурсите в киберпространството.

В анализа на изпълнението на стратегията си за киберсигурност в периода 2022-2023 г. Великобритания отбелязва напредък в следните пет направления:[3]

- повишаване на нивото на киберсигурност чрез инвестиране в хората и в техните умения по пътя на партньорство между правителството, частния бизнес и академичната общност;
- изграждане на устойчиво среда, чрез управление на риска и максимизиране на полезността на технологиите при on-line обработване на конфиденциални данни и информация;
- заемане на лидерска роля в областта на технологиите, които са жизнено важни за кибермощта на страната чрез изграждане на индустриален капацитет и рамка за сигурни бъдещи технологии;
- разширяване на ролята на глобален лидер в процеса за изграждане на по-сигурно и отворено киберпространство чрез взаимодействие с правителствата и бизнеса на партньорски страни;
- разкриване и противодействие срещу киберпрестъпността с цел повишаване на нивото на общата киберсигурност.

Стратегическият подход в последното от горните направления разчита на сътрудничеството на Великобритания с дипломатическите партньори при разкриване, споделяне и противодействие срещу атаки на киберпрестъпници. Страната подкрепя санкции срещу извършителите на киберпрестъпления, повишаване на оперативните способности на националните киберсили.

Целта, която Дания си поставя чрез своята стратегия за киберсигурност[4] е да подпомогне постигането на технологична устойчивост; сигурност и защита на критичната информационна инфраструктура, повишаване на знанията и уменията на потребителите, бизнеса и публичните институции. В стратегията се посочва, че противодействието срещу кибератаките и киберпрестъпността изисква прилагането на стратегически подход и обединяването на усилията на всички групи заинтересовани лица. Като стратегически цели в документа се поставят следните:

- защита на жизнено важните социални функции, които следва да са достатъчно устойчиви дори в смутена среда;
- повишаване на знанията и уменията на потребителите в областите на защитата на активите, познаване на уязвимостите, заплахите и рисковете и т.н.;
- засилване на публично-частното партньорство чрез споделяне на информация за заплахи и инциденти;
- активно участие в международни проекти и инициативи за противодействие срещу киберпрестъпността в рамките на ООН, ЕС и НАТО. Разбирането е, че

[3] National Cyber Strategy. Annual Progress Report 2022-2023. Cabinet Office.
[4] The Danish National Strategy for Cyber and Information Security 2022-2024.

извършването на киберпрестъпление срещу интересите на Дания не може да остава без последствия за извършителите.

Испания използва стратегически подход в полето на киберсигурността и противодействието срещу киберпрестъпността за да осигури достатъчно надеждни способности за превенция, защита, разкриване и противодействие срещу инциденти. В тази посока се поставят следните цели:[5]

- осигуряване на сигурност и устойчивост на информационните и комуникационните системи на публичните и правителствените институции;
- осигуряване на сигурност и устойчивост на информационните и комуникационните системи, използвани от бизнеса и в частност от операторите на обекти от критичната инфраструктура;
- нарастване на способностите за превенция, разкриване, реакция, анализ, отговор, възстановяване, разследване и координиране при случаи на киберпрестъпления и терористични актове в киберпространството;
- повишаване на нивото на знания и умения на гражданите, професионалистите, компаниите и публичните власти по отношение на заплахите и рисковете в киберпространството;
- допринасяне за повишаване на киберсигурността в международен мащаб.

За постигането на горните цели в стратегията се определят т.нар. главни линии за действие, сред които заслужават да се отбележат следните:

- развиване и поддържане на способности за превенция, разкриване, отговор и възстановяване от киберинциденти и киберпрестъпления;
- гарантиране на сигурността и устойчивостта на информационните и комуникационните системи, използвани от публичните институции, бизнеса и в частност от операторите на обекти от критичната инфраструктура;
- участие и инициириане на форми за международно сътрудничество за противодействие срещу киберпрестъпността.

Украйна приема своята национална стратегия за киберсигурност през 2016 г. в отговор на широкоспектърни кибератаки срещу нейната критична инфраструктура[6]. В стратегията се отбелязва, че едновременно с нарастването на приложението на информационните и комуникационните технологии в управлението, бизнеса и ежедневието на потребителите, нараства броя на заплахите и престъпленията в киберпространството. В отговор на тези предизвикателства страната прилага стратегически подход за да осигури сигурно киберпространство и неговото използване от страна на индивидуалните потребители, публичните институции и бизнеса. Усилията на страната се концентрират в следните три области:

- създаване на национална система за киберсигурност;
- нарастване на способностите в сектора за сигурност и отбрана;
- гарантиране на киберсигурността на критичната информационна инфраструктура и на правителствените информационни ресурси.

В сферата на противодействието срещу киберпрестъпността стратегическите намерения на Украйна се концентрират върху участие в регионални и международни проекти и инициативи, фокусирани върху взаимната юридическа помощ, осигуряване на електронни

[5] National Cyber Security Strategy. Departamenot de Seguridad National, 2013.
[6] Cybersecurity in Ukraine: National Strategy and International Cooperation, 2017.

доказателства, внедряване на съвременен софтуер и хардуер за разкриване и разследване на киберпрестъпления.

В актуализираната стратегия за киберсигурност на България[7] въпросите, свързани с противодействието срещу киберпрестъпността са изведени като отделен компонент на съдържанието. Като основни цели в това направления са посочени постигане на ефективност пре превенцията, защитата, реакцията, разследването и правоприлагането при киберпрестъпления и подобряване на оперативния капацитет и способности за противодействие и сътрудничество на национално, регионално и международно ниво.

Противодействието срещу киберпрестъпността се определя като втори основополагащ стълб за постигане на киберсигурност. Като приоритетни направления за работа се определят следните:

- превенция на киберпрестъпленията чрез повишаване на нивото на информираност, засилване на сътрудничеството с всички заинтересовани групи, определяне и прилагане на специфични мерки за превенция на киберпрестъпления и т.н.
- повишаване на административния, организационния и техническия капацитет и способности на компетентните органи по пътя на институционалното укрепване, засилване на информационния обмен, включително с партньорски и международни органи, участие в регионални и международни проекти и инициативи, свързани с противодействието срещу киберпрестъпността.

Направеният преглед на стратегиите за киберсигурност на изброените държави дава възможност да бъдат направени следните обобщения:

- страните прилагат стратегически подход при решаване на въпросите за противодействие срещу киберпрестъпността като елемент на общата киберсигурност;
- в различните документи съществува сходство при поставените цели и планираните действия в интерес на противодействието срещу киберпрестъпността;
- включването на въпросите за противодействие срещу киберпрестъпността в един по-общ документ като стратегия за киберсигурност не позволява навлизане в детайли.

На базата на горните обобщения се формулира извода за това, че стратегическият подход е без съмнение необходим в процеса за противодействие срещу киберпрестъпността и навлизането в детайли изисква разработването на отделен документ под формата на стратегия за противодействие срещу киберпрестъпността. Този извод стои в основата на идеята да бъде предложен следния модел за съдържанието на една стратегия за противодействие срещу киберпрестъпността.

[7] Актуализирана национална стратегия за киберсигурност: Киберустойчива България 2023. (2021), София, Министерски съвет, https://www.strategy.bg/StrategicDocuments/View.aspx?lang=bg-BG&Id=1587

ВЪВЕДЕНИЕ В СТРАТЕГИЯТА

Концепциите за киберсигурност и за противодействие срещу киберпрестъпността

В последните години се налага разбирането за важността и значимостта на сигурността на информационно-комуникационните технологии и информационни активи спрямо обществото като цяло, което е в процес на постоянно трансформиране на базата на технологиите и мрежите. Нещо повече, сигурността на информационно-комуникационните технологии и на информационните активи се превръща в приоритет за политиките на управленските институции на национално, регионално и глобално равнище на сигурност. В общ план усилията се фокусират върху осигуряването на конфиденциалност, интегритет, достъпност и безопасност на информационните активи и на потребителите. На тази база се подчертава важността на способностите за превенция и защита от инциденти, атаки и киберпрестъпления, с акцент върху защитата на критичната информационна инфраструктура.

Стратегиите и мерките против киберпрестъпността допълват техническите и процедурните усилия за киберсигурност. Те са свързани с превенцията, разкриването, разследването и правоприлагането в случаи на киберпрестъпления.

Казано накратко, стратегията за киберсигурността и стратегията за противодействие срещу киберпрестъпността са взаимно свързани и допълващи се, но не са идентични. Това налага разработване на отделна стратегия за противодействие срещу киберпрестъпността, с която да се усили компонента относно противодействието срещу киберпрестъпността в стратегията и политиките за киберсигурност.

Цел и предназначение на стратегията за противодействие срещу киберпрестъпността

Формулирането на целта на стратегията за противодействие срещу киберпрестъпността следва модела, който включва форма на въздействие, обект на въздействие и гледна точка. В този смисъл въздействието е насочено към повишаване на ефективността на противодействието срещу киберпрестъпността от гледна точка на законодателна база, технологични средства за превенция, разкриване и разследване, организираност и структурираност, изграждане на капацитет и способности, използване на инструменти на международно сътрудничество. Обект на стратегията е противодействието срещу киберпрестъпленията с акцент върху тези с международен характер, а гледната точка е киберсигурността като цяло.

Предназначението на стратегията за противодействие срещу киберпрестъпността е двустранно. От една страна се цели повишаване на ефективността на системния подход за постигане на желано ниво на киберсигурност, а от друга страна се прави опит за задълбочаване на професионалния разговор за проблемите на противодействието срещу киберпрестъпността и на киберсигурността като цяло.

Компоненти на стратегията за противодействие срещу киберпрестъпността

Подходът към киберпрестъпността се повлиява от редица фактори, в това число природа на заплахите, състояние на правосъдната система, ниво за защита на правата на човека, върховенство на закона, състояние на киберсигурността, отношения между публичния и частния сектор и др. В тази връзка компоненти на стратегията за противодействие срещу киберпрестъпността се явяват:

- обхват на стратегията, който определя кои деяния се приемат като киберпрестъпления в националните законодателни стандарти на страните, особеностите в тяхното инкриминиране и връзката с националните законодателни стандарти на останалите държави по света;
- цели на стратегията, които могат да бъдат разделени на:

  обща цел, касаеща приложението на правилата и законите, както и защитата на правата на потребителите в киберпространството;

  специфични цели, които са свързани с ефективното противодействие на престъпления срещу конфиденциалността, интегритета, достъпността и безопасността на информационните активи;
- метрики, които от една страна дават възможност да бъде измервано оперативното, текущото състояние на противодействието срещу киберпрестъпността, от друга страна изразяват и съхраняват желаните или още целевите стойности на управляваните параметри и на тази база определяне на мащаба и посоката на необходимите промени;
- отговорности във връзка с мениджмънта, координирането, изпълнението и мониторинга на политиките, стратегиите и мерките за противодействие срещу киберпрестъпността на различните равнища на сигурност;
- технически капацитет и изграждане на способности за превенция, защита, разкриване и разследване на киберпрестъпления на базата на човешки потенциал, технически стандарти, сценарии и ресурси.

Защо е необходима стратегията за противодействие срещу киберпрестъпността

Резултатите от проведени изследвания и от статистики показват, че киберпрестъпността е една от най-бързо развиващите се форми на международна (организирана) престъпност. Без съмнение са доказателствата за това, че последствията от киберпрестъпленията се реализират в различни социални, икономически, политически, военни и други области и са измерват със значим мащаб. На практика киберпрестъпленията подпомагат други видове престъпна дейност, в това число и тероризма. Глобалната свързаност и значимият брой международни киберпрестъпления изискват създаване и използване на способности за сътрудничество между отделните държави при превенцията, разкриването, разследването и правоприлагането срещу киберпрестъпността. Горните характеристики обясняват необходимостта от използването на стратегически подход при противодействието срещу киберпрестъпността, което на практика означава необходимост от разработване и прилагане на стратегия за противодействие срещу киберпрестъпността.

Защо е трудно да се разработи стратегия за противодействие срещу киберпрестъпността

Трудностите пред разработването и успешното прилагане на стратегия за противодействие срещу киберпрестъпността могат да бъдат търсени в следните направления:

- *Интернет на нещата (IoT) и Edge Computing*: разпространението на IoT устройства и преминаването към периферни изчисления значително разширява повърхността за кибератаки. Въпреки, че IoT предлага удобство и автоматизация, те също въвеждат уязвимости, които киберпрестъпниците могат да използват. Защитата на огромна мрежа от взаимосвързани устройства, всяко със своите потенциални слабости в сигурността,

представлява значително предизвикателство за стратегията за противодействие срещу киберпрестъпността. Балансирането на предимствата на IoT и периферните устройства със стабилни мерки за сигурност се превръща в решаващ фактор при прилагането на стратегия, която защитава както данните, така и физическите системи.

- *Облачни системи и виртуализация*: широкото въвеждане и използване на облачните системи и виртуализацията революционизира начина, по който организациите съхраняват, осъществяват достъп и обработват данни. Въпреки, че облачните услуги предлагат повишен мащаб и ефективност на разходите, те също така въвеждат нови съображения за сигурност. Гарантирането на сигурността и поверителността на данните, съхранявани в облака, адресирането на потенциални неправилни конфигурации и управлението на споделената отговорност между доставчиците на облачни услуги и потребителите са критични аспекти на цялостна стратегия за киберсигурност и в частност за противодействието срещу киберпрестъпността.

- *Изкуствен интелект (AI) и машинно обучение (ML)*: технологиите AI и ML притежават огромен потенциал за подобряване на защитата на киберсигурността. Те могат да автоматизират откриването на заплахи, да анализират големи набори от данни за аномалии и да активират предсказуеми мерки за сигурност. Въпреки това, същите технологии могат да бъдат използвани и от заплахи, което води до появата на сложни атаки, управлявани от AI. Постигането на баланс между използването на AI и ML за отбрана, като същевременно се справят с рисковете, свързани с конкурентния AI, е предизвикателство, с което трябва да се справят стратегиите за противодействие срещу киберпрестъпността.

- *Криптиране и запазване на поверителността*: тъй като опасенията за поверителността нарастват, технологиите за криптиране играят основна роля в защитата на чувствителни данни. Широкото използване на криптиране, както при пренос, така и при съхранение на данните, допринася за стабилна позиция на сигурност. Въпреки това дебатът за криптиране, включващ баланса между поверителността и законния достъп, представлява значителна пречка при разработването на стратегии за противодействие срещу киберпрестъпността. Постигането на точния баланс между криптирането и необходимостта от законен достъп до данни е предизвикателство, с което трябва да се борят политиците и специалистите по сигурността.

- *Недостатъци в уменията и развитие на работната сила*: недостигът на квалифицирани специалисти по киберсигурност представлява постоянна пречка пред създаването и прилагането на ефективни стратегии за противодействие срещу киберпрестъпността. Търсенето на експертен опит в области като мрежова сигурност, реагиране при инциденти и управление на уязвимости продължава да изпреварва наличието на квалифицирани специалисти. Преодоляването на недостига на умения и инвестирането в стабилни инициативи за развитие на работната сила в киберсигурността се превръщат в критични компоненти на всяка цялостна стратегия за противодействие срещу киберпрестъпленията.

- *Регулаторни рамки и рамки за съответствие*: ориентирането в сложния пейзаж от регулаторни изисквания и изисквания за съответствие е постоянно предизвикателство за организациите. Стратегията за противодействие срещу киберпрестъпността трябва да бъде в съответствие с различни специфични за индустрията разпоредби, като например с Общия регламент за защита на личните данни (GDPR). Придържането към тези рамки, като същевременно се балансират практическите аспекти на изпълнението, представлява значително препятствие пред противодействието срещу киберпрестъпността.

Като обобщение може да се каже че, технологичният напредък създава както възможности, така и пречки пред разработването и прилагане на стратегия за

противодействие срещу киберпрестъпността. Въпреки че нововъзникващите технологии предлагат иновативни решения за подобряване на сигурността, те също така въвеждат нови уязвимости и предизвикателства, а също и възможности пред киберпрестъпниците които трябва да бъдат адресирани. Преодоляването на препятствия като сигурността на IoT, сложността на облака, заплахите, управлявани от AI, и липсата на умения изисква многостранен, стратегически подход, който съчетава нормативна база, техническа експертиза, сътрудничество и непрекъснато адаптиране. Чрез възприемане на технологичния напредък, като същевременно смекчава свързаните рискове, стратегията за противодействие срещу киберпрестъпността може да се развива, за да предпазва от възникващи заплахи и да защитава достатъчно ефективно цифровите екосистеми.

Ползи от стратегията за противодействие срещу киберпрестъпността

Разработването и прилагането на стратегия за противодействие срещу киберпрестъпността носи ползи, които могат да бъдат обобщени по следния начин:

- постигане на задълбочено разбиране за заплахите, уязвимостите и рисковете за киберсигурността под формата на киберпрестъпления;
- определяне на ролите и отговорностите в процедурите за противодействие срещу киберпрестъпността;
- оценяване на напредъка в противодействието срещу киберпрестъпността;
- повишаване на осведомеността на потребителите и на различните групи заинтересовани лица;
- очертаване на рамка за действие по превенция, разкриване, разследване и правоприлагане срещу киберпрестъпления в контекста на изграждане на киберсигурност.

Заинтересовани страни и техните роли при създаване на стратегия за противодействие срещу киберпрестъпността

Създаването и прилагането на цялостна стратегия за противодействие срещу киберпрестъпността изисква сътрудничество и ангажираност от страна на различни групи заинтересовани страни в едно или друго юридическо звено. Характерна особеност е, че всяка заинтересована страна е носител на уникални перспективи, опит и отговорности. Ключовите заинтересовани страни, участващи в създаването и прилагането на стратегията за противодействие срещу киберпрестъпността, както и техните роли са следните:

- *Държавни агенции и ведомства*: министерство на отбраната, което отговаря за националната сигурност, способностите за киберотбрана и защита на критичната инфраструктура; министерство на вътрешните работи, което в своята работа се фокусира се върху правоприлагането, предотвратяването на киберпрестъпления и поддържането на обществената безопасност; национални разузнавателни агенции с тяхното участие в събирането на разузнавателна информация за кибернетични заплахи на различните равнища на сигурност; регулаторни и политически агенции, отговорни за създаването и прилагането на политики, разпоредби и стандарти за киберсигурност.

- *Частен сектор:* доставчици на интернет услуги (ISP) отговорни за осигуряване на интернет свързаност и гарантиране на сигурността на мрежата; телекомуникационни компании, които поддържат националната телекомуникационна инфраструктура и защитени комуникационни мрежи; оператори на критична инфраструктура, представляващи субекти, управляващи важни обекти от сектори като енергетика, транспорт, здравеопазване, финанси

и телекомуникации, които са от решаващо значение за националната сигурност; технологични компании, разработчици на софтуер, хардуер и решения за киберсигурност, които могат да подобрят националните способности за киберзащита противодействие срещу киберпрестъпността; финансови институции с техните отговорности за осигуряване на финансови транзакции, защита на клиентските данни и предотвратяване на киберизмами; индустриални асоциации, които представляват различни сектори и играят съществена роля в оформянето на политики, стандарти и най-добри практики за киберсигурност.

- *Академични и изследователски институции: у*ниверситети и изследователски центрове, които са ангажирани с изследвания на киберсигурността, разработване на нови технологии и предоставяне на образователни програми за създаване на квалифицирани кибер професионалисти; институти за обучение, предлагащи специализирани програми за обучение по киберсигурност за държавни служители и професионалисти в индустрията.

- *Организации на гражданското общество:* организации за защита на потребителите с ангажименти по гарантиране на сигурността на потребителските данни и застъпничество за стандарти за киберсигурност в продуктите и услугите; групи за осведоменост и обучение по киберсигурност, които участват в насърчаване на осведомеността за киберсигурност, обучение на обществеността относно онлайн заплахите и предоставяне на ресурси за безопасни онлайн практики; общности за етично хакерство и изследване на сигурността, подпомагащи идентифицирането на уязвимостите и допринасящи за цялостното подобряване на киберсигурността чрез отговорно разкриване на констатациите.

- *Международни организации и партньори:* международни организации за киберсигурност, осъществяващи сътрудничество със страната по инициативи за киберсигурност, споделяне на информация и изграждане на капацитет; двустранни и многостранни партньори, страни по споразумения за сътрудничество в областта на киберсигурността, провеждащи съвместни учения и споделящи програми за обмен на знания; чужди правителства, стоящи в основата на сътрудничеството за споделяне на информация за кибернетични заплахи, извършващи съвместни разследвания и координация на политиката за борба с транснационалните кибернетични заплахи и престъпления.

- *Широката общественост:* индивидуални потребители във вида на крайни потребители, които играят жизненоважна роля в поддържането на киберсигурността и противодействието срещу киберпрестъпността, като следват най-добрите практики, актуализират софтуера и докладват за подозрителни дейности; малки и средни предприятия (МСП), имащи необходимост от прилагането на мерки за киберсигурност, за да се защитят техните активи, клиентски данни и да се допринесе за цялостната национална киберустойчивост; медии в различен вид, отговарящи за повишаване на осведомеността относно киберзаплахите, разпространение на информация за киберпрестъпленията и насърчаване на общественото разбиране по проблемите на киберсигурността.

Създаването и прилагането на стратегия за противодействие срещу киберпрестъпността изисква активно участие и сътрудничество на изброените по-горе заинтересовани страни. От изпълнително ръководство през оперативни отдели, правни екипи и екипи за съответствие до човешки ресурси и външни партньори, всяка заинтересована страна носи уникален опит и отговорности. Ангажирането на тези заинтересовани страни гарантира холистичен подход към киберсигурността и противодействието срещу киберпрестъпността, съгласуване на техническите възможности, стратегическите цели, изискванията за съответствие и силна култура на сигурност. Чрез насърчаване на сътрудничеството и участието на всички заинтересовани страни могат да бъдат разработени и внедрени устойчива визия и стратегия за противодействие срещу киберпрестъпността, както и за киберсигурност като цяло.

ТЕКУЩО СЪСТОЯНИЕ НА ПРОТИВОДЕЙСТВИЕТО СРЕЩУ КИБЕРПРЕСТЪПНОСТТА

Основни определения

Като общо определение в настоящия модел се приема, че киберпрестъпление е това обществено опасно деяние (действие или бездействие), което използва компютър, компютърна мрежа или свързано устройство като средство/инструмент или като цел/мишена, извършено е виновно и е обявено от закона за наказуемо.[8]

От своя страна, киберпрестъпността е подкатегория на компютърната престъпност, отнасяща се до престъпленията, при които се използва Интернет и други компютърни мрежи като елемент (компонент, средство) на престъплението[9].

В настоящия модел киберпрестъпленията се разделят в две основни категории:

- киберпрестъпления, при които компютърът се използва като средство/инструмент: сред тях попада използването на компютър, за да бъдат разпространени малуеър, неправомерна информация или неправомерни изображения;
- киберпрестъпления, при които компютърът се използва като цел/мишена: сред тях попадат инфектирането с малуеър с цел компрометиране на устройствата, изтриване или кражба на данни, както и атаките от типа „отказ от услуга“.[10]

Често киберпрестъпниците извършват деяния, попадащи едновременно и в двете категории, посочени по-горе. Така например, те могат да инфектират един компютър с малуеър и след това да го използват, за да бъде разпространен малуеърът към други устройства или в рамките на мрежа.

Някои юрисдикции разграничават и трета категория компютърни престъпления, при които компютърът се използва като допълнение към престъплението – например, за да бъдат съхранявани в паметта му неправомерно придобити данни.[11]

Измерване на мащабите на киберпрестъпността

Мащабът на киберпрестъпността може да бъде измерван с помощта на различни метрики. Като пример може да бъде използван броя на киберпрестъпленията отнесени към броя на населението в определен район. В тази посока най-много киберпрестъпления на глава от населението у нас са регистрирани в Русе, Враца и Смолян. Според статистиката, в България през 2021 г. са регистрирани общо 51 компютърни престъпления. От тях са разкрити едва 6, което означава, че общата разкриваемост е под 12%.

Реалният брой на компютърните престъпления в България вероятно е много по-голям. Много киберпрестъпления не се докладват по различни причини, сред които непознаване на реда и начините за докладване при случай на киберпрестъпление, недоверие в способностите на органите за разкриване и разследване, срам и неудобство от попадане в положение на жертва на киберпрестъпление и т.н. Често самите жертви на киберпрестъплението не разбират, че са ощетени по някакъв начин. Също така статистиката не уточнява какви точно са регистрираните в България киберпрестъпления. В световен мащаб

---

[8] *National Plan to Combat Cybercrime*, Australian Government, 2022.
[9] Георгиев, В. *Противодействие срещу киберпрестъпността* (София, 2020)
[10] *Cyber Crime Strategy*, Home Department, 2010.
[11] “What is cybercrime? How to protect yourself from cybercrime,” Kaspersky, 2022, https://www.kaspersky.com/resource-center/threats/what-is-cybercrime.

най-често потребителите се оплакват, че са станали жертва на някой от следните видове киберпрестъпления:

- фишинг: под формата на кражба на данни като потребителско име и парола, с което потребителят достъпва някаква онлайн услуга;
- измама в сайтове за обяви: при което най-често потребителят плаща за стока, която не получава или пък не си получава парите за стока, която е продал;
- кражба на лични данни;
- кражба на идентичност: най-често под формата на случаи, при които някой се представя за потребителя, подписва документи или прави плащания от негово име;
- изнудване: най-често под формата на продаване на мълчание срещу пари.

В Таблица 1 са посочени резултатите от измерването на мащаба на киберпрестъпността на базата на брой престъпления на 100 хил. души[12].

Таблица 1. Разпределение по градове на броя киберпрестъпления на 100 хил. души

Област	**Регистрирани престъпления**	**Престъпления на 100 хил. души**
Русе	4	1.87
Враца	2	1.27
Смолян	1	0.97
Стара Загора	3	0.96
Плевен	2	0.85
Монтана	1	0.79
Бургас	2	0.489
Хасково	1	0.45
Велико Търново	1	0.43
Пазарджик	1	0.4

По време на пандемията от Covid-19 се наблюдава изместване на някои престъпни дейности във виртуална среда и тенденция на покачване с 3-4 пъти на кибер престъпления. С 30 до 50 пъти е нараснал броят на получените сигнали в ГДБОП. Проведени са 66 полицейски операции срещу киберпрестъпността, от тях 9 международни[13].

[12] „Топ 10 на българските градове с най-много киберпрестъпления," *Questo*, 2021, https://questona.com/top-10-bg-cybercriminals/

[13] Видев, Д. „Ръст на киберпрестъпността и домашното насилие през 2021-ва," *Българско национално радио*, 2022, https://bnr.bg/horizont/post/101625182/rast-na-domashnoto-nasilie-kiberprestapnostta-i-patnite-proizshestvia-prez-2021-va

Оторизирани институции за противодействие срещу киберпрестъпността

Ефективното противодействие срещу киберпрестъпността следва да бъде адресирано към съответните институции. Съществено е да се отбележи, че това противодействие е нужно да бъде функция на съвместните и координирани действия на различни нива от държавния апарат, включително политическо, стратегическо, оперативно, техническо. Важно е да се има предвид, че нерелевантни на пръв поглед държавни органи като президента и министерския съвет чрез предоставените им законови функции са неизменна част от холистичния подход към темата. Представените по-долу институции са сред онези, които имат стратегическо, оперативно или техническо отношение към противодействието срещу киберпрестъпността:

- *Съвет по киберсигурност, представляващ консултативен орган към Министерски съвет.* В правомощията на съвета се включват анализиране на тенденциите в измененията на киберзаплахите, рисковете и методите за противодействие, взаимодействие с Министерски съвет, Съвет по сигурността към Министерския съвет, компетентните органи в областта на киберсигурността, даване на предложения за хармонизиране и координиране на секторните политики за постигане на високо общо ниво на киберсигурност на икономиката и обществото;

- *Дирекция „Киберпрестъпност“ към Главна дирекция „Борба с организираната престъпност“ на Министерство на вътрешните работи.* Дирекцията представлява основен орган за борба с киберпрестъпността. Правомощията на дирекцията в сферата на противодействието срещу киберпрестъпността включват, но не се изчерпват с разследване и преследване на престъпления във виртуалното пространство, включително компютърни хакерски атаки, измами с използването на компютри и други киберпрестъпления, както и противодействие на организирани престъпни групи.

- *Национална координационно-организационна мрежа за киберсигурност.* За този орган е характерно, че не се занимава пряко с киберпрестъпността, но в същото време е отговорен за създаването на рамка и стратегии за киберсигурност като цяло, което по косвен начин повлиява ефективното противодействие срещу киберпрестъпността. Във функциите на органа се включва координационното сътрудничество с останалите релевантни институции, оценка на риска, образование и обучение, международно сътрудничество.

- *Национален координатор по киберсигурност, представляващ определян от министър-председателя орган, който се явява и секретар на Съвета по киберсигурността.* На него се възлага ръководството при изготвянето и актуализирането на Националната стратегия за киберсигурност и пътната карта към нея, взима участие при изграждането и развитието на Националната координационно-организационна мрежа за киберсигурност и осигуряването на нейната надеждност, сигурност и устойчивост, участва при създаването и развитието на Националния киберситуационен център за координиране на действията и комплексната реакция при заплаха от киберкриза и заплахи от хибриден характер, осъществява взаимодействие на Съвета по киберсигурността и секретаря на Съвета по сигурността към Министерския съвет.

- *Национално единно звено за контакт към Министерство на електронното управление,* представляващо звено за сътрудничество и координация във връзка с електронното управление. Правомощията му включват координиране на въпросите, свързани с мрежовата и информационната сигурност, както и въпросите, свързани с трансграничното сътрудничество със съответните органи в други държави - членки на Европейския съюз.

- *Комисия за защита от дискриминация,* представляваща независим специализиран държавен орган, осъществяващ контрол по прилагането и спазването на Закона за защита от

дискриминация и други закони, уреждащи равенство в третирането, с цел предотвратяване на дискриминация, защита от дискриминация и осигуряване равенство на възможностите. В кръга на правомощията на органа се включват установяване на нарушения на закони, уреждащи равенство в третирането, постановяване на предотвратяване и преустановяване на нарушението и възстановяване на първоначалното положение, налагане на санкции и прилагане на мерки за административна принуда, даване на задължителни предписания, предложения и препоръки до държавните и общинските органи, предоставяне на независима помощ на жертвите на дискриминация, включително и по пътя на киберпрестъпления.

- *Комисия за защита на личните данни,* която е постоянно действащ независим надзорен орган, осъществяващ защитата на лицата при обработването на техните лични данни и при осъществяването на достъпа до тези данни, както и контрола по спазването на Регламент (ЕС) 2016/679 и на Закона за защита на личните данни. Изпълнява функции по анализиране и осъществяване на цялостен надзор и осигуряване спазването на Регламент (ЕС) 2016/679, на Закона за защита на личните данни и на нормативните актове в областта на защитата на лични данни, осигурява прилагането на решенията на Европейската комисия в областта на защитата на личните данни и изпълнението на задължителните решения на Европейския комитет по защита на данните по чл. 65 от Регламент (ЕС) 2016/679.

Съществуващо законодателство за противодействие срещу киберпрестъпността

Сред основните нормативни актове, в чиито предмет влиза противодействието срещу киберпрестъпността могат да бъдат посочени:

Наказателен кодекс, представляващ нормативен акт на националното законодателство и третиращ защита от престъпни посегателства срещу личността и правата на гражданите, както и цялостния установен в страната правов ред.

Закон за киберсигурност, представляващ нормативен акт на националното законодателство, уреждащ дейностите по организацията, управлението и контрола на киберсигурността и предприемане на необходимите мерки за постигане на високо общо ниво на мрежова и информационна сигурност.

Наредба за минималните изисквания за мрежова и информационна сигурност, представляваща нормативен акт на националното законодателство, занимаващ се с уреждане на мерки за мрежова и информационна сигурност, относими правила и модели.

Директива 2011/93/ЕС на Европейския парламент и на Съвета от 13 декември 2011 година относно борбата със сексуалното насилие и със сексуалната експлоатация на деца, както и с детската порнография и за замяна на Рамково решение 2004/68/ПВР на Съвета. Целта е установяване на минимални правила за определянето на престъпленията и наказанията в областта на сексуалното насилие и сексуалната експлоатация на деца, детската порнография и установяването на контакт с деца за сексуални цели, засилване на превенцията по отношение на тези престъпления и засилване на защитата на жертвите от тях.

Директива 2013/40/ЕС на Европейския парламент и на Съвета от 12 август 2013 година относно атаките срещу информационните системи и за замяна на Рамково решение 2005/222/ПВР на Съвета. Установяване на минимални правила за определянето на престъпленията и наказанията в областта на атаките срещу информационните системи; способстване за предотвратяването на тези престъпления и да подобряване на сътрудничеството между съдебните и други компетентни органи.

Директива (ЕС) 2019/713 на Европейския парламент и на Съвета от 17 април 2019 година за борба с измамите със и подправянето на непарични платежни средства и за замяна на Рамково решение 2001/413/ПВР на Съвета. Цели установяване на правила във връзка с определянето на престъпленията и наказанията в областта на измамите със и подправянето на непарични платежни средства; улесняване на предотвратяването на такива престъпления, както и оказването на помощ и подкрепа за пострадалите.

Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните). Целта е определяне на правилата по отношение на защитата на физическите лица във връзка с обработването на лични данни, както и правилата по отношение на свободното движение на лични данни.

Конвенция за престъпления в кибернетичното пространство (Будапещенска конвенция на Съвета на Европа). Първият международен договор за престъпления, извършени чрез интернет и други компютърни мрежи, занимаващ се по-специално с нарушенията на авторските права, компютърните измами, детската порнография и нарушенията на мрежовата сигурност.

Стратегията за противодействие срещу киберпрестъпността следва да бъде в синхрон и да допринася за изпълнение на изискванията на горните документи, както и на останалите релевантни нормативни актове от националното и международното законодателство.

Анализ на влиянието на външната и вътрешната среда върху противодействието срещу киберпрестъпността

Противодействието срещу киберпрестъпността и неговата ефективност са в пряка зависимост от влиянието на вътрешната среда (състоянието на системата за национална сигурност) и външната среда (включващо състоянието на политическата, икономическата, социалната, технологичната, правната и околната среда).

На първо място е извършен анализ на влиянието на външната среда върху ефективното противодействие срещу киберпрестъпността. Използван е метода за анализ, познат като PESTLE – анализ. В Таблица 2 са представени политическите, икономическите, социалните, технологичните и правните фактори, както и фактори на околната среда, които оказват най-съществено влияние върху състоянието и противодействието срещу киберпрестъпността.

Таблица 2. Фактори на външната среда по категории, отчитани при извършването на PESTLE анализа

Политически фактори - Липса на стабилно, редовно правителство в България - Липса на международно сътрудничество, което се изпълнява на практика - Наличие на актуализирана стратегия за киберсигурност, която съдържа в себе си добри практики и политики за противодействие срещу киберпрестъпността - Наличие на визия за засилване на международното сътрудничество и съвместна работа на партньорските структури и организации - Наблюдавана тенденция за засилване на кибершпионажа и кибервойните	**Икономически фактори** - Отделяне от бюджета на недостатъчно средства за проекти за киберсигурност и информационни технологии - Опасност от кибератаки срещу малкия и средния бизнес, което би довело до значими финансови загуби - Необходимост от адекватно инвестиране в модерни технологии, програми за обучение и създаване на квалифицирани специалисти по киберсигурност - Недостатъчно участие в международна проекти и програми за киберсигурност, финансирани от международни финансови органи
Социални фактори - Липса на доверие в полицейските органи от страна на обществото, което води до това всеки да се справя сам когато стане жертва на кибератака, а това в някои случаи води до нанасяне на по-големи щети - Недостатъчно обучение по киберсигурност и липса на осведоменост на потребителите за потенциалните заплахи в мрежата - Масово използване на модерните технологии, което прави организациите и потребителите по уязвими - Липса на достатъчно ефективно публично-частно партньорство - Склонност към корупция и злоупотреба с положение	**Технологични фактори** - Недостатъчни инвестиции в технически системи за защита от следващо поколение - Липса на квалифицирани киберспециалисти, които да имат практически умения и познания за съвременните технологии и заплахи - Ниско ниво на технологична култура в голяма част от обществото - Използване на „Изкуствен интелект“ за кибератаки и киберпрестъпления - Тенденция за нарастваща дигитализация и необратимо навлизане в ерата на „Интернет на нещата“.
Правни фактори - Съществуване на международни закони и регулации по GDPR, предвиждащи огромни финансо- ви наказания за неспазване на изискванията - Наличие на национални и международни нормативни актове за противодействие срещу киберпрестъпността, нуждаещи се от преглеждане и актуализиране	**Фактори на околната среда** - Последствията от Ковид-19 принудиха бизнесите да започнат да оперират дистанционно, което направи контрола върху служителите по-труден и увеличи рисковете за киберсигурността и броя на киберпрестъпленията

- Наличие на задължения за внедряване и сертификация, като пример, стандарт ISO 27001:2013 - Липса на пряко адресиране и съществени различия в ролите и отговорностите в сферата на киберсигурността и противодействието срещу киберпрестъпността.	- Войната в Украйна създаде предпоставки за увеличаване на случаите на кибератаки и киберпрестъпления

Направеният PESTLE – анализ в настоящия модел разкрива няколко предизвикателства. От политическа гледна точка липсата на стабилно редовно правителство и ограниченото международно сътрудничество възпрепятстват ефективните мерки за киберсигурност. От икономическа гледна точка е необходимо заделянето на достатъчно бюджетни средства и инвестиции в съвременни технологии. В социално отношение е необходимо да се подобри общественото доверие, информираността и формите за публично-частно партньорство. В технологично отношение от решаващо значение са усъвършенстването на системите за сигурност от следващо поколение и изграждането на квалифицирани специалисти в областта на киберсигурността. От правна гледна точка е жизнено важно актуализирането и спазването на разпоредбите на релевантните национални и международни нормативни актове. По отношение на околната среда от съществено значение е адаптирането към отдалечени операции и повишаването на бдителността поради въздействието на COVID-19 и нарастващите кибератаки. Като цяло, за справянето с тези предизвикателства чрез сътрудничество и системни подходи е необходимо разработването на стратегия за противодействие срещу киберпрестъпността в България.

Анализът на влиянието на вътрешната среда върху ефективното противодействие срещу киберпрестъпността е направен с помощта на SWOT – анализ. В Таблица 3 са представени силните и слабите страни, както и възможностите и заплахите пред противодействие срещу киберсигурността у нас.

Резултатите от SWOT – анализа помагат да бъде направен извода за това, че най-удачният вариант е разработването на стратегия за развитие на противодействието срещу киберпрестъпността. Това означава фокусиране върху използване на възможностите за справяне със заплахите при отчитане на силните страни на националната система за киберсигурност.

Таблица 3. Матрица за SWOT - анализа

Силни страни	**Слаби страни**
- Наличие на добри професионалисти в сферата на киберсигурността, които биха могли да спомогнат за подобряването на текущата стратегия за противодействие срещу киберпрестъпността - Наличие на добри чуждестранни примери за адекватни стратегии за противодействие срещу киберпрестъпността, от които би могло да се взаимства - Наличие на академичен капацитет, който би могъл да подпомогне органите,	- Недостатъчно добре развита нормативна база по отношение на противодействието срещу киберпрестъпността - Недостатъчен капацитет за разкриване и разследване на киберпрестъпления - Липса на достатъчно ефективно международно сътрудничество по отношение на уеднаквяването на нормативната база на европейско и на глобално ниво

отговорни за разработването на стратегията за противодействие срещу киберпрестъпността	
Възможности - Възможност за съставяне на стратегия за противодействие срещу киберпрестъпността в синхрон с най-добрите международни практики - Възможност за обучение на обществото и повишаване на осведомеността по отношение на основните елементи от стратегията за противодействие срещу киберпрестъпността и на актуалните киберзаплахи - Възможност за съставяне на експертен екип, отговорен за създаването и прилага -нето на стратегия за противодействие срещу киберпрестъпността	**Заплахи** - Заплаха от неадекватно изготвена стратегия за противодействие срещу киберпрестъпността, която да не отговаря на най-добрите националните потребности - Заплаха от назначаване на неквалифициран екип за създаване на стратегията за противодействие срещу киберпрестъпността - Заплаха от липсата на комуникация на национално и международно ниво, което би довело до незадоволителни резултати при прилагането на стратегията - Заплаха от неправилно адресиране на отговорностите за прилагането на стратегията за противодействие срещу киберпрестъпността - Заплаха от провал на стратегията поради неинформираност на потребителите

ВИЗИЯ ЗА РАЗВИТИЕ НА ПРОТВОДЕЙСТВИЕТО СРЕЩУ КИБЕРПРЕСТЪПНОСТТА

Картината на киберпрестъпността продължава да се развива, което изисква освен наличие на способности за отговор на моментните предизвикателства, също и формулиране на визия за развитие на способностите за противодействие срещу киберпрестъпността в средносрочен и дългосрочен времеви период. Ключови елементи на една перспективна визия за противодействие срещу киберпрестъпността са следните групи фактори:

- *Проактивна и адаптивна защита*: конкретната визия за противодействие срещу киберпрестъпността обхваща проактивен и адаптивен подход на защита. Това включва използване на напреднали технологии като изкуствен интелект, машинно обучение и анализ на поведението за откриване и реагиране на заплахи в реално време. Чрез непрекъснато наблюдение на системите, мрежите и поведението на потребителите, организациите могат да идентифицират и смекчат рисковете, преди те да ескалират и да доведат до киберпрестъпление. Бъдещето на киберсигурността е в способностите за прогнозиране и автоматизиране на механизми за реакция, които могат да бъдат една крачка пред нововъзникващите заплахи.

- *Сигурност за запазване на поверителността*: защитата на личната неприкосновеност, като същевременно се гарантира стабилна сигурност, е решаващ аспект от бъдещето на противодействието срещу киберпрестъпността. Организациите трябва да дадат приоритет на технологиите и принципите за подобряване на поверителността, като

анонимизиране на данните, диференцирана поверителност и поверителност по проект. Постигането на правилния баланс между сигурност и поверителност изисква силно криптиране, сигурни практики за обработка на данни и прозрачни рамки за управление на данните. Конкретната визия за противодействие срещу киберпрестъпността подчертава значението на запазването на правата на поверителност, като същевременно се предпазва от киберзаплахи.

- *Екосистема за съвместна отбрана*: бъдещето на противодействието срещу киберпрестъпността разчита на екосистема за съвместна отбрана, която обхваща индустрии, сектори и граници. Организациите трябва активно да участват в инициативи за споделяне на информация, да си сътрудничат с партньори в индустрията и да участват в публично-частни партньорства. Чрез споделяне на информация за заплахи, най-добри практики и научени уроци, колективната защита срещу кибернетични заплахи се укрепва. Конкретната визия за противодействие срещу киберпрестъпността насърчава култура на сътрудничество, което позволява на организациите да реагират ефективно на развиващите се заплахи и да се адаптират към възникващите вектори на атаки.

- *Устойчивост и реакция при инциденти*: в една все по-взаимосвързана и сложна цифрова среда организациите трябва да се съсредоточат върху изграждането на устойчивост и стабилни способности за реакция при инциденти. Конкретната визия за противодействие срещу киберпрестъпността включва създаване на всеобхватни планове за реагиране при инциденти, провеждане на редовни тренировки и инвестиране в мерки за киберустойчивост. Организациите трябва да възприемат нагласата за „предполагане на нарушение“, при която се подготвят за неизбежни киберинциденти и развиват способността да откриват, ограничават и възстановяват бързо. Чрез интегриране на реакцията на инциденти в цялостната стратегия за противодействие срещу киберпрестъпността, организациите могат да минимизират въздействието на атаките и бързо да възстановят операциите.

- *Непрекъснато образование и обучение*: бъдещето на противодействието срещу киберпрестъпността зависи от добре информираната и киберосведомена работна сила. Организациите трябва да инвестират в програми за непрекъснато образование и обучение, за да подобрят уменията за киберсигурност и осведомеността сред служителите. Инициативите за обучение трябва да обхващат възникващи заплахи, тактики за социално инженерство, сигурни практики за кодиране и протоколи за обработка на данни. Чрез насърчаване на култура на осведоменост за киберсигурността, организациите могат да дадат възможност на служителите да станат първата линия на защита срещу киберзаплахи и киберпрестъпления.

- *Етичен и отговорен AI в киберсигурността*: тъй като изкуственият интелект (AI) става все по-вграден в киберсигурността, от съществено значение е да се гарантира неговата етична и отговорна употреба. Конкретната визия за противодействие срещу киберпрестъпността включва разработване на AI модели и алгоритми, които са в съответствие с етичните принципи и човешките права. Организациите трябва да създадат управленски рамки за AI в киберсигурността, като се занимават с въпроси като пристрастност, прозрачност и отчетност. Чрез отговорно внедряване на AI технологии организациите могат да укрепят защитата си, като същевременно спазват етичните стандарти.

Във визията за противодействие на киберпрестъпността отговорностите се разделят между правителство, бизнес сектор, гражданско общество и отделни частни потребители.

Правителство отговаря за изграждането на подходящи правни рамки, равноправно правоприлагане, интензивно международно сътрудничество, сформиране на компетентни институции, последно, но не на последно място осигуряване на обществена осведоменост и образование:

- Създаване и налагане на всеобхватни правни рамки, дефиниращи киберпрестъпленията, описващи наказания за правонарушителите и едновременно даващи възможност за международно сътрудничество при разследвания и наказателни преследвания.

- Влагане на ресурси в оборудване и обучения на правоприлагащи агенции, занимаващи се с разследване на киберпрестъпления.

- Активно участие във форми за международно сътрудничество, координиране на киберпрестъпленията и споделяне на информация е от особено значение за превенцията.

- Сформиране на компетентни органи като се обърне особено внимание на изграждане на експерти в областта на цифровата съдебна медицина, реакция при инциденти, както и анализ на заплахи.

- Водене на кампании за обществена осведоменост, обучителни процеси на гражданите за реакция при киберзаплахи, предоставяне на добри практики за безопасно онлайн присъствие в мрежата и съответно правилни реакции при евентуално настъпване на киберпрестъпление.

Бизнес секторът би следвало да бъде ангажиран с противодействието срещу киберпрестъпността чрез споделяне на информация, планиране на реакция при настъпване на инциденти, управление на веригите за доставка:

- Приоритет на бизнеса по отношение на мерките за киберсигурност. Например: контрол на достъп, криптиране, редовна актуализация на новите системи, обучение на служителите, запознаване с новостите в сектора на киберсигурността.

- Споделяне на информация между компаниите относно възникнали заплахи, добри практики, подобряване на вече създали се такива.

- Частният бизнес носи отговорност за създаване на обширни планове за реакция при инцидент както и да гарантира, че притежава протоколи за откриване, ограничаване и възстановяване от кибератаки.

- Корпорациите следва да бъдат тези, които извършват надеждни проверки при избора на доставчици от трети страни, проследяване на спазването на строги стандарти за киберсигурност.

- Бизнесът носи отговорност при защитата на лични данни на своите клиенти, както и за цялостното, адекватно съхранение и използване на информация.

От гражданското общество се изисква да бъде закрила за кибержертвите, да бъде осведомено относно заплахите в дигиталната сфера, да осъществява сътрудничество между правителството и бизнес сектора:

- Гражданските организации биха имали особено важна роля за повишаването на грамотността относно киберпрестъпленията, кибератаките. Също така би имало голяма сила при застъпничество относно правата и отговорностите във виртуалния свят.

- Осигуряването на подкрепа на жертвите на киберпрестъпления чрез консултиране, правна помощ, предоставяне на ресурси за навременно докладване на инциденти.

- Сътрудничество между гражданското общество, правителството и бизнес сектора при разработване на политики, насоки и инициативи в областта на противодействието срещу киберпрестъпността.

Отговорности на частните лица/потребителите:

- Поддържане на достатъчно ниво на киберхигиена по пътя на използване на силни

пароли, поддържане на актуален софтуер, внимаване при опити за фишинг и избягване на подозрителни уебсайтове и изтегляния.

- Стремеж към информираност и осведоменост за често срещани киберзаплахи, за безопасни онлайн практики, за механизмите за докладване на киберпрестъпления.

- Своевременно/незабавно докладване за киберинциденти на правоприлагащите органи или съответните платформи за докладване, за да подпомогнат разследванията и да защитят другите да не станат жертва на подобни атаки.

- Защита на личната информация чрез филтрирано споделяне на информация онлайн, използване на настройки за поверителност в социалните медийни платформи и внимание при споделянето на чувствителна информация.

ГЛАВНИ ОБЛАСТИ, СТРТЕГИЧЕСКИ ЦЕЛИ И ОПЕРАТИВНИ ДЕЙНОСТИ ЗА ИЗПЪЛНЕНИЕ НА СТРАТЕГИЯТА ЗА ПРОТИВОДЕЙСТВИЕ СРЕЩУ КИБЕРПРЕСТЪПНОСТТА

При прегледа на част от съществуващите стратегии за противодействие срещу киберпрестъпността се установи, че същите се фокусират върху пет главни области, които включват нормативна база за противодействие срещу киберпрестъпността, технологии и стандарти, организираност на противодействието, способности за разкриване, разследване и правоприлагане при киберпрестъпления, международно сътрудничество при противодействието срещу киберпрестъпността. С цел опростяване на настоящия модел в него са отчетени само две от изброените по-горе главни области, а именно нормативна база и способности за разкриване, разследване и правоприлагане при киберпрестъпления. Изборът на първата основна област се базира на това, че нормите на материалното и процесуалното наказателно право стоят в основата на цялостния процес за противодействие срещу киберпрестъпността. Ниската ефективност на тези норми и съществуващите различия между тях в законодателните стандарти на различните държави затрудняват и често възпрепятстват противодействието срещу киберпрестъпността, най-вече в нейните форми с международен характер. Развитието и прилагането на тези норми изискват способности от страна на органите за разследване, разкриване и правоприлагане в случаи на киберпрестъпления. Тези способности включват човешки потенциал с необходимото обучение и практически опит, адекватни информационни, финансови и материални ресурси, визии, доктрини и стратегии за противодействие.

Основните предизвикателства в избраните две главни области в случаи на разкриване, разследване и правоприлагане при киберпрестъпления с международен характер могат да бъдат определени по следния начин:

- нормативна база: остаряло и непълно законодателство при различните държави; несъответствие при условията за инкриминиране/криминализиране на престъпните деяния в киберпространството; значително разминаване в съдържанието на законодателните стандарти на развитите и развиващите се страни и т.н.
- способности за разкриване, разследване и правоприлагане в случаи на киберпрестъпление: недостатъчен брой квалифицирани експерти, работещи в областта на киберпрестъпленията; неефективни процесуални норми, особено в случаи на киберпрестъпления с международен характер; липса на специфични инструменти за разкриване и разследване на киберпрестъпления, отговарящи на техните особености, идващи от средата, в която същите се извършват и т.н.

Изброените предизвикателства в разглежданите две главни области дават възможност за формулиране на стратегическите цели, които биха довели до подобряване на противодействието срещу киберпрестъпността. Разглеждани по области тези стратегически цели могат да бъдат формулирани по следния начин:

- по отношение на нормативната база: повишаване на ефективността на нормите от материалното и процесуалното наказателно право, релевантни към разкриване, разследване и правоприлагане при киберпрестъпления с акцент върху съответствие на тези норми при противодействие срещу международни киберпрестъпления;
- по отношение на способности за противодействие: развитие на способностите и повишаване на тяхната ефективност при разкриване, разследване и правоприлагане при локални и международни киберпрестъпления по системен начин с отчитане на състоянието на отделните компоненти на тези способности.

Постигането на така дефинираните цели е свързано с формулирането и изпълнението на конкретни оперативни дейности, структурирането на които е представено при построяването на модела за измерване на способностите за противодействие срещу киберпрестъпността.

Модел за измерване на степента за изпълнение на стратегията за противодействие срещу киберпрестъпността

Степента за изпълнение на стратегията за противодействие срещу киберпрестъпността изисква създаване на инструмент, с помощта на който да бъдат измервани постиганите резултати и тяхното сравняване с желаните/целевите стойности. В структурата на този модел се включват следните компоненти: главни области на измерването; цели за постигане в главните области, нива на постиганите способности, оперативни дейности за всяка от целите и всяко от нивата; метрики за измерване на резултатите от оперативните дейности и за задаване на желаните/целевите стойности.

Развити на базата на горната структура моделът за измерване на степента за изпълнение на стратегията за противодействие срещу киберпрестъпността има следния вид:

Главна област 1: Нормативна база за противодействие срещу киберпрестъпления

Стратегическа цел: Поддържане и развитие на адекватна на средата за сигурност нормативна база за противодействие срещу киберпрестъпността.

Ниво 1

Оперативна дейност 1: Нормативните актове в сферата на противодействието срещу киберпрестъпността се разработват на базата на несистемен подход и при възникване на необходимост

Оперативна дейност 2: Транспонирането на европейските документи в сферата на противодействието срещу киберпрестъпността се извършва със закъснение и в непълен обхват.

Оперативна дейност 3: Институциите, ангажирани с нормативната база за противодействие срещу киберпрестъпността работят при отсъствие на процедури за съгласуваност.

Ниво 2

Оперативна дейност 4: Налице е системен подход при разработването на нормативни актове в сферата на противодействието срещу киберпрестъпността.

Оперативна дейност 5: Европейските директиви в областта на противодействието срещу киберпрестъпността се транспонират в националното законодателство своевременно и в пълен обем.

Оперативна дейност 6: Налице са синхронизирани механизми за съгласуване на работата на институциите с ангажименти по нормативните актове, свързани с киберпрестъпността.

Ниво 3

Оперативна дейност 7: Подходът, прилаган при разработването и актуализирането на нормативните документи по противодействието срещу киберпрестъпността периодично се преглежда и актуализира в посока към повишаване на неговата ефективност.

Оперативна дейност 8: Съществува механизъм за усъвършенстване на механизма за транспониране на европейските директиви в сферата на противодействие срещу киберпрестъпността.

Оперативна дейност 9: Механизмите за съгласуване на работата на отговорните институции в сферата на законодателството за противодействие срещу киберпрестъпността периодично се преглеждат и актуализират.

Главна област 2: Способности за разкриване, разследване и правоприлагане при киберпрестъпления

Стратегическа цел: Повишаване на степента на способности за разкриване, разследване и правоприлагане при киберпрестъпления до ниво, адекватно за средата за сигурност.

Ниво 1

Оперативна дейност 1: Решенията за промяна в способностите за разкриване, разследване и правоприлагане при киберпрестъпления се взимат ad-hoc при отсъствие на системност.

Оперативна дейност 2: Капацитета на институциите, ангажирани с оперативни действия при киберпрестъпления не са адекватни на мащабите на киберпрестъпността.

Оперативна дейност 3: Способностите за противодействие срещу киберпрестъпността не се актуализират на базата на адекватни сценарии.

Ниво 2

Оперативна дейност 4: Решенията за промяна на способностите за противодействие срещу киберпрестъпността се актуализират на базата на разработена методика.

Оперативна дейност 5: Капацитетът на институциите, ангажирани с оперативните действия при киберпрестъпления отговарят на мащабите на киберпрестъпността.

Оперативна дейност 6: Способностите за противодействие срещу киберпрестъпността се актуализират на базата на сценарии, разработени на базата на специална методика.

Ниво 3

Оперативна дейност 7: Методиката за взимане на решение относно развитие на способностите за противодействие срещу киберпрестъпността периодично се преглежда и актуализира.

Оперативна дейност 8: Капацитетът на институциите, ангажирани с оперативните дейности при киберпрестъпления редовно се оценява и развива.

Оперативна дейност 9: Методиката за разработване на сценариите за оценяване на способностите за разкриване, разследване и правоприлагане при киберпрестъпления периодично се преглежда и подобрява.

Описаният по-горе модел има следните особености:

- нивата за изграждане на способности са кумулативни, което означава, че за да бъдат изградени способности от ниво три трябва предварително да са изградени способностите от нива едно и два;
- използването на модела изисква първоначално определяне на целевите стойности за нивата на способности във всяка от главните области;
- не се препоръчва стремеж към максималното трето ниво на способностите за всяка от отчитаните области. Целевите нива следва да отчитат реалните възможности и потребности.
- моделът може да бъде използван както за първоначална оценка на степента за изпълнение на стратегията за противодействие срещу киберпрестъпността, така и за следващи оперативни оценки.

ЗАКЛЮЧЕНИЕ

Стратегията за противодействие срещу киберпрестъпността играе ролята на инструмент за повишаване на ефективността на борбата с киберпрестъпниците, но не е панацея. Постиганите резултати зависят в еднаква степен от начина, по който е разработена стратегията, както и от начина за нейното прилагане. Разработеният модел няма претенциите за изчерпателност, но може да послужи за основа на дискусия по релевантните теми.

ИЗПОЛЗВАНА ЛИТЕРАТУРА

[1] Seger, A. *Cybercrime strategies*, Discussion paper, 2012, https://rm.coe.int/16802fa3e1

[2] National Cybersecurity Strategy (2023).| The White House, Washington, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

[3] National Cyber Strategy. Annual Progress Report 2022-2023 (2022) Cabinet Office https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1180089/14.283_CO_National_Cyber_Strategy_Progress_Report_Web_v3.pdf

[4] The Danish National Strategy Cyber and Information Security (2022), https://en.digst.dk/strategy/the-danish-national-strategy-for-cyber-and-information-security/

[5] National Cyber Security Strategy (2013). Departamento de Seguridad Nacional, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_ESen.pdf

[6] Cybersecurity in Ukraine: National Strategy and International cooperation (2017), https://thegfce.org/cybersecurity-in-ukraine-national-strategy-and-international-cooperation/

[7] Актуализирана национална стратегия за киберсигурност: Киберустойчива България 2023. (2021), София, Министерски съвет, https://www.strategy.bg/StrategicDocuments/View.aspx?lang=bg-BG&Id=1587

[8] *National Plan to Combat Cybercrime*, Australian Government, 2022,

https://www.homeaffairs.gov.au/criminal-justice/files/national-plan-combat-cybercrime-2022.pdf

[9] Георгиев, В. *Противодействие срещу киберпрестъпността* (София, 2020).

[10] *Cyber Crime Strategy*, Home Department, 2010, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/228826/7842.pdf

[11] “What is cybercrime? How to protect yourself from cybercrime,” *Kaspersky*, 2022, https://www.kaspersky.com/resource-center/threats/what-is-cybercrime

[12] „Топ 10 на българските градове с най-много киберпрестъпления,“ *Questo*, 2021, https://questona.com/gradove-s-nai-mnogo-kiberprestaplenia/

[13] Видев, Д. „Ръст на киберпрестъпността и домашното насилие през 2021-ва,“ Българско национално радио, 2022, https://bnr.bg/post/101625182/rast-na-domashnoto-nasilie-kiberprestapnostta-i-patnite-proizshestvia-prez-2021-va