СТРАТЕГИЧЕСКИ АСПЕКТ НА КИБЕРСИГУРНОСТТА НА НАЦИОНАЛНО И РЕГИОНАЛНО РАВНИЩЕ

доц. д-р Венелин ГЕОРГИЕВ
департамент „Национална и международна сигурност“, НБУ

Резюме: Успешното решаване на проблемите пред сигурността на различни равнища на сигурност зависи от редица фактори, сред които намира място синхронът и приемствеността в политиките и стратегии за справяне с тези проблеми. Това твърдение е в сила и по отношение на проблемите пред киберсигурността. От друга страна характерът на стратегията за киберсигурност изразява намеренията на нейните автори за начинът, по който се очаква да бъдат използвани ресурсите за постигане на целите в областта на сигурността на киберпространството. В доклада се представят резултатите от проведено изследване на стратегиите за киберсигурност на България и на ЕС, в основата на което се поставя тезата, че успехът на стратегическите документи в областта на киберсигурността на различни равнища на сигурност в значителна степен зависи от степента на тяхната приемственост и съгласуваност по отношение на принципите, мерките и действията.

Ключови думи: киберсигурност, стратегия, устойчивост, киберпространство, киберпрестъпление

Въведение

Съвременните анализи на заплахите за сигурността извеждат на преден план тези, свързани с използване на информационните и комуникационните технологии, системи и мрежи в бизнеса и бита, познати като заплахи за киберсигурността или още заплахи в киберпространството. Сред основните аргументи за тази констатация намират място нарастващият дял на on-line услугите, увеличаването на броя на хората, разполагащи с достъп до интернет, нарастващият брой на престъпленията, експлоатиращи първите два фактора и т.н. Значимостта на заплахите за киберсигурността изискват фокусиране на вниманието върху съществуващите уязвимости и върху способностите за справяне с тях, което в комплексния си вид изисква провеждане на адекватни изследвания в областта.

В доклада се представят резултатите от направено изследване, в което като цел се поставя определяне на характера на предлаганата за обсъждане национална стратегия за киберсигурност „Кибер устойчива България 2020“ и степента на приемственост и съгласуваност на тази стратегия с аналогичната на нея, отнасяща се до регионално ниво на сигурност „Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace“. Тезата, доказването на която се преследва в рамките на изследването се състои в това, че успехът на стратегическите документи в областта на киберсигурността на различни равнища на сигурност в значителна степен зависи от степента на тяхната приемственост и съгласуваност по отношение на принципите, мерките и действията. Изследователската методика включва основно използване на

сравнителния анализ, с помощта на който на първо място е определен характерът на националната стратегия, а в последствие е определена степента на сходство с аналогичната стратегия на ЕС.

Определяне на характера на националната стратегия за киберсигурност

Един от възможните подходи за разработване на стратегия, в частност на стратегия за киберсигурност, е чрез използване на резултатите от предварително извършен анализ на силните и слабите страни, на възможностите и заплахите пред изследвания обект, т.е. с помощта на SWOT-анализ. Съчетаването на резултатите в тези четири области в съдържанието на разработваната стратегия дава възможност за създаване на четири типа стратегии[1]:

- настъпателна стратегия (SO), съчетаваща в себе си предимствата на разкритите силни страни при реализиране на възможностите, разкриващи се пред изследвания обект;

- отбранителна стратегия (ST), в съдържанието на която разкритите силни страни се използват за справяне с идентифицираните заплахи;

- стратегия за развитие (WO), характеризираща се със съчетаване на възможностите и слабите страни с идея за тяхното преодоляване;

- сдържаща стратегия (WT), при която усилията са насочени към отстраняване на идентифицираните слаби страни и снижаване на съществуващите заплахи.

За нуждите на изследването, от текста на националната стратегия за киберсигурност за извадени десет произволно избрани зависимости (логически връзки), за които е определено коя от изброените по-горе зависимости е в сила. Като източник на информация за силните и слабите страни, възможностите и заплахите за киберсигурността са използвани резултатите от SWOT-анализа, публикувани в края на документа. Резултатите от проведеното изследване са представени в таблица 1.

Таблица 1. Характер на логическите връзки в националната стратегия за киберсигурност

Развитие на стратегии, политики и мерки	**W**	**O**	Постигане на високо равнище на мрежова и информационна сигурност
Изграждане на собствен организа - ционен и технически капацитет на бизнеса	**W**	**O**	Запазване на устойчивостта на киберпространството
Използване на партньорството с операторите на критична инфраструктура	**S**	**W**	Създаване на общи и специфични стандарти за киберсигурност
Хармонизиране на националното законодателство	**W**	**O**	Извеждане на тенденциите в заплахите за киберсигурността
Разкриване и разследване на	**S**	**W**	Създаване на мерки за ранно

[1]Георгиев В. Информационно-аналитична дейност в системата за сигурност. София, Авангард, 2015

киберпрестъпленията			идентифициране, откриване и превенция
Повишаване на информираността на потребителите	**W**	**O**	Избягване на престъпните деяния в киберпространството
Използване на форми за публично-частно партньорство	**S**	**O**	Повишаване на сигурността на връзките и инфраструктурата
Развитие на политиките и доктрините на въоръжените сили	**O**	**W**	Развитие на способностите за киберсигурност
Създаване на експертен капацитет за киберотбрана	**S**	**O**	Провеждане на периодични обучение и тренировки
Специализация на България в областта на киберотбраната	**W**	**O**	Създаване на адекватни организационни структури и използване на възможностите на програми за изграждане на центрове и лаборатории

От анализа на резултатите, представени в таблица 1, става ясно, че при избраните логически връзки от текста на националната стратегия за киберсигурност преобладават тези от типа слаби страни – възможности WO (60%), което дава основание да се направи извода, че стратегията се отнася до групата на т.нар. стратегии за развитие.

Изследване на степента на приемственост и съгласуваност между националната стратегия за киберсигурност и стратегията за киберсигурност на ЕС

Различните равнища на сигурност се характеризират с различен обхват и степен на детайлност на заплахите, уязвимостите, влияещите фактори и мерките за справяне с несигурността. В същото време между различните равнища на сигурност следва да съществува достатъчна степен на приемственост и съгласуваност в изброените направления, с което да се осигури увереност за постигане на желаните резултатите. Тези твърдения са в сила и по отношение на равнищата за киберсигурност, което предизвиква интереса към изследване на степента на съгласуваност между националната стратегия за киберсигурност и стратегията за киберсигурност на ЕС. Изследването е направено с помощта на сравнителен анализ. Критериите, по които е извършено сравнението, са определени по метода на художествена абстракция, при която авторът сам избира кои са съществените критерии, които най-добри биха изразили степента на сходство или различие между изследваните обекти.

Сравнителният анализ на националната стратегия за киберсигурност и стратегията за киберсигурност на ЕС е извършено с помощта на следните критерии:

- съвременна среда за киберсигурност;
- принципи, върху които се изгражда и поддържа киберсигурността;
- приоритети, мерки и дейности в областта на киберсигурността.

Съвременна среда за киберсигурност

В стратегията за киберсигурност на Европейския съюз се прави оценка, че през последните две десетилетия Интернет като цяло и в по-широк аспект киберпространството оказват изключително влияние върху обществата и тяхното развитие в различни области: ежедневен живот, социално взаимодействие, фундаментални права, икономика, сигурност и т.н. Благодарение на своите особености, киберпространството премахва бариерите на физическите и географските граници между отделните страни и техните граждани, като в същото време създава условия за споделяне на данни и информация в глобален мащаб. Информационните и комуникационните технологии се превръщат в гръбнака на икономическото развитие и в същото време представляват критически важен ресурс за икономическия сектор. Успоредно с нарастването на свободата на потребителите в киберпространството, нараства и потребността от защита на техните права и като цяло защита на принципите на демократичното общество и валидността на закона. В документа се прави констатацията, че свободата на on-line услугите и комуникациите се нуждае без съмнение от защитеност и сигурност. Водещата роля в това направление се делегира на отделните държави. От друга страна, частният бизнес се определя като един от големите собственици и потребители в киберпространството, което определя значимостта на неговото място и неговата роля и отговорности за създаване на сигурно киберпространство.

Особено внимание в съдържанието на стратегията на ЕС за киберсигурност следва да се обърне на оценката за това, че случващото се през последните години от една страна доказва предимствата и възможностите, които киберпространството предлага, но от друга страна категорично подчертава уязвимостите пред сигурността на това пространство. Броят на инцидентите с киберсигурността, които в огромната си част са с международен характер, нараства с алармиращи темпове и води до създаване на различен тип кризи в различни области на социално-икономическия живот: кризи със сигурността на веригите за доставка на стоки и услуги; кризи с управлението и функционирането на обекти от критичната инфраструктура и т.н. Оценката на заплахите за киберсигурността по отношение на техния източник е категорична и включва организираната престъпност, международния тероризъм, политически мотиви, държавно спонсорирани атаки, природни бедствия, неумишлени и умишлени човешки действия и др. Характерна особеност е стремежът на киберпрестъпниците да развиват и използват все по-нови, усъвършенствани и иновативни методи и инструменти за добиване на нерегламентиран достъп до компютърни системи и мрежи, кражба на чувствителна информация, извършване на икономически шпионаж и т.н. В страните извън ЕС съществуват държави, чиито правителства използват киберпространството за наблюдение и контролиране на дейността и живота на гражданите.

В проекта на национална стратегия за киберсигурност се посочва тенденцията за целенасочено използване на възможностите на киберпространството за развитие на различни сфери на обществения живот: икономика, социални отношения, култура, наука, образование, политически живот и т.н. Изразена в цифри тази тенденция показва, че близо 60% от домакинствата и над 90% от фирмите разполагат и използват

достъп до Интернет. Освен това 50% от фирмите използват автоматизиран обмен на данни с външни за тях информационни и комуникационни системи. Оценката е, че почти цялата комуникация между бизнеса и публичната администрация е по електронен път, а броят на услугите за гражданите, предоставяни с помощта на Интернет, нараства. Заслужава да се отбележат оценките за това, че на национално ниво страната се нарежда сред първите двадесет страни по осигуряване на скоростен Интернет, което представлява сериозна предпоставка за развитие на предлаганите услуги[2].

Успоредно с ползите от развитието на киберпространството, в проекта за национална стратегия за киберсигурност се изтъква появата на нови свързани заплахи и рискове, източниците на които се търсят в дейността на държавни, военни и терористични организации, индустриален шпионаж, киберпрестъпници, умишлени или неумишлени действия на крайни потребители. Обхватът на мотивите за извършване на киберпрестъпления се оценява като широк и включващ от извличане на икономически ползи до проява на любопитство и демонстриране на надмощие. Заслужава да бъде обърнато внимание на оценката за това, че кибератаките са „асиметрични“, т.е. такива, които с помощта на малки усилия и неголеми инвестиции могат да нанесат огромни поражения, които при това не винаги са предсказуеми.

Обобщаването на резултатите от сравнителния анализ по отношение на съвременната среда за киберсигурност дава възможност да се направи извода, че в съдържанието на проекта за национална стратегия за киберсигурност и стратегията за киберсигурност на ЕС съществува необходимото ниво на синхрон и приемственост, което създава обща или сходна основа за по-нататъшното изследване на проблемите, свързани с киберсигурността.

Принципи, върху които се изгражда и поддържа киберсигурността

В стратегията на ЕС са посочени основните принципи, които служат като основа или като фундамент при създаване на политики, разработване и прилагане на мерки за постигане на приемливо ниво на киберсигурност на регионално равнище. Тези принципи се отнасят до следното[3]:

- прилагане на политики, процедури и мерки за киберсигурност, които отговарят и защитават ключовите ценности на Европейския съюз;

- защита на фундаменталните права на всички актьори в киберпространството, защита на свободата на словото, личното пространство, личните данни и идентичността на гражданите;

- осигуряване на достъп на всеки потребител до Интернет, предлаганите услуги и публичните потоци от информация;

- изграждане и прилагане на ефективни модели за управление в киберпространството, зачитащи демократичните ценности при участие на всички заинтересовани страни;

[2] Национална стратегия за киберсигурност „Кибер устойчива България 2020“ (проект), 2016
[3] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. European Commission, 2013

- споделена отговорност на всички участници в киберпространството по отношение на гарантиране на сигурността.

В проекта за национална стратегия за киберсигурност са изброени принципите, върху които трябва да стъпи изграждането на среда за киберсигурност и на способности за противодействие срещу киберпрестъпността. Централно място в списъка на принципите заема осигуряване на защитата на основните ценности на ЕС и запазване на силата на закона. Като допълващи или подпомагащи принципи са изведени следните[4]:

- неделимост на киберсигурността от националната сигурност;

- защита на правата на гражданите, свободата на словото, личните данни и личния живот на хората;

- пропорционалност на разходите и обхвата на мерките за осигуряване на киберсигурност и значимостта на съответните заплахи и рискове;

- споделена отговорност, намираща израз в прилагане на интегриран подход при разпределение на ролите и отговорностите, свързани с киберсигурността на всички нива на управление и в областите на държавните институции, частния бизнес и гражданите;

- периодична оценка на състоянието на заплахите и рисковете за киберсигурността, както и на способностите за противодействие срещу киберпрестъпността при използване на адекватни методи и интегриране на резултатите в осъвременените варианти на стратегии и пакети от мерки;

- прозрачност при формиране и изпълнение на политиките за киберсигурност и кибер устойчивост;

- ангажираност на всички заинтересовани страни и развиване на адекватни механизми за публично-частно партньорство, мрежово управление и мета-управление;

- съгласуваност с международните ангажименти и принципи на сътрудничество, активно участие в процеса по създаване на общи способности за защита на киберпространството;

- обвързване на целите, приоритетите и мерките от стратегията с конкретен план за действие, отговорности, ресурси и показатели за ефективност.

Сравнителният анализ показва съответствие между принципите, на базата на които се предвижда създаването на мерки за киберсигурност и които са формулирани в проекта за национална стратегия за киберсигурност и стратегията за киберсигурност на ЕС.

Приоритети, мерки и дейности в областта на киберсигурността

Във фокуса на дейностите и мерките за постигане на киберсигурност на регионално равнище са поставени няколко основни зависимости. На първо място в стратегията на ЕС за киберсигурност се посочва стремежа към балансиране на достъпността до киберпространството и сигурността на същото това пространство. Очевидна е обратно пропорционалната зависимост, която свързва тези два параметъра: при увеличаване на достъпността ще намалее сигурността на услугите в

[4] Национална стратегия за киберсигурност „Кибер устойчива България 2020“ (проект), 2016

киберпространството и обратно – засилването на мерките за сигурност като следствие ще снижат достъпността до предлаганите услуги. Търсенето на баланс между достъпност и сигурност се затруднява от една страна предвид динамичния характер на промените в киберпространството и от друга страна за сметка на необходимостта от постигане на баланс на различни нива и между апетитите на риска на различни актьори в киберпространството. Друга зависимост определя отделните държави като носители на основната отговорност за справяне с предизвикателствата пред киберсигурността. В своята цялост, дейностите и мерките, които ЕС определя в стратегията за киберсигурност, могат да бъдат определени като краткосрочни и дългосрочни, включващи изискванията на разнообразни политически документи, изпълнявани от различен тип актьори, опериращи в киберпространството. Всички предвидени мерки и дейности на регионално равнище обслужват зададените в стратегията приоритети, които могат да бъдат определени по следния начин[5]:

- постигане на киберсигурност, която в последствие да прерасне в кибер устойчивост: ключов момент при изграждане на среда за киберсигурност на регионално ниво и възможности за противодействие срещу киберпрестъпността е създаване на общи способности и процедури за ефективно взаимодействие. Съществен компонент на процеса по изграждане на пакет от способности за киберсигурност е обучението на всички участници в киберпространството за разпознаване и противодействие срещу инциденти от различен тип;

- нарастване на степента на готовност за отговор на инциденти с киберсигурността: в основата на този приоритет стои разбирането за това, че киберсигурността представлява обща и споделена отговорност на страните от ЕС, на държавните институции, частния бизнес, академичната общност и отделните потребители. Нещо повече, в стратегията за киберсигурност на ЕС се прави оценката, че крайните потребители на услугите в киберпространството играят ключова роля при осигуряване на сигурността на компютърните системи и мрежи;

- снижаване на размерите на киберпрестъпността в нейните различни нюанси (области): в анализираната стратегия се подчертава факта, че киберпрестъпността към момента е най-бързо развиващата се престъпност на регионално равнище (като пример: за един ден броят на жертвите на киберпрестъпления в световен мащаб се оценява на един милион души). Мерките за повишаване на ефективността на противодействието срещу киберпрестъпността следва да отчитат особеностите на киберпрестъпленията, каквито са: използването на нови технологии; сравнително нисък риск за престъпниците; наличие на висока мотивация, идваща от възможностите за извличане на значителни ползи, в това число и финансови и т.н.

- изграждане на оперативни способности за противодействие срещу киберпрестъпленията: в този аспект в стратегията за киберсигурност на ЕС се прави оценка, че правоприлагащите органи не са в състояние да противодействат по един достатъчно ефективен начин на киберпрестъпленията с помощта на традиционните методи и средства или поне не без комбиниране на традиционните методи и средства

[5] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. European Commission, 2013

със специфични инструменти, отговарящи на особеностите на този вид престъпност. В стратегията се препоръчва на страните да обърнат внимание върху изграждането на специализирани структури и способности за противодействие срещу киберпрестъпността, които освен всичко друго да предполагат достатъчно ефективно международно сътрудничество;

- подобряване на координацията на ниво ЕС при изграждане на среда за киберсигурност и противодействие срещу киберпрестъпленията.

В проекта за национална стратегия за киберсигурност са определени неотложните действия (приоритетите) в областта на киберсигурността. Сред тези приоритети попадат:

- създаване на обща визия, национална стратегия и политика за киберсигурност и кибер устойчивост

- обединяване на капацитета и способностите на всички заинтересовани страни, в това число държава, бизнес, академични, научни и неправителствени организации;

- осигуряване на необходимите човешки, финансови, организационни и технически ресурси за изграждане и поддържане на среда за киберсигурност;

- периодичен преглед и оценка на рисковете за киберсигурността и координиране на стратегиите за противодействие срещу кибер заплахите;

- усъвършенстване на правната рамка и регулаторните механизми в областта на киберсигурността;

- балансиране на мерките по отношение на запазване на правата и свободите на гражданите и изграждане и поддържане на желано ниво на сигурност;

- особено внимание и ангажимент към проблемите на киберсигурността на обектите от критичната инфраструктура;

- компенсиране на сравнителното изоставане от партньорите от НАТО и ЕС в мерките и дейностите във връзка с киберсигурността.

Така изброените приоритети очертават полето от дейности, които са намерили място в проекта за национална стратегия за киберсигурност. В документа тези дейности са групирани в няколко направления, всяко от които е подробно описано. На първо място като област на действие е посочено установяването и развитието на национална система за киберсигурност и кибер устойчивост, която се характеризира с достатъчно високи нива на ефективност и ефикасност. Тази система се разглежда като неделима част на системата за управление и защита на националната сигурност и включва органи и институции с определени роли и задължения на национално и секторно ниво. Съвкупността от мерки, целящи изграждане и поддържане на национална система за киберсигурност включва:

- разработване и внедряване на стратегически документи под формата на политики, стратегии и планове за изграждане на желано ниво на киберсигурност. В организационен аспект стратегията предвижда създаване на Съвет за кибер устойчивост към Министерски съвет с направляващи и стратегически функции. Ролята на секретар на съвета по кибер устойчивост се изпълнява от Националния координатор по киберсигурност;

- постигане на оперативна координираност между всички участници в киберпространството с акцент върху проблемите на сигурността. Стратегията

предвижда на оперативно ниво да се създаде организационна мрежа със съответната техническа платформа, а именно Национална координационно-организационна мрежа за киберсигурност, както и Национален кибер ситуационен център, който да бъде в рамките на Националния ситуационен център;

- изграждане на Национална система за управление при кибер кризи, която да бъде интегрирана част на Националната система за управление при кризи. Управленските процедури при възникване на кибер криза е предвидено да следват насоките от Европейските стандартни оперативни процедури за взаимодействие и модела за взаимодействие и управление при кризи на НАТО.

Втората област от дейности в проекта на стратегия за киберсигурност на България се отнася до мрежовата и информационната сигурност, които се представят като фундамент на кибер устойчивостта. Тези дейности са насочени към:

- постигане на високо общо ниво на мрежова и информационна сигурност във всички сегменти на киберпространството;

- постигане на сигурност и устойчивост на комуникационните и информационните системи на държавните институции, администрацията и електронното управление;

- ангажиране на частния сектор в подобряване на мрежовата и информационната сигурност;

- развитие от киберсигурност към кибер устойчивост.

Следващата група дейности в проекта за национална стратегия за киберсигурност касае защитата и устойчивостта на дигитално зависимата критична инфраструктура и целят гарантиране на надеждно и безпроблемно изпълнение на основните функции на тази чувствителна от гледна точка на сигурността система. Като основни направления за развитие на дейностите в това направление се разглеждат:

- подобряването на взаимодействието между държавата и операторите на критични инфраструктури. Като възможни инструменти се посочват разпределението на ангажиментите и засилване на сътрудничеството между държавата и операторите на критична инфраструктура, изработване и внедряване на общи и специфични стандарти за киберсигурност, прилагане на процес за оценяване и управление на рисковете за киберсигурността, въвеждане на оперативни процедури за комуникация и координация в условия на кибер криза и др.

- развитие и модернизация на системата за управление и защита на критична инфраструктура;

- своевременна защита на новите области на киберпространството, появяващи се за сметка на разширяване на оценката за критичност на информационните и комуникационни системи.

Като обособена група от дейности, към които са насочени мерките в проекта за национална стратегия за киберсигурност са определени тези, свързани с подобряване на взаимодействието и споделяне на информация между държава, бизнес и общество. Тези мерки са разделени в следните групи:

- установяване на ефективни механизми за споделяне на информация и ангажираност на всички заинтересовани лица, което включва идентифициране на тези лица; определяне на техните роли, интереси и адекватни форми за участие в

националната система за киберсигурност; създаване на условия за споделяне на информация чрез изграждане на колективни платформи; изграждане на доверие за обмен на информация чрез използване на адекватни протоколи и правила; установяване на ефективно публично-частно партньорство за киберсигурност

- развитие на индустриален технологичен капацитет и споделени способности, което да бъде постигнато за сметка на технологично развитие на индустрията, модернизация и интелигентна специализация; изграждане на технологични паркове, центрове за върхови постижения и центрове за компетентност; създаване на достатъчно ефективни механизми за споделяне на ресурси, капацитет и способности за киберсигурност; стимулиране на националните и мултинационалните компании в областта на информационните и комуникационни системи;

- фокус върху малкия и среден бизнес, към който ще бъдат отправени предложения под формата на проекти и програми за развитие на конкурентоспособността чрез изграждане на адекватна кибер култура; включване в мрежите за превенция и споделяне на информация; организиране на специфични секторни и между-секторни упражнения, симулации и учения;

- установяване на обща комуникационна стратегия за информираност относно кибер въздействия и противодействия;

- изграждане на сигурна, свободна и достъпна интернет среда посредством адаптиране и прилагане на препоръките на международните интернет институции и организации.

Анализът на съдържанието на двете стратегии в частта им, описваща приоритетите, мерките и дейностите в областта на киберсигурността, показва наличие на сходство и приемственост.

Заключение

Резултатите от проведеното изследване, които са представени в доклада, дават възможност да бъдат направени два основни извода. На първо място може да се каже, че определеният характер на националната стратегия за киберсигурност като „стратегия за развитие“ отговаря на намеренията на страната да изгражда способности за киберсигурност, да си партнира със страните от НАТО и ЕС в тази област и дори в определени сегменти да се пребори за заемане на водеща роля. На второ място резултатите от изследването доказват наличието на видима степен на съгласуваност и приемственост между двата аналогични документа, отнасящи се до национално и регионално равнище на сигурност. Този факт засилва положителните очаквания за приноса, който стратегиите за киберсигурност ще осигурят по пътя към изграждане на сигурно киберпространство и преход към кибер устойчивост. Като цяло може да се каже също така, че резултатите от изследването потвърждават формулираната теза, доказват постигането на целта и като следствие определят приноса на самото изследване към решаване на проблемите по справяне със заплахите за киберсигурността.

Използвана литература

1. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. European Commission, 2013

2. Национална стратегия за киберсигурност „Кибер устойчива България 2020“ (проект), 2016

3. Георгиев В. Информационно-аналитична дейност в системата за сигурност. София, Авангард, 2015