# ОБМЕН НА ИНФОРМАЦИЯ ЗА КИБЕРИГУРНОСТТА ЧРЕЗ ПУБЛИЧНО-ЧАСТНО ПАРТНЬОРСТВО

# EXCHANGING THE CYBERSECURITY INFORMATION THROUGH PUBLIC AND PRIVATE PARTNERSHIP

**Todor Todorov**[1, 2]
[1]*Faculty of Mathematics and Informatics, St. Cyril and St. Methodius University of Veliko Tarnovo, Veliko Tarnovo, Bulgaria*
[2]*Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, Sofia, Bulgaria*
*t.todorov@ts.uni-vt.bg*

**Shpend Lutfiu**[1]
[1]*Faculty of Mathematics and Informatics, St. Cyril and St. Methodius University of Veliko Tarnovo, Veliko Tarnovo, Bulgaria*
*shpendlutfiu@gmail.com*

**Abstract**

*An important component of a coordinated response in the field of cyber security is the exchange of information between the parties related to the perpetrators and the methods they use, and based on this information to take concrete actions in preventing the dangers that appear in cyberspace.*

*In the paper are considered issues related to exchanging the information between public institutions and private sector in order to prevent the cybersecurity threats.*

**Keywords:** cyber security • information sharing • threats prevention • partnership.

## ВЪВЕДЕНИЕ

Изграждането на информационно общество изисква укрепване на доверието в информационните и комуникационни технологии (ИКТ), изисква личните данни и поверителността да бъдат защитени и насърчава глобалната култура на киберсигурност в контекст, в който обществата по света са все по-зависими от информационните и комуникационните технологии и като резултат може да бъде обект на киберпрестъпност [7], [8].

Правителствата в рамките на една държава не могат да защитават само киберпространството, защото не притежават и не управляват публична инфраструктура за електронни комуникации. Публичните мрежи и услуги, разположени в националния кибер домейн, в повечето случаи не са под контрола на правителствата и това подчертава необходимостта от публично-частно сътрудничество в обмена на информация и ранното откриване на кибер заплахи.

Националните стратегии за киберсигурност, разработени от правителствата, трябва да включват и да се консултират с частния сектор при разработването, прилагането на разпоредби, инициативи и политики в областта на киберсигурността [4].

Близкото и правилно публично-частно сътрудничество е от жизненоважно значение, тъй като:

- Улеснява обмена на информация за развитието на законодателството и новите регулации между заинтересованите страни;
- Осигурява съвместна работа и обмен на курсове за обучение, които могат да помогнат за облекчаване на изразения недостиг на квалифицирани специалисти по киберсигурност;
- Активира обмена на информация в реално време за заплахи и уязвимости онлайн. Комуникационният канал е ценен за Националните Екипи на Общността за реагиране при извънредни ситуации (CERT), тъй като обменът допълва разширените национални източници за откриване и предупреждение на заплахи;

Координацията на публично-частните партньорства е от съществено значение за защитата на критичната инфраструктура, тъй като подобрява обмена на информация и сътрудничеството при идентифициране на онлайн заплахи, реагиране на инциденти и предприемане на мерки за справяне със ситуацията.

Чрез обмен на информация между организациите може да се постигне разбиране на техническите методи и методите на атака. Обменът на стратегии, техники и процедури (TTP) позволява на организациите да принудят зложелателите да работят по-усилено върху всяка цел.

## СЪТРУДНИЧЕСТВО И ОБМЕН НА ИНФОРМАЦИЯ

Неуспехът на сътрудничеството между публичния и частния сектор при обмена на информация за киберсигурност може да бъде формулиран съгласно следните хипотези [1]:

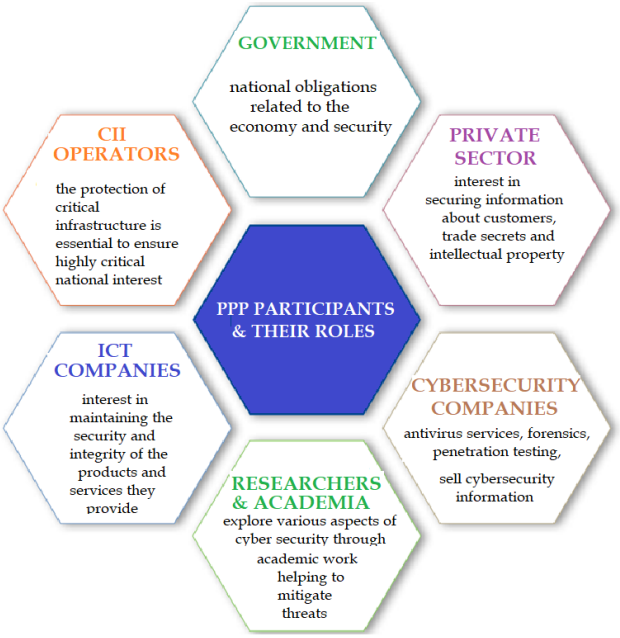
- Участие в публично-частното сътрудничество не възниква, ако страните не са склонни да споделят информация за кибер заплахите по подходящ и точен начин;
- Частният сектор, основан на задължението да спазва необходимите стандарти за сигурност, не е склонен да инвестира в стандартите за сигурност, ако първоначално няма финансов стимул от правителството;
- Като цяло частният сектор няма необходимите ресурси за участие в публично-частното сътрудничество при обмена на информация.

За да създаване на политики за устойчиво сътрудничество при обмена на информация, трябва да се съблюдават следните цели:

- За да участват в публично-частното сътрудничество, първо трябва да бъдат идентифицирани участващите страни, които имат капацитет да се справят със заплахите и инцидентите в киберсигурността;
- Насърчаване и повишаване на доверието между страните;
- Модели на сътрудничество и обмен между страните, регламентирани от съответните процедури;
- Определяне на видовете информация, която ще се обменя въз основа на добре дефинирана таксономия за класифициране на инциденти, заплахи и уязвимости, включително целта и обработката на информацията от страните;
- Технически механизми за обмен чрез платформи за обмен на информация.

## Страните и тяхната роля

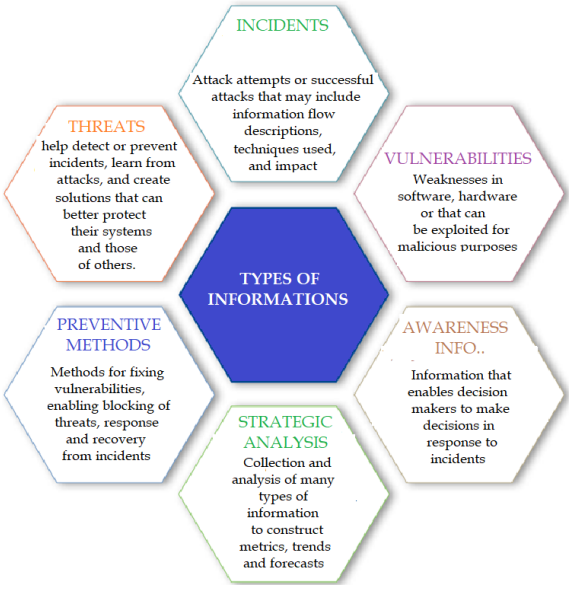
Страните, участващи в публично-частни партньорства, както и в обмена на информация относно заплахите и инцидентите в областта на киберсигурността, както и друга информация, имат различни интереси и нужди и всеки трябва да бъде разгледан от собствената си гледна точка, когато регулира това сътрудничество. Техническите възможности, видовете кибер инциденти и заплахи също могат да варират. Разбирането на стойността на всяка страна, както и повишаването на доверието чрез определяне на критериите за участие между страните е от решаващо значение. Следващата фигура представя страните и тяхната роля в публично-частното сътрудничество:




**Фиг. 1.** Страните и тяхната роля в публично-частното сътрудничество

## Видове информация

Като цяло има седем вида информация, които могат да се споделят в общностите за киберсигурност. Всеки тип информация има различно приложение. Част от тази информация помага на правителството и частния сектор при оценката на риска от киберсигурност на национално ниво или на нивото на други страни, участващи в публично-частни партньорства, включително риск от критична инфраструктура.




**Фиг. 2.** Видове информация за обмен между страните

## МОДЕЛИ НА СЪТРУДНИЧЕСТВО

Различните подходи на моделите за обмен на информация се основават главно на доверието между страните, правната рамка, според която действат различните участници, и отношенията на сътрудничество между страните. Тези модели варират от спорадично ad-hoc обмен на информация до дългосрочен обмен, регулиран чрез правно обвързващи официални споразумения. Всеки от моделите има своите предимства и недостатъци, но изборът на подходящ модел е жизненоважен за гарантиране на успех при предотвратяване на рисковете и предприемане на подходящи действия при реагиране на инциденти в киберсигурността [2], [3], [5].

### Доброволен обмен на информация

Доброволният обмен на информация е може би най-ценният обмен, който съществува в пространството за киберсигурност. Чрез доброволно споделяне на информация страните идентифицират необходимост или причина за обмен на информация, като споделят и използват тази информация, която е ценна и значима за предприемане на подходящи действия. Правителствата и компаниите често решават с кого да споделят информация въз основа на типа информация и целите на страните.

Нуждите на правителствата за национална сигурност му дават ясен мандат да споделят важна информация с индустрията, особено информация, свързана със заплахи и уязвимости.

По същия начин доброволните усилия в частния сектор могат да бъдат двустранни или да включват група от субекти. Субектите от частния сектор често споделят информация за инциденти, заплахи, уязвимости и смекчаване, наред с други неща:

- Допринасят за национална колективна защита или отговор;
- Защитават клиентите и техните продукти;
- Информират властите за сериозни ситуации;
- Докладват за престъпна дейност.

В някои случаи компания от частния сектор доброволно споделят информация както с индустрията, така и с правителството.

Най-ефективните сценарии за обмен на информация изглежда са обмен между частни компании в допълнение към колективните реакции на големи инциденти или заплахи.

По този начин, подобно на правителствата, те се стремят да разработят по-ефективни режими за обмен на информация или задължения за докладване на инциденти, трябва да обмислят как да задълбочат доверието, да осигурят колективна изгода чрез минимизиране на риска за репутацията и да реагират на ясно формулиран национален инцидент.

И накрая, също така си струва да се отбележи, че част от информацията за киберсигурността се обменя чрез търговски продажби от охранителни компании и изследователи. Поради увеличаването на информацията за заплахи, инциденти и уязвимости се появи значителен пазар, който да отговори на търсенето на по-добра сигурност. Фирмите за частни инциденти и съдебни експерти наскоро станаха важни като реагиращи на нарушения и действащи по собствена информация или по информацията, споделена от трети страни. Въпреки това, определена закупена информация може да се използва извън предвиденото й предназначение (например за използване на системите), така че е важно всяка такава информация да бъде защитена.

**Принудителен обмен и разкриване на информация**

Правителствата все по-често изискват обмен на информация за събития в областта на сигурността въз основа на публично-частни партньорства между страни с отговорности в областта на киберсигурността. Въпреки че понастоящем разпоредбите за разкриване на информация са ограничени в повечето страни, има непрекъснат натиск, който изисква докладване на инциденти, особено когато инцидентът засяга критична инфраструктура.

Въз основа на Директивата за NIS, приета от Европейската комисия, е определено допълнително изискване операторите на пазара да докладват инциденти, които имат сериозно въздействие върху държавните органи.

Има опасения, че задължителният подход при докладването на инциденти ще отклони вниманието от най-важния акцент върху споделянето на информация или реагирането на инциденти. От решаващо значение е правителствата да не комбинират отчитането на инциденти или необходимостта им да повишат осведомеността за ситуацията с обмена на информация между доверени страни.

Нещо повече, предложенията за преминаване от доброволно споделяне на информация към задължително споделяне на информация обикновено са били неохотно получени от частния сектор. Задължителното докладване на инциденти е по същество мениджър и само по себе си не подобрява безопасността на експлоатацията или нейната реакция. Често акцентът е върху самото отчитане, а не върху това как ще се използва събраната информация, поставяйки под въпрос основните цели на задължителното докладване. От решаващо значение е задължителното докладване на инциденти да бъде ясно фокусирано и тясно съгласувано, за да се гарантира, че докладваните данни се използват за подобряване на сигурността и че поверителността е защитена.

## ПРОТОКОЛ ЗА ОБМЕН НА ИНФОРМАЦИЯ - TRAFFIC LIGHT PROTOCOL (TLP)

Протоколът (TLP) е създаден, за да насърчи най-добрия обмен на чувствителна (но некласифицирана) информация в областта на киберсигурността [6]. Подателят на тази информация трябва да посочи къде информацията може да изтече извън непосредствения получател и това трябва да се консултира с първоначалния подател, когато информацията трябва да бъде разпространена до трети страни.
Използва се четирицветен код, чието значение може да се намери в следната таблица:

**TLP categories**

| | |
|---|---|
| TLP-RED | "For your eyes only". Only to be used by you and not to be spread to other people, even within your own organisation. |
| TLP-AMBER | To be used and shared with co-workers within your organisation on a need-to-know basis and with clients or customers who need to know this information to protect themselves or prevent further damage. |
| TLP-GREEN | Used for information that is not very sensitive and can be shared with partners and peers, but not via publicly accessible channels (e.g. websites). |
| TLP-WHITE | Public information that can be shared freely, taking into account standard copyright rules. |

Авторът трябва да провери информацията с правилния цвят, за да посочи целта, която TLP разпространява такава информация, обикновено включваща текста „TLP: COLOR" в горната и долната част на документа, като използва цветовете в горната таблица.

Ако получателят трябва да разпространява тази информация на трети страни извън обхвата на посочения TLP, той трябва да се позовава на източника на информацията.

TLP е проста и интуитивна схема за показване кога и колко чувствителна информация за киберсигурността ще бъде споделена и улеснява сътрудничеството с други образувания или организации на национално и международно ниво.

Определението за TLP не е категория или подкатегория на тези стандарти и трябва да се използва само оперативно.

TLP се използва от публични и частни организации в областта на киберсигурността в повечето страни.

За повече информация относно стандарта TLP, моля, посетете www.first.org/tlp

## ЗАКЛЮЧЕНИЕ

Намаляването на риска от кибер заплахи все повече зависи от обмена на информация и сътрудничеството между страните, като се използват много различни модели, методи и механизми. Създаването на ефективни механизми и процедури за обмен на информация е сложен и труден процес, който изисква ангажираност, доверие и тясно сътрудничество между страните, участващи в публично-частното партньорство.

Опитът, технологиите и процедурите на страните, участващи в публично-частното партньорство, се различават в зависимост от дейностите и отговорностите, които те имат, поради което заплахите, пред които са изправени, могат да бъдат различни, така че такова сътрудничество ще даде възможност за споделяне на практики и опит, особено с публичния сектор, където в повечето случаи този сектор е изправен пред липса на професионални ресурси.

### ЛИТЕРАТУРА

[1] Johnson, T., Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare, Routledge, 2015.
[2] MISP-User Guide Threat Sharing Platform, https://www.circl.lu/doc/misp/book.pdf
[3] National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, CreateSpace Independent Publishing Platform. 2014.
[4] NIS DIRECTIVE, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=GA
[5] Public Private Partnership – Cooperative Models, https://www.enisa.europa.eu/publications/public-private-partnerships-ppp-cooperative-models/at_download/fullReport
[6] Traffic light protocol (TLP), https://www.first.org/tlp/
[7] https://www.securitysales.com/emerging-tech/cybersecurity-tech/cybersecurity-approach-proactive/
[8] https://www.forbes.com/sites/forbestechcouncil/2017/01/17/why-cybersecurity-should-be-the-biggest-concern-of-2017/#712004755218