**Сценариен анализ на обществените мнения по отношение на киберсигурността**

Темата за киберсигурността на пръв поглед изглежда не би могла да предизвика полемика, тъй като е широкоизвестно, че често се случват злоупотреби, кражби и т.н. във все по-бързо развиващата се мрежа, но всъщност има мнение, че тя би могла да ограничи някои основни човешки права. Както бизнеса, така и държавния апарат все повече разчитат на системи, които извършват функциите си чрез глобалната мрежа – спестяват много време и финансови средства, но в същото време такива бази данни са уязвими от кибератаки. Дори обикновените потребители, които използват интернет за забавление все по-често стават жертви на такива престъпления.

Разногласието основно произтича от несигурността по няколко основни въпроса: каква система трябва да се изгради, така че да защитава данните, но самата тя да не стане жертва на такива, давайки директен достъп до всичко, което е пазила; доколко е намесен човешкия фактор чрез орган, който следи за сигурността; дали това няма да повлияе на качеството на информацията в мрежата, както и бързината ѝ; по какъв начин ще се формулира съответен закон, който да не позволява подвеждането под отговорност на ползватели на мрежата, които не са планирали и извършвали кибер престъпление, но са изразили мнението си по някой по-деликатен за държавата въпрос.

В целия свят се създава и надгражда нормативната база по отношени на киберсигурността, главно поради зачестяването на кибер престъпления и това, че те стават все по – обиграни - зловредните софтуери се осъвършенстват след всяко противодействие. Заплахите в киберпространството допринасят и за увеличаването на уязвимостта на военни ИКТ системи, системите за командване и управление и тези на критичната инфраструктура. Най-актуалните нормативни актове са *Директивата за мрежова и информационна сигурност*, която трябва да бъде транспонирана в националните законодателства до 9 май 2018 г., и задължителният *регламент 679 за защита на личните данни на физическите лица*, налагащ глоби на редица организации в случай на пробив и изтичане на лични данни.



 Графиката показва съотношението между пострадалите от кибератаки, като основните три са производството, отделни индивиди и правителствата. Според оценката на Европол на организираната престъпност в интернет, основните приоритети за киберсигурността следва да са:

* кибер-зависимо престъпление
* сексуална експлоатация на деца онлайн
* платежна измама
* онлайн криминални пазари

Становището е, че правоприлагащите органи трябва да продължат да се съсредоточават върху актьорите, разработващи и предоставящи инструменти и услуги за киберпрестъпността, както и ransomware, банкови троянци и друг злонамерен софтуер, инструменти за атака -DDoS, контра-антивирусни услуги и ботнети.





 Очевидно е, че киберпрестъпността става все по-сериозна заплаха. Поради тази прична е важно да се проследи развитието и процеса по изграждането и прилагането на мерки за сигурност. Ще разгледаме три варианта – оптимистичен, реалистичен и песимистичен с оглед гледните точки на обществото.

**Оптимистичен вариант**

Имайки предвид нуждата от защита на личните и друг тип данни, чрез достатъчно информационни кампании обществото ще бъде склонно да преотстъпи част от личното си пространство в името на сигурността си, ще се довери на системите за сигурност както в бизнеса, така и в държавния сектор. Това ще помогне на борбата с тероризма и превенцията на престъпления спрямо личността. Ще се постигне подходяща отбранителна способност, без да се вреди на бизнес процесите.

**Песимистичен вариант**

Част от обществото ще сметне, че това е ограничаване от техни изконни права, имайки предвид нарушаването на личното пространство, ограничаване на анонимността, налагане на цензура в свободния Интернет, както и достъпа на „контролиращ орган“ до техните комуникации, снимки, файлове и т.н., които индивидите смятат за лични. Няколко примера по света и у нас показват някои от тези вероятности:

* *Случаят с Едуард Сноудън*

 Е. Сноудън разкрива, че американската национална агенция по сигурността събира данни за милиони граждани чрез проследяване на телефонните им обаждания, фейсбук и кореспонденция в други социални мрежи. Това повдига въпроса за държавното наблюдение на аспекти от личното пространство на индивидите. Опасението е, че след като има такава „вратичка“ за държавата, то и други биха могли да достигнат до тези бази данни и да ги трансферират в други сървъри. Достъпът до такава информация може да се даде и от доставчика на интернет. Идеята зад това е превенция на тероризма, но Сноудън смята, че истинските престъпници биха могли да променят поведението си в интернет и да интерпретират кореспонденциите си по различен начин. В данните, които НСА събира се включват и снимки от устройствата, които показват местоположението на собственика им.

* *Други случаи по света*

-В Иран, поради религиозни причини, през 2014 г. Властите са издирили и наказали шестима младежи заради клипче в YouTube. Лицата са осъдени, защото са нарушили забраната да се появяват разбулени публично. Но това предизвика сериозен обществен отклик, тъй като интернет пространството е глобално, мнозина разчитат на анонимността си в него, а в конкретния случай изглежда че властите на Иран са използвали киберсигурността за да наказват по други поводи, далеч от кибер престъпления и от каквото и да е престъпление срещу някого във финансов или психологически план.

- В Русия има над 400 забранени уебсайта, а блогъри с повече от 3000 посещения на ден се третират като медии. В този ред на мисли те неминуемо биват ограничени от свободата да изразяват мнението си, особено когато държавата иа по-деликатна позиция по въпроса. Такъв е случая с инженера от Твер Андрей Бубеев, който е съден по обвинение в публични призиви към екстремизъм и сепаратизъм заради споделяне в социална мрежа на публикация под заглавие "Крим - това е Украйна".Една от най-големите небивалици обаче е съдебното дело срещу блогъра от Ставропол Виктор Краснов, който написал в социална мрежа , че Господ няма. Краснов е съден по обвинение, че е накърнил чувствата на вярващите.

* *Случай от българската действителност*

Специализираният сектор Киберпрестъпност към ГДБОП изпълнява задачи по противодействие на организирани престъпни групи и лица, извършващи нерегламентиран достъп до информационни ресурси, финансови измами, нарушаващи авторски права, кражба на виртуална самоличност и др. Служителите от сектора взаимодействат с правителствени организации, частни фирми, фондации и граждани с цел навременно противодействие на престъпления, в които се използват високотехнологични средства и похвати.

Един конкретен акт на ГДБОП достигна до медиите и въздейства неблагоприятно върху общественото мнение за киберсигурността. Поводът за разпита на Васил Коцев от ГДБОП е негова публикация във Фейсбук. Той е бил посетен в дома си от полицията и твърди, че е имало заплахи за убийство. ГДБОП настояли да им се предостави физически достъп до всичките му електронни устройства. Бил принуден да се „извини“ на премиера.

Всички тези случаи са повод за увеличаване на недоверието в киберсигурността и по-скоро мерките и методите, които се използват. Разкритията на Сноудън засягат нарушаването на личното пространство, в други случаи държавата се намесва и наказва за поведение, което не е регламентирано в правомощията им по опазване на киберпространството, в трети случаи хората са ограничени от правото си на мнение, порицавани за това, че са го изказали, а често дори осъждани.

**Реалистичен вариант, препоръки за оптимизация**

Включващ чертите на оптимистичния и песимистичния. При предприемане на сериозни универсални стъпки в законодателството неминуемо ще има както защитници, така и противници. Поради тази причина е нужно да се създаде правилно законовата уредба, така че „песимистите“ да бъдат по-мотивирани да приемат мерките за киберсигурност. Технологиите непрестанно се развиват, затова и киберсигурността трябва да успява да догонва тяхното темпо, за да се разсее недоверието в системите за съхранение на бази данни.Вероятно няма изцяло да изчезнат атаките, както при оптимистичния вариант, но ще бъде осъществена превенция за голяма част от случаите.



 За да се избегне негативния обществен отклик, трябва да се осъществява контрол по наказанията, основани на употребата на киберпространството. Потребители на мрежата не бива да бъдат подвеждани под отговорност за изразяване на мнението си, стига това мнение да не накърнява директно правата на друг индивид. Киберсигурността следва да отговаря на киберзаплахата, т.е. да се използват инструменти, базирани на това кои сектори всъщност са засягани, да бъде по-специализирана.

 Технологиите са средство, което може да се използва по добър или лош начин. Интернетът може да бъде използван за разпръскването на информация в големи мащаби с лош умисъл. Повечето личности не го разбират достатъчно, а именно разбирането е ключа към създаването на условия за защита от злоупотреби. Киберсигурността неминуемо става все по-важна и нужна, но тя следва да бъде дефинирана конкретно, да има прозрачност относно мерките и методите, използвани за превенция на киберпрестъпления и да се предотврати опълномощаването на дадения орган до твърде висока степен, така че той да предприема анти-демократични действия.

**Основни източници:**

[https://www.europol.europa.eu/iocta/2017/](https://www.europol.europa.eu/iocta/2017/CYBER-DEPENDENT_CRIME.html)

<http://www.cybercrime.bg/bg/internet/>

<http://www.gdbop.bg/bg/cyber>

[24](https://www.24chasa.bg/novini/article/6673390) часа

[БНТ](http://news.bnt.bg/bg/e/kibersigurnost)

Студент: Аделина Стилиянова, ф.н. 78 242

Специалност Публична администрация, 3. курс