DOI: https://doi.org/10.37075/ISA.2022.2.04

Икономически аспекти на модели за оценка на киберсигурност в умни градове

Недко Тагарев*

Резюме: Тази публикация е резултат от УНИВЕРСИТЕТКИ ПРОЕКТ ЗА ИЗСЛЕДВАНИЯ №NID NI-15/2018 „Икономически аспекти на модели за оценка на киберсигурността в интелигентните градове“. Изследването представя е анализира моделите на интелигентните градове, подходите към строителството и ги анализира и сравнява. Показан е модел за киберсигурност на интелигентните градове. Този модел е изграден върху удължен модел на интелигентни градове. Подходът към модела се основава на специфичните уязвимости и заплахи за всеки от модулите. На този етап от изследването започва изграждането на връзката на икономическите ефекти върху киберсигурността. Тази връзка показва, че инвестирането в киберсигурност ускорява дигитализацията. Следващата стъпка от изследването прилага критичен анализ на показателите, традиционно използвани за оценка на киберсигурността. Предлагат се критерии за избор на „добри показатели“. Моделите за изграждане на киберсигурност са сравнени и са показани техните силни и слаби страни. Тези модели могат да се прилагат в комбинация с управление на проекти за модел на киберсигурност или методология за създаване на модел за икономическа оценка на киберсигурността. В подкрепа на модела на икономическа оценка се прилага прагматичната методология за оценка на сигурността. Информацията от различни случаи беше използвана в подкрепа на проекта и беше проведено проучване с потребителите на продукта за киберсигурност.

Ключови думи: интелигентни градове, киберсигурност, икономически аспекти.

JEL: A12, B49, D80, M15.

Въведение

Проблем на изследването е пренебрегването или поставянето на втори план на моделите за оценка на икономическите аспекти на киберсигурността на умните градове. Не са известни предходни изследвания по така зададения проблем, въпреки че концепцията, че киберсигурността е икономически и управленски проблем се защитава още през 90-те години на миналия век. Това се дължи на все още експерименталните приложения на информационните технологии в модерната инфраструктура на 21-ви век. Друга причина за поставянето на заден план на подобни модели за оценка на икономическите аспекти на киберсигурността се обуславя от приоритизирането на техническите и технологичните спецификации при създаването и управлението на подобни модели за умни градове, без да се отчита цената на сигурността. Проблемът може да бъде разглеждан като мултидисциплинарен и обхваща областите на икономическия анализ и управлението на киберсигурността.

* Недко Тагарев е доктор, главен асистент в катедра „Национална и регионална сигурност“ на УНСС.

В близко бъдеще проблемът на изследването ще става все по-актуален. Това ще следва примера на масовото разпространение и употреба на умните телефони, умните битови уреди, умните автомобили, облачните технологии и не на последно място Интернет.

Умните градове ще следват тези тенденции на развитие и разпространение както в производствената дейност и работната среда, така и в бита на хората. Това навлизане ще бъде съпътствано с изисквания към сигурността на тези обекти. Пандемията от COVID-19 е пряко доказателство за масовото навлизане на безчовешките технологии в масова употреба. Пример за това е дистанционното обучение, един от модулите, характерни за умните градове. С тази технология се разполага повече от десет години, но това, което стартира масовата им употреба, беше не толкова очакваното събитие на обявената от Световната здравна организация световна пандемия.

Обект на изследването са модели за киберсигурност в умни градове, а **предмет на изследване** са икономически модели за оценка в умни градове. Авторите предполагат, че доставчиците на умните технологии и услуги предварително са изградили системи за киберсигурност, с минимални изисквания, базирани на съответните законови и нормативни рамки в съответните държави. В България това са „Закон за киберсигурност" и „Наредба за минимални изисквания към мрежовата и информационната сигурност".

Целта на изследването е да се установи дали има модел за икономическа оценка на киберсигурност в умни градове и дали могат да бъдат обхванати различни модели с еднакви характеристики.

В изследването основно ще бъдат използвани следните **методи за анализ** – Приложение на добрите практики, Програмно управление/управление и оценка на проекти; PRAGMATIC Security Metrics; Анкетно проучване между заинтересованите страни.

В настоящата публикация е показана много малка част от направените анализи и изследваните модели. Също така е показана и малка част от анкетното проучване.

1. Модел на умните градове и проблеми с киберсигурността

Броят на умните градове *(градовете, както ще се наричат в текста)* в световен мащаб се очаква да нарасне, като се прогнозираше до 2020 г. пазарният им дял да формира капитализация повече от 1,56 трилиона американски долара (Frost & Sullivan, n.d.). Модернизацията на градовете се съсредоточава върху „умни технологии" (На места в текста се използва изразът интелигентни технологии, по-популярен след 2019 г.) с цел предлагането на по-добро *управление на отпадъците, транспорта, управление на енергията и повишена мобилност*, като по този начин се повишават качеството и стандартът на живот на гражданите. Тези технологии, насочени в определени сектори, наричаме модули.

Умните градове налагат съвременна сигурност и политики за осигуряване на своите данни и мрежи, гарантирайки на бизнеса и жителите на града, че са безопасни и с непрекъсваемост на бизнес процесите. Очаква се гарантирането на безопасността и сигурността да представляват огромни предизвикателства по отношение на разработване и поддържане.

Основният базов модел, върху който се извършва анализът в проекта, е основан на следните елементи:

Умен град/модули на умния град – показва архитектурата и модулите за изграждане на системата спрямо политиките за управление. Модулите на умния град са отделните сектори, които се управляват върху принципите на умните градове. Например здравеопазване, уличен трафик, умна електрическа мрежа и т.н.

Дигитална инфраструктура в умните градове – със своите елементи осигурява

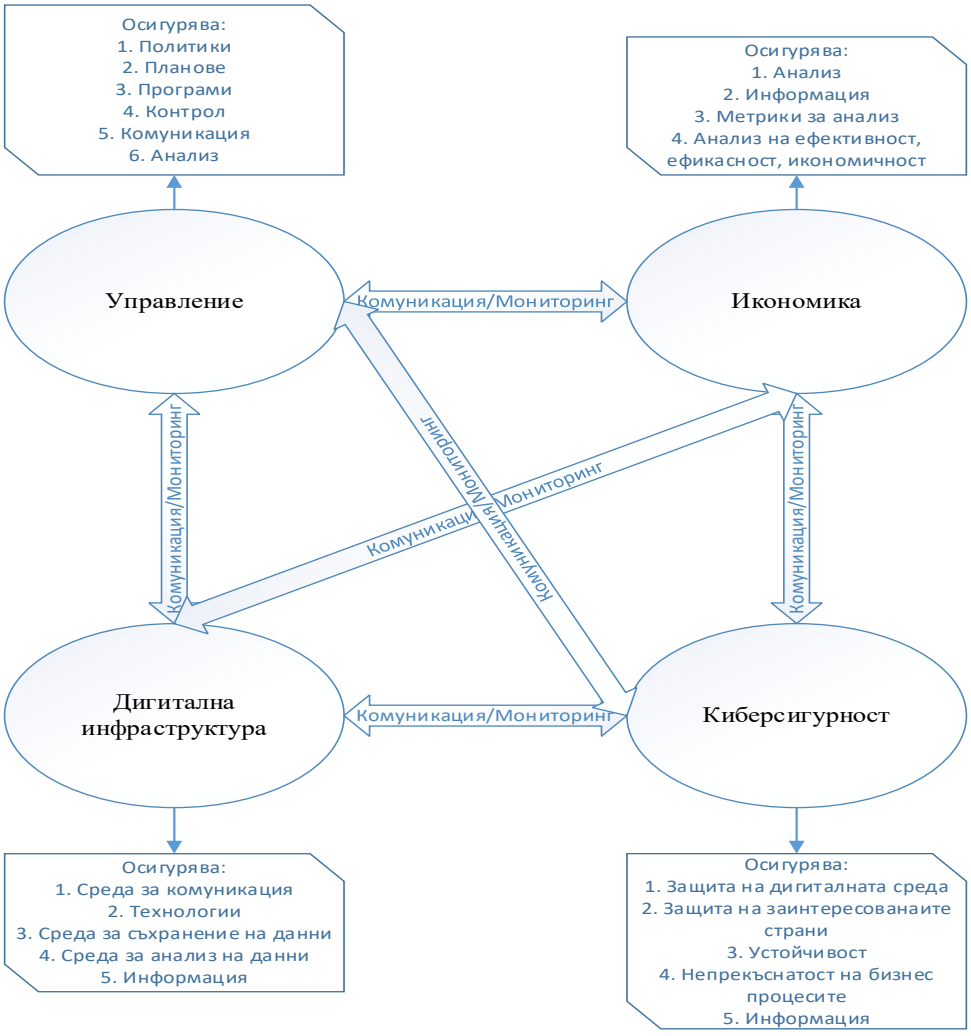
функционирането на умния град. Тя свързва различните модули и осигурява обмена на данни и комуникация.

Киберсигурност в умните градове – осигурява устойчивост и гарантира продължителността на бизнес процесите в умния град.

Управление на умния град – осигурява контрол и мониторинг на процесите, разпределя ресурсите и следи за ефективното и навременно изпълнение на задачите. Управлението може да е централизирано или да бъде насочено спрямо специфичните модули.

Икономически аспекти на сигурността в умните градове – осигуряват метриката за измерване на икономичност, ефективност и ефикасност. Спомагат за определянето на проблемите и дават информация за проектното управление.

Взаимодействието на елементите в умните градове е графично представено във фигура 1.



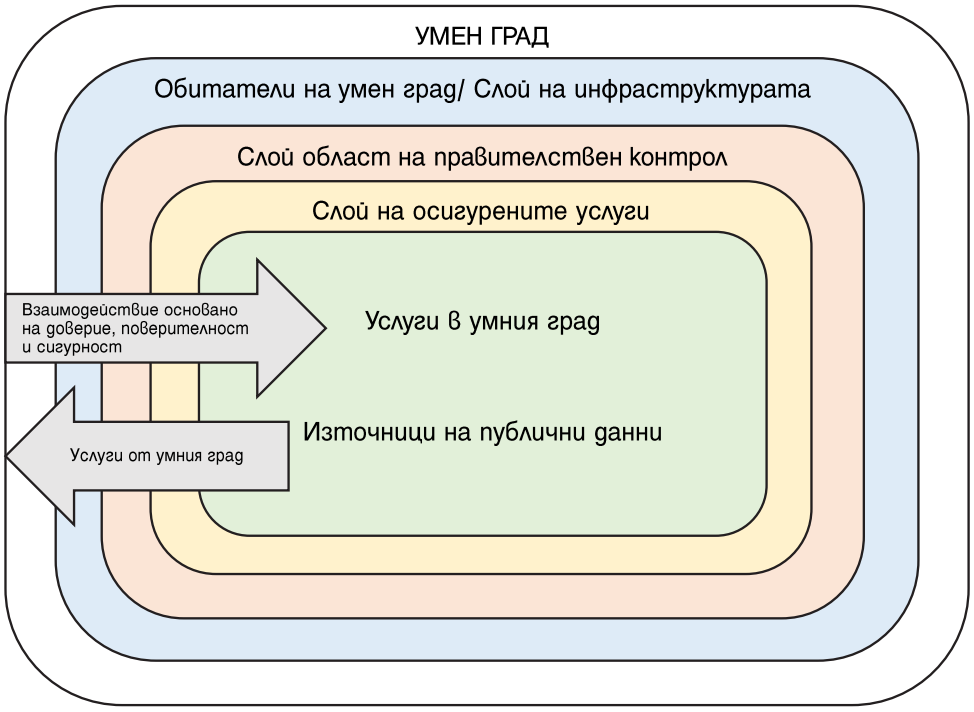
Фигура 1. *Взаимодействие и функции на елементите в умния град*

Първият изследван модел е референтният. При него се разчита на взаимодействието на големи данни. Други от изследваните модели са „многослойният модел“ и „3-слоен onion модел“. Тези модели спомагат за противодействието на постоянно увеличаващата се повърхност на атаката на умната мрежа. Многослойният е подход, при който има система, в която всички умни устройства разполагат с уникален идентификационен номер и функционират на три слоя на сигурност – приложение за защита данните на сървъра, слой за контрол на данните и сигурен умен софтуер за устройства (Braun et al., 2018). 3-Onion Model (фигура 2) се състои от три слоя.

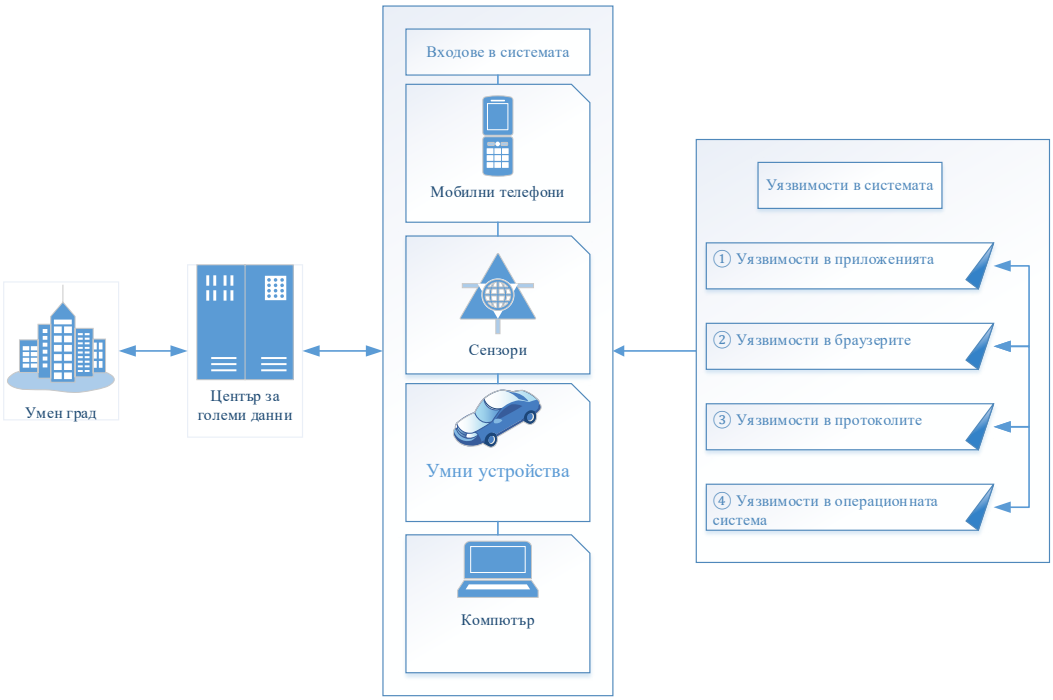
Успешните интелигентни градове адаптират традиционните организационни модели на доставка, за да реализират възможностите на данните и цифровите технологии. Те инвестират в модели на партньорство за цялата система, фокусирани върху споделените резултати. Основният проблем при изграждането на архитектурата на киберсигурност се състои в това, че входовете в системата често са изходите на някои други системи, и изходите на системата се използват като входове към други системи. Трябва да се отбележи, че умният град няма да се разглежда като стандартен йерархичен модел (Vrancken et al., 2009). На всеки градивен елемент трябва да се гледа като на агент с индивидуално поведение в околната среда и агентите могат да бъдат взаимно повлияни (фигура 3).

Основен модел на проекта е модел за сигурност в умните градове, базиран на разширен модел на умни градове и основни уязвимости в модулите.

Повече от 50 процента от хората на планетата живеят в големи градове. Според Организацията на обединените нации,



Фигура 2. *Многослоен модел на умния град*



Фигура 3. *Места за вход в информационната система*

Заплахи	Мерки
Управление на наличността на данни;	Разширени протоколи за криптиране;
Управление на интегритета на данните;	Системи за контрол на достъпа;
Управление на поверителността на данните;	Непрекъснат системен мониторинг за откриване и предотвратяване на неоторизиран достъп;
Наличност на съобщителна среда.	Системи и сървъри за отказ;
	Архивиране и планиране за възстановяване при бедствия.

Фигура 4. *Заплахи и мерки по отношение на ИКТ*

този брой ще нарасне до 70 процента за по-малко от 50 години (United Nations, 2016). В рамките на решенията тип „умни градове“, обществото се сблъсква с три специфични теми, които са: Системна оперативна съвместимост; Платформи; Приложения.

Разширеният модел на умния град включва 16 модула. Моделът на киберсигурност се изгражда спрямо уязвимостите на модула и евентуалните мерки, които могат да бъдат предприети по отношение на сигурността. Като пример може да послужат **уязвимостите при управлението на инфраструктурата на информационните и комуникационните технологии (ИКТ)** (фигура 4).

Управление на наличността на данни. Кибер атакуващите могат да компрометират ИКТ системите чрез отказ на атаки за услуги, измама, атаки за откуп или изтриване с цел да направят услугите или данните недостъпни.

Управление на интегритета на данните. Нарушаването на целостта на данните може да причини големи усложнения. По този начин нападателите могат да повлияят на контрола на достъпа, поведението на операциите или да причинят прекъсвания на градските системи.

Управление на поверителността на данните. Този проблем е свързан с личните данни, които могат да бъдат данни за пациентите в сектора на здравеопазването или финансови детайли, които са привилегировани и трябва да останат поверителни. Проблемите с поверителността на данните за гражданите биха застрашили доверието на лицата в доставчиците на услуги.

Наличност на съобщителна среда. Традиционните проблеми с ИКТ инфраструктурата често се обсъждат като взаимосвързаност на мрежи и устройства в протокола TCP/IP. Експоненциалният растеж на използването на мобилна широколентова връзка означава, че бъдещето на IoT ще включва разчитане на 4G/5G, предоставено от далекосъобщителните доставчици. Тези „доставчици“ също са отговорни за надеждността и сигурността в SMS/MMS пространството, на което гражданите все още разчитат за многофакторно удостоверяване и известия.

Подходящи инструменти за сигурност са **разширени протоколи за криптиране** и **системи за контрол на достъпа** за интелигентни градове, съчетани с **непрекъснат системен мониторинг за откриване и предотвратяване на неоторизиран достъп** и подозрителни изменения на критичната ИКТ инфраструктура и данни. **Системите и сървърите за отказ** също могат да бъдат разгърнати, за да се гарантира, че умният град може да продължава да работи след като активните сървъри са били хакнати.

Интелигентните градове трябва да разработят **архивиране и планиране за възстановяване при бедствия** чрез управление на кризи, за да се подготвят за кибератаки и съпътстващи щети (от бедствия), които биха могли да повлияят на ИКТ инфраструктурата, които биха могли да причинят опустошителни загуби или напълно да блокират услугите. С подходящ план за възстановяване при бедствия, умните градове могат да възстановят компрометираните си системи за минути или часове след инцидент, за да предотвратят по-нататъшни смущения на работните процеси в градската среда.

2. Критичен поглед върху метриките за анализ на киберсигурността

Целта на анализа и избора на правилна метрика е от значение за вземането на правилни решения по отношение на киберсигурността на умните градове. *Резултат от правилните решения е устойчивост на системите и непрекъсваемост на бизнес процесите.* В умните градове е трудно да се приложи метриката или една от метриките за анализ на киберсигурността. Това е продиктувано от множеството възможни точки на атака, което увеличава мащаба на атаката и възможния последващ инцидент. При това положение е от значение оценката на качеството и полезността на входящата информация, процеса на анализ и изходящия продукт под формата на продукт на киберсигурността.

Събираните *данни* се определят от използваната метрика за измерване на *киберсигурността*. Целта на използването на „правилните“ метрики е да се оцени правилно ефективността на киберсигурността и **да може да се обосноват приложените мерки за защита, както и инвестициите**, направени за тях. Процесът на оценка на метриките (SMITH, n.d.) може да се определи в пет етапа: 1) Разпознаването на измерените „лоши“ метрики; 2) Познаване на потребителите; 3) Добри метрики; 4) Обобщение; 5) Допълнителни ресурси за оценка на метриките.

Значението на използваните метрики за измерването на киберсигурността цели да оцени вътрешната среда, с цел да бъдат внедрени мерките за киберсигурност трябва да се *„говори с бизнеса на негов език“*. От друга страна, обективно представяне на проблемите, свързани със сигурността, с цел оценка и третиране (*Aligning Security Services with Business Objectives*, 2013), обосноваване на нови инвестиции (Santos, 1991). Не на последно място, подобрение, което обикновено е свързано с пет елемента: одит на киберсигурността, криптиране на всички данни, обучение на персонала, внедряване на най-добрите практики в киберсигурността, наемане на специалист в киберсигурността.

Основна характеристика на „лошите“ метрики е, че са лесни за събиране, но много трудни за приложение.

Показателите, които се измерват, може да се резюмират *на база на технологиите и оперативните показатели, чрез анкетна карта*.

Добрите метрики трябва да отговарят на следните характеристики:

- Подлежащи на действие – необходими действия, които трябва да се предприе-

Анкетна карта за вътрешен одит по отношение на технологиите и оперативните показатели:	
Информационна система:	
Брой насочени атаки към системата за изминалия месец*:	
Брой успешни атаки към системата за изминалия месец:	
Брой атаки към системата за изминалия месец, които са нанесли щети върху информационните активи (цялостност, наличност, поверителност):	
Брой атаки към системата за изминалия месец, които са нанесли щети върху бизнес активите на организацията (финанси, репутация, законност):	
Брой незакачени уязвимости при атаките:	
Брой незакачени критични уязвимости спрямо критични системи:	
Процент незапазени критични уязвимости спрямо критични системи:	
Брой дни, необходими за закърпване на критични системи с критични кръпки**:	
Брой дни, необходими за закърпване на системи, поддържащи производството, при установяване на уязвимост:	
* Това са атаки, които са насочени конкретно към организацията и/или информационната система. Не се отчитат случайно насочените атаки. ** При нулев ден на уязвимостта.	

мат, са ясни, когато показателят премине предварително зададени стойности;
- Обща интерпретация – Хората в организацията разпознават какво означава показателят;
- Прозрачно и просто изчисление – Как се генерира показателят е споделен и лесен за разбиране;
- Достъпни, достоверни данни – Данните могат да бъдат получени със скромни усилия от източник, на който хората имат доверие.

При избора на метрики трябва да се отговори на следните три въпроса:

1) Приети ли са на сляпо предложените метрики на доставчика?

2) Приложими ли са метриките?

3) Имат ли метриките само едно тълкуване?

Често използвани метрики са метриките за измерване на риска и метрики за качеството на софтуера. Основни метрики за икономическа оценка са: годишна продължителност на загубите, единична продължителност на загубата, общата стойност на собствеността, възвръщаемост от инвестициите в сигурността, нетна настояща стойност и вътрешна норма на възвръщаемост (IRR).

Изборът на метрика служи за обосновка на приложените мерки за защита, както и инвестициите, направени за тях. За целта трябва да се разграничат „добрите“ от „лошите“ метрики, което би позволило подобряване на работата на организацията. Подборът на правилни метрики би подобрил комуникацията с бизнеса, което би довело до по-големи инвестиции в информационни технологии.

При оценката на моделите за киберсигурност бяха оценени „Динамичен бизнес модел на сигурността (Business Model for Information Security (BMIS)) за изграждане на сигурността в умните градове“ и „Модел на сигурността IOActive“. Също така беше засегнат въпросът с модел за връзка между модулите на умния град и защитата на личните данни. И при трите модела подходът е от доставчиците към потребителите.

При динамичен бизнес модел на сигурността критичен фактор, който не се наблюдава в други модели, е тежестта, която се отделя на организационната култура. Също така, ако бъде направена промяна на един от елементите, това може да доведе до дисбаланс при останалите елементи. Това се дължи на парадигмата „сигурност по дизайн“.

Модел на сигурността IOActive предоставя защита от и към доставчиците. За целта се създават специални анкетни карти. Специално се набляга на отношенията с трети страни.

Проблемите на Urban security network (“UrbSecurity – An Action-Plan Network for planning safer cities”, 2020) или проблеми със сигурността, накратко, в контекст на интелигентен град са ситуации, които могат да представляват проблеми към цялата инфраструктура на умния град. Проблемите, свързани с личните данни, са тези, които в много от случаите нанасят големи финансови щети на организациите.

3. Pragmatic security – Прагматичен модел за оценка на киберсигурността

Прагматичният подход предлага методика отдолу нагоре, т.е. от потребителите на услугите на умния град, към доставчиците на услугите и съответно изискванията към киберсигурността. Този подход и метрики могат да бъдат приложени върху всеки един от елементите, включително технико-технологичните показатели. Подходът се базира на пет ключови стъпки:

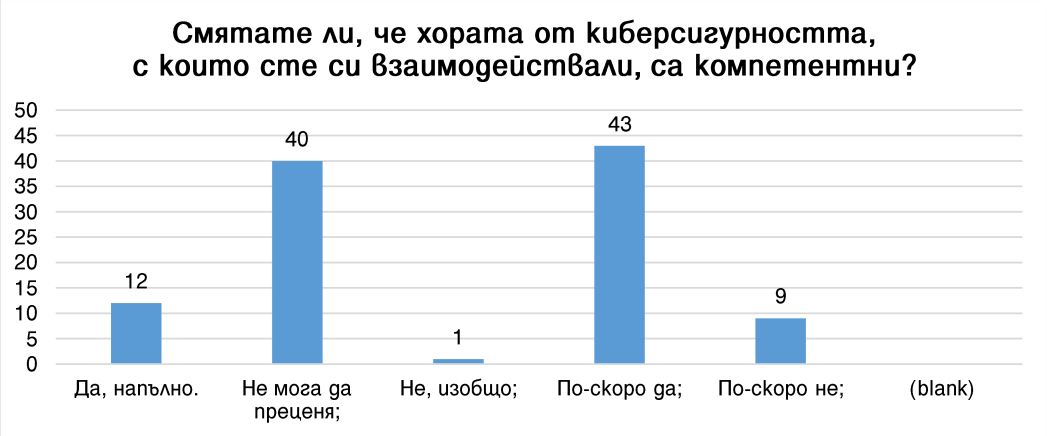
Стъпка 1. Определяне целите за измерване.

Стъпка 2. Спецификация на метриките (**Правилното нещо за измерване, Правилните хора**, **Правилният формат на данните,**

Позиции на разходите	Небрежност на служител или доставчик	Криминална дейност	Самозванец	Средно	Покачване на разходите през последните три години
Мониторинг и наблюдение	$21538	$21857	$22977	$22124	79%
Кибер разследване	$49441	$114524	$147429	$103798	86%
Ескалация на инцидента	$9282	$29513	$26619	$21805	84%
Отговор на инцидента	$62877	$159398	$132677	$118317	56%
Сдържане/ Ограничаване	$75903	$175962	$382794	$211553	53%
Последващи анализи	$21035	$19282	$18121	$19480	78%
Саниране на системата	$67036	$235223	$141069	$147776	47%
Общо	$307111	$755760	$871686	$644852	60%

Фигура 5. *Средни разходи при възстановяване при инцидент при вътрешна заплаха (Ponemon Institute, 2020)*

Смислена времева линия). *Потребителите обикновено са:* **Служителите; Мениджмънтът; Собствениците на информационни активи.** За целта на по-доброто управление на информационните активи от техните собственици в умния град е изработен Наръчник за управление на информационните активи, който е изработен в проекта (фигура 5).



Фигура 6. *Оценка на компетентността от потребителите*

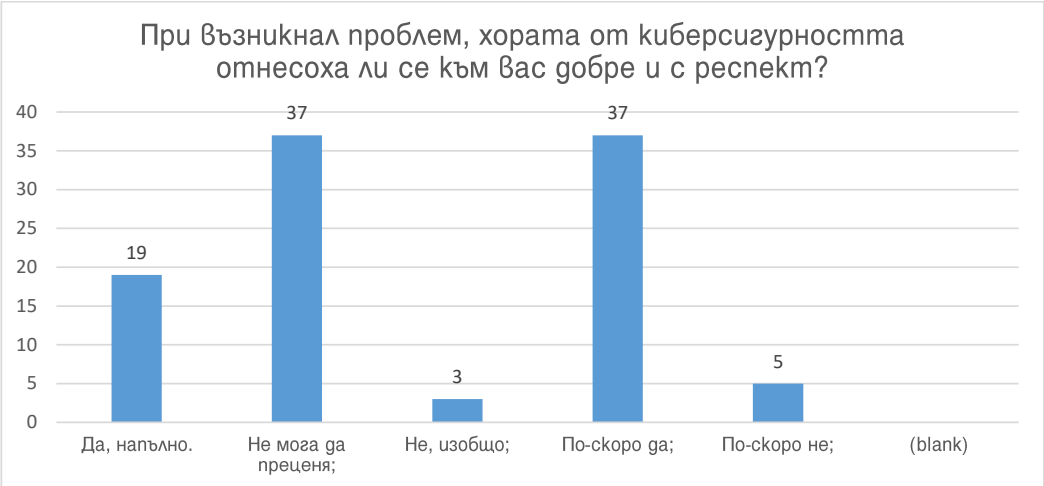
За управлението на информационната сигурност е проблем, ако резултатът от обратната връзка с клиентите е „нисък“. Възприемането, че не се добавя стойност от функционирането на киберсигурността води до отсъствие на търсене на помощ по отношение на сигурността. Установяването на тази зависимост се прави на базата на анкети за обратна връзка. Трябва с голяма прецизност да се подбира кого точно изследваме и по кое време го изследваме. Изследването трябва да се фокусира върху определени клиенти. Най-добрият вариант е, ако те са имали контакт в скоро време с предлагащ услугите на киберсигурността. За да се получи оценка на възприятието може да се подходи със следните въпроси (фигура 6, фигура 7, фигура 8, фигура 9):

При проведената анкета с хора, които са имали взаимодействие със специалисти, които предлагат услугата киберсигурност, само 12 са напълно удовлетворени (от 105 отговорили), а 43 са по-скоро удовлетворени. Това означава, че по-голямата част от анкетираните или не са удовлетворени, или не могат да преценят ролята на киберсигурността. Това може да се дължи и на отношението на предлагащите киберсигурност.

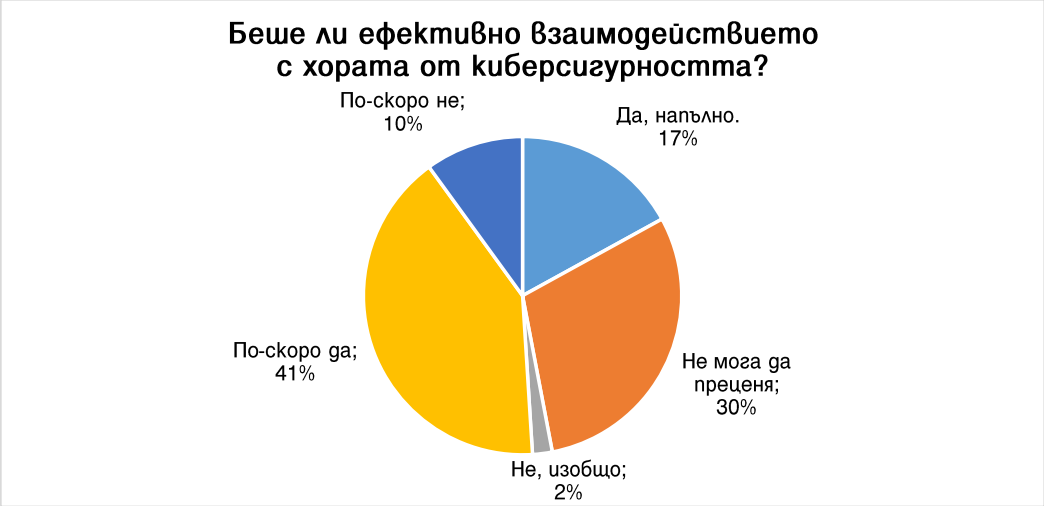
Целта на този въпрос е да се установи отношението на хората от киберсигурността *(независимо от специализацията)* към потребителите на тяхната услуга. При умните градове, логично може да се предположи, че хората, които са почувствали, че не са се отнесли към тях с необходимото уважение, ще се мултиплицират. *Неуважителното отношение към потребителите може да доведе до небрежност и немарливост по отношение на управлението на информационните активи.*

От проучването се вижда, че над 50% от анкетираните са усетили положителен ефект от взаимодействието с киберсигурността. Проблемът е в това, че голяма част от анкетираните не могат да преценят ефективността, т.е. нямат обективни измерители (метрики), чрез които да измерят ефекта и съответно ефективността. *Целта на този въпрос е не толкова да оцени взаимодействието, а да се установи броят на хората, които не разполагат с инструментите да го оценят.*

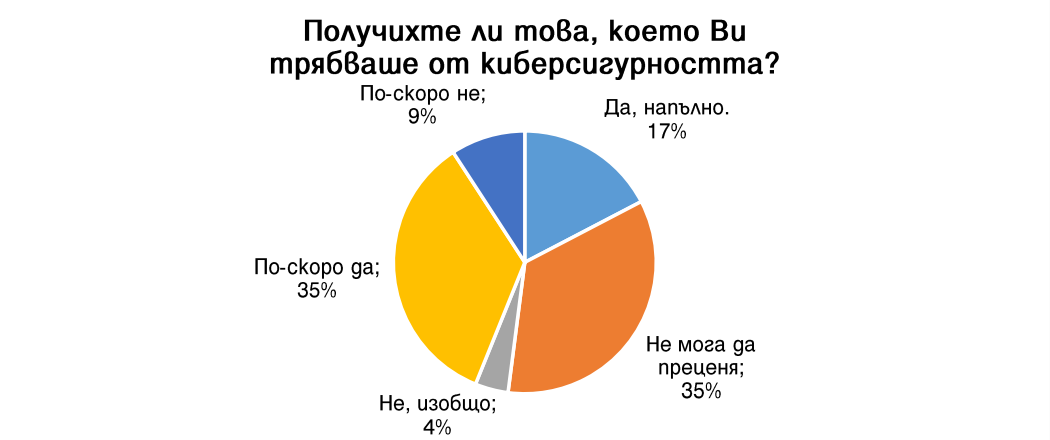
От изключително значение за организацията е да получи това, което търси от



Фигура 7. *Отношение към потребителите*



Фигура 8. *Субективна оценка на потребителите за ефективността*



Фигура 9. *Субективна оценка на потребителите за резултати спрямо очаквания*

сигурността. При проучването под 50% са получили това, което търсят. Причините за това са много и обикновено се състоят в несъответствие на очаквания и получени резултати. При съответствие на бизнес целите и целите на сигурността, такова несъответствие може да се избегне в голяма степен.

Оценяване и ранжиране на метриките, използвайки критерия PRAGMATIC. Резултатът за всяка метрика може да се обобщи като 9 изисквания за нея, които са приемливи за организацията (фигура 10).

Правилно избраната метрика позволява измерването на ефикасността на инвестициите в киберсигурност. *За съжаление, ползите и резултатите от тези инвестиции могат да се изчислят при извеждането на защитаваната технология от употреба, като се съпоставят с проблемите/загубите, възникнали при експлоатацията на подобна технология.*

Финансови метрики за киберсигурност	PRAGMATIC рейтинг в %									
	Прогнозируем	Съответстващ	Приложим	Оригинален	Смислен	Точен	Навременен	Независим	Икономичен	Обща оценка
NPV – 6,17	77	72	25	35	85	55	44	60	88	60%
ROI – 6,18	65	72	25	25	88	50	44	60	90	58%
IRR – 6,19	70	72	25	30	82	50	44	60	88	58%
Срок на възвръщаемост на инвестицията -6,20	69	72	25	30	82	50	44	60	88	58%
VAR – 6,26	70	65	20	30	35	40	30	30	22	38%
ROSI – 6,27	40	40	20	20	55	45	25	40	30	35%

Фигура 10. *Оценка на метриките за икономическа оценка (Brotby and Hinson, 2013)*

4. Изграждане на модел за икономическа оценка на киберсигурността в умните градове на проектен принцип

Проектният подход е задълбочено изследване на проблема, за който се търси решение. За всеки отделен проблем проектният подход, независимо от стандартите и методологията, е уникален поради факторите на времевата рамка, участниците (заинтересовани страни) и финансирането. Проектният подход, с помощта на проектните мениджъри, спомага за спазването на бюджета, целите и времевите срокове на проекта. За да е успешно управлението, то трябва да се фокусира върху факторите, върху които може да влияе, а не върху тези, които са външни за управлението на киберсигурността на умния град и не може да се влияе върху тях.

Подходяща методика за конкретния случай с управлението на проект за оценка на киберсигурност в умните градове е PRINCE 2. Според определението, дадено от методиката, *проект е временна организация, създадена умишлено за доставянето на един или повече продукти в бизнес контекста на организацията* (Office, n.d.).

При такава ситуация възникват два основни въпроса, които обикновено пораждат проблеми и нанасят икономически щети:

- Как да се осъществи контрол върху работата но трети страни?
- Кой носи отговорност при инциденти, т.е. кой ще покрие щетите?

Основната цел на киберсигурността е осигуряване на устойчивост, при хипотеза за неизбежност на инцидентите. За постигане на целта се изграждат способности, като не е необходимо да се спира на определена методология. От по-голямо значение е инструментите и техниките, които се използват, да са съобразени с разполагаемата времева и бюджетни рамки.

Мандатът на проекта е *предпроектна фаза*, която е ключът към стартиране на проекта за изграждане на модел на икономи-

ческа оценка на киберсигурността. Реално това е фаза, която се извършва преди да са направени инвестиции или отделено време за проучване или разработване. На този етап в конкретния случай се поставят въпросите:

- Проект ли е изграждането на модел за оценка на киберсигурността в умните градове?
- Наистина ли организацията има нуждата от този проект?

За периода 2017-2021 г. в света ще се изразходват над 1 трилион долара за киберсигурност ("Global Cybersecurity Spending Predicted To Exceed $1 Trillion From 2017-2021", 2019). Пряко или косвено тези разходи засягат всеки един потребител на информационни технологии. При умните градове обосноваването на тези разходи е сериозен проблем, защото те могат да са публични средства, а контролът по спазване на минималните изисквания на киберсигурността се осъществява с публични средства.

Стъпките в управлението чрез предложената методика се извършват на принципа на *процес*. Този процес може да бъде представен и като *лист за проверка на изпълнени задачи.* В зависимост от обекта, при който се реализира проектът за модел за оценка на киберсигурността, може и да не се изпълняват всички задачи. От значение е *последователността* на изпълнение на задачите, някои от които са паралелни, а други са последователни.

Първият етап е създаване на организация – структура, задаване на роли и отговорности. На този етап се създава т.нар. борд, който определя основен изпълнител, основен потребител и основен доставчик. В *контекста на умния град ролята на борд може да се изпълнява от общинския съвет*.

Основните разходи за икономическа оценка на киберсигурността са за одит или по-точно за персонал. Тези разходи може да са еднократни или да са постоянни за заплащане на работното време. По принцип при одита на информационната или киберсигурността, извършвана от специалисти, се заплаща на час.

На този етап се създават два основни мениджърски продукта, които трябва да се доставят:

- Кратко описание на проекта – основни линии на „бизнес казуса", описание на продукта на проекта, проектния подход, очаквано качество от потребителите, критерии за приемливо изключение.
- План за стартиране на проекта.

Планът за стартиране на проекта е първият управленски етап от проекта. Другите етапи след етапа на стартиране на проекта се наричат етапи на доставка, т.е. във всеки един от следващите етапи трябва да се достави определен „специализиран продукт". В конкретно разглеждания казус това е някой от елементите или целият модел за оценка на икономическите аспекти на киберсигурността.

Вторият етап се състои от процес на борда. Върху основата на „краткото описание на проекта", бордът трябва да вземе решение дали е съгласен с определените критерии, дали да продължи с проекта или не. Каква сума пари е склонен да инвестира в първата стъпка от проекта. За целта се изготвя документация за „стартиране на проект", която включва план на проекта, ресурси, които са необходими, времево ограничение на проекта. Бордът влиза в процес, наречен насочване на проекта.

Иницииране на процеса стартира след *оторизирането на проекта от борда*, стартира **трети процес,** наречен **иницииране на проекта**. На този етап от проекта се извършва детайлно планиране, като ключова роля има мениджърът на проекта. Мениджърът събира цялата документация, която включва планирането, стратегиите и контрола, както и бизнес аспектите на проекта.

Основен елемент е ***планът на проекта***, който включва детайлно описание на продукта и ако се използват артикули, записи на техните конфигурации. За управление на плана трябва да се създадат **контролите на проекта**, които се използват и на ниво на борда. В съчетание с тях и директно от плана на проекта се извежда **бизнес казусът**. Този бизнес казус е детайлен, защото в плана на проекта се съдържат детайли за времето и финансирането. Тук трябва да се извърши анализ на ползите *(„разходи-ползи“)* или рентабилността на проекта, както и нуждите на организацията. Такъв анализ трябва да се извърши за всеки инструмент за киберсигурност.

Базиран на бизнес казуса, се изготвя документ за **подход за управление на ползите**, който се използва след приключването на проекта. Този документ показва как целите на проекта ще се реализират, кога ще се реализират, колко ще струва реализацията им. Ако проектът е динамичен и гъвкав, не всички ползи ще се реализират по време на *жизнения цикъл на проекта*. ***Съществува разлика между резултатите на проекта и пълния потенциал на ползите от проекта***.

Работни пакети започват при одобряване на **следващия етап**, първата задача е одобряването на работните пакети. Работните пакети са свързани с управлението на доставката на продукти. Това е процес, който реално „изнася“ работата по продукта. Тук е отговорността на ръководителя на екип, който управлява работния пакет. Ръководителят на екип трябва да се увери, че продуктите, заявени в работния пакет, могат да се осигурят в условията на зададените ограничения. Екипът включ-

Елемент на бюджета		**Тип на разход**	**Минимален разход в USD**
Общ бюджет за киберсигурност			350 000
Планиран срещу актуален бюджет			
Използван процент от бюджета			
Продукт			
Категория	Име на продукта		
Разширена защита от заплахи	NGAV\EDR\Анализ на мрежовия трафик\UEBA\Подвеждане	Месечен	250
Мрежова защита	Защитна стена\Защита на SD WAN	Месечен	560
Защита на електронната поща	Доставчик на електронна поща\ Решения от трета страна	Годишен	20000

Управление на идентичността	На място\облачно управление на идентичността	Месечен	600
Защита на софтуера като услуга (SaaS)	CASB\WAF		120
Защита на приложенията	WAF\SQL Защита		450
Защита от облачно натоварване	IaaS\PaaS		100
Интеграция	SIEM\Анализ на дневниците		250
Защита на данните	DLP\CASB	Месечен	680
Управление на уязвимостите		Месечен	450
Антивирусни пакети		Месечен	580
Персонал			
Категория	Специфично		
Допълнително заплащане на екипа за киберсигурност (работят в организацията)	Системен администратор	Месечен	5000
	Мениджър по защита на личните данни	Месечен	5800
	Мениджър по сигурността	Месечен	4200
	Аналитик	Месечен	5100
Обучение на екипа по сигурност	Курс за „тестове за проникване“		300
	Конференции/работни групи по сигурността	Няколко пъти годишно	13 500
	Работна група за анализ на зловредния софтуер		6000
Обучение на останалия персонал	Обучение срещу фишинг		2200

Услуги			
Категория	Име на услугата		
Продукти на сигурността вкл. доставка, поддръжка и обслужване	Доставка	Месечно	900
	Поддръжка	Месечно	350
	Обслужване	Месечно	1500
Консултации	Външен консултант	Месечно	700
Отговор на инциденти	Външен екип	Непредвиден разход на годишна база	10000
Одит	Външен одитор	Месечно	140

Фигура 11. *Примерен модел за минимални разходи в бюджет за киберсигурност*

ва и вътрешни специалисти по продукта, които също участват в изготвянето на плана за следващия етап. Цялата информация се записва в регистъра на качеството.

На принципа на докладите за напредване на работни проекти, бордът изготвя разписание за изготвяне на доклади по напредъка на етапа. Обикновено след тези доклади отново следват ад-хок насоки.

В момента, в който специалните продукти са доставени, се преминава към третата фаза от етапа – доставка на работния пакет. Целта е да се информира мениджърът на проекта, че продуктът е завършен. Това може да задейства няколко активности, като например заплащане на екипа, ако е от трета страна, задействане на следващ работен пакет и т.н., до момента, в който всички работни пакети в етапа са приключени.

Последният етап от проекта е **процес на затваряне на проекта**. Това е свързано с предаване на проектите. Изготвя се доклад за приключване на проекта и доклад за научените уроци. Двата доклада са свързани с оценката на проекта.

От ключово значение за размера на бюджета е размерът на обекта, или в разглеждания случай модул на умния град. Други елементи, които засягат бюджета, са брой на устройствата, които ще се защитават, подход и инструменти за защита и от основно значение брой на персонала, който ще отговаря за киберсигурността. Също така може да бъде от значение и броят на доставчиците/третите страни. От ключово значение за организацията е, че ***инвестициите в киберсигурност ускоряват процеса на дигитална трансформация.***

Като основа на модела могат да се приемат три фактора: наименование на разхода, вид на разхода (еднократен, постоянен – на час, на ден, на година) и минимален раз-

ход за единица (хора, устройства, антивирусен пакет и т.н.). Месечните разходи са постоянни, а годишните са еднократни, но това не пречи в договорите да се предлагат разплащания на няколко вноски. В примерния бюджет не се отчитат разходите за сертифициране на персонала *(примери за това има в текста)*. В примерната фигура 11 са включени само най-популярните разходи за киберсигурност, извлечени на основата на добрите практики.

Заключение и изводи

В умните градове може да бъде приложен модел за икономическа оценка на киберсигурността. В проекта е установен подходът при модулите в умни градове. Връзката киберсигурност – икономически ефекти е установена на основа на проектния принцип. Връзката е изградена и оценена върху основата на моделите за киберсигурност и моделите за оценка на киберсигурността. Представените модели са сравнени и са оценени метриките за оценка на ефективността им.

В разработката е направено изследване на моделите на умни градове, като са изведени трите основни модела за създаването им. Те са оценени и са изведени техните специфики и положителни страни. В проекта е представен основният проектен модел за киберсигурност. Той е основан на разширен модел на умен град, обхващащ максимално количество модули. Самият модел се базира на конкретните заплахи за конкретните модули в умния град. Моделът е сравнен с други модели за изграждане на системи за киберсигурност.

В изследването се използва подход от потребител към доставчик, като за целта е проведена анкета, която да насочи или покаже детайлите при създаване и приложение на модел. Предимството на проектния подход се състои в съсредоточаване върху описването на това, което трябва да се направи, вместо върху предписването на това как се прави всичко.

Основният извод е, че инвестициите в киберсигурност ускоряват процеса на дигитализация.

Цитирани източници:

Aligning Security Services with Business Objectives, 2013. Elsevier. https://doi.org/10.1016/C2012-0-07728-9

Braun, T., B.C.M. Fung, F. Iqbal, B. Shah, 2018. Security and privacy challenges in smart cities. Sustain. Cities Soc. 39, 499–507. https://doi.org/10.1016/j.scs.2018.02.039

Brotby, W.K., G. Hinson, 2013. PRAGMATIC Security Metrics: Applying Metametrics to Information Security, 1 edition. ed. Auerbach Publications, Boca Raton, Fla.

Frost & Sullivan, n.d. Smart Cities, A Frost & Sullivan Accelerated Program.

Global Cybersecurity Spending Predicted To Exceed $1 Trillion From 2017-2021, 2019. Cybercrime Mag. URL https://cybersecurityventures.com/cybersecurity-market-report/ (accessed 8.23.20).

Office, T.S. (Ed.), n.d. Managing Successful Projects with PRINCE2.

Ponemon Institute, 2020. 2020 Cost of Insider Threats Global Report. Observe IT, IBM Security.

Santos, B.L.D., 1991. Justifying Investments in New Information Technologies. J. Manag. Inf. Syst. 7, 71–89. https://doi.org/10.1080/07421222.1991.11517904

SMITH, B., n.d. Measuring Security – How Do I Know What a Valid Metric Looks Like?

United Nations, 2016. The World's Cities in

2016, Statistical Papers – United Nations (Ser. A), Population and Vital Statistics Report. UN. https://doi.org/10.18356/8519891f-en

UrbSecurity – An Action-Plan Network for planning safer cities [WWW Document], 2020. URBACT. URL https://urbact.eu/urbsecurity-action-plan-network-planning-safer-cities (accessed 8.4.20).

Vrancken, J., J.H.V. Schuppen, M. dos S. Soares, F. Ottenhof, 2009. A hierarchical network model for road traffic control. 2009 Int. Conf. Netw. Sens. Control. https://doi.org/10.1109/ICNSC.2009.4919298