КИБЕРСИГУРНОСТ И ПРОТИВОДЕЙСТВИЕ НА КИБЕРЗАПЛАХИТЕ НА НИВО „ОБЩИНА“ (ПО ПРИМЕРА НА ОБЩИНА РУСЕ)

Тодор Станков Милков

докторант отчислен с право на защита

Варненски Свободен университет „Черноризец Храбър”

Факултет „Социални, стопански и компютърни науки“

Катедра „Администрация и управление“

РЕЗЮМЕ: *Настоящата статия разглежда така актуалния въпрос в сферата на сигурността на информационните системи, а именно – разбирането за киберсигурност и противодействието на киберзаплахите, разгледани през призмата на конкретна административна структура – Община Русе. Описват се основни показатели – организация и политика на ниво община; рискове и заплахи; възможности и силни страни. Изследват се възможностите за прилагане на съвременни технологични решения в областта на киберсигурността, както и възможностите за моделиране на административните общински процеси. Оценяват се текущите системи за гарантиране на киберсигурността в Община Русе.*

Ключови думи: *информационни технологии, киберсигурност, киберзаплахи, риск, управление, противодействие.*

CYBER SECURITY AND COUNTERMEASURE OF CYBER THREATS AT THE "MUNICIPALITY" LEVEL (ON THE EXAMPLE OF THE MUNICIPALITY OF RUSE)

Todor Stankov Milkov –
PhD student
Varna Free University "Chernorizets Hrabar"
Faculty of "Social, Business and Computer Sciences"
Department of Administration and Management

SUMMARY: *This article examines the current issue in the field of information systems security, namely, the understanding of cyber security and the counteraction of cyber threats, examined through the prism of a specific administrative structure - the Municipality of Ruse. Basic indicators are described - organization and policy at the municipality level; risks and threats; capabilities and strengths. The possibilities of applying modern technological solutions in the field of cyber security, as well as the possibilities of modeling administrative municipal processes, are being explored. The current systems for ensuring cyber security in the Municipality of Ruse are evaluated.*

Keywords: *information technology, cyber security, cyber threats, risk, management, countermeasures.*

ВЪВЕДЕНИЕ

С оглед наличието на рисково общество[1] и рискови социални и икономически сфери не е изненадващ факта за интензивното развитие на киберсигурността и наративното придружаващо понятие киберзаплахи и тяхното противодействие. Рискът предикира и заплахи от всякакво естество. А киберсредата е особено добър проводник за тяхното разрастване. Колкото повече се развиват информационните технологии и процесите по дигитализация, толкова повече нараства опасността от киберзаплахи за сигурността. Не е достатъчна само бдителност по време на работа в Интернет, нужни са и интелигентни решения/системи в областта на киберсигурността.

[1] Димитров, Н., Управление на риска за сигурността в Център за компетентност „КВАЗАР“, – В: Военен журнал, №3-4, 2020, с. 76.

Все повече бизнеси и административни организации се замислят за укрепване на киберсигурността. Сякаш това е неизбежно и неизменно върви синхронно с развитието на цифровизацията. Заплахите и фишинг атаките в Интернет са напълно реални и те не подбират според размера на организацията/компанията или конкретния потребител. Те се отнасят за всички. Затова важна се оказва постреакцията. Това е една нелека борба, чийто резултат не подлежи на предварително планиране.

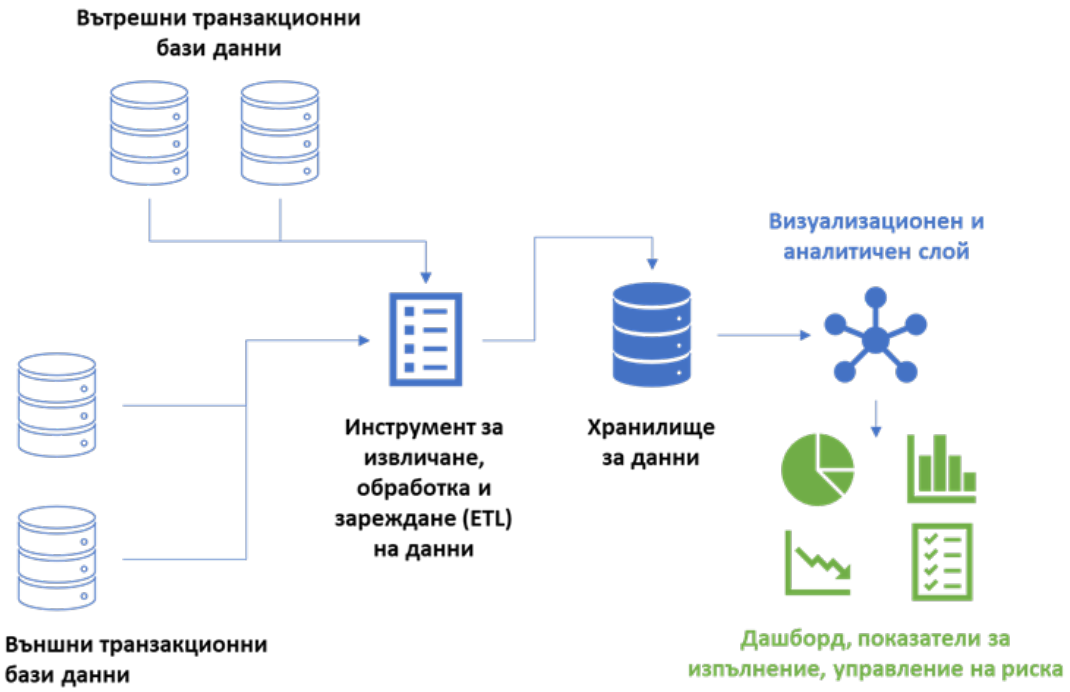
Именно тези факти предпоставят избора и необходимостта от разглеждане на настоящата статия. Анализът акцентира на релацията *киберсигурност – киберзаплахи – противодействие – интелигентни решения на ниво Община*. Целта е да се онагледи взаимното влияние и факторната предпоставеност. Това води до широка информативност и осветляване на проблема.

Основна цел на изследването е да разгледа развитието на киберсигурността и начините за противодействие на киберзаплахите на ниво Община на примера на Община Русе.

Основни задачи:

1. *Да се съберат първични и вторични данни по изследвания проблем.*
2. *Да се проведе теоретично проучване, което да обясни процеса на взаимодействие.*
3. *Да се проведе емпирично проучване на ниво Община за съществуващите и планираните системи за киберсигурност.*
4. *Да се анализира и обобщи резултатът от направеното първично и вторично изследване.*

ИЗЛОЖЕНИЕ



Фиг. 1[2]. Архитектура на държавна администрация.

В поддържането на киберсигурността Община Русе следва повелите на Актуализираната стратегия за национална киберсигурност за 2023 година [3]. В тази връзка определя своите основни цели:

- превентиране и защита на киберсигурността в областта на предлагане на електронни административни услуги;
- подобряване на вътрешноадминистративния капацитет и способностите на служителите – назначаване на специалисти-експерти в областта на информационните технологии [4];

[2] Адаптирана по: Йоцов, Вл., Интелигентни системи за информационна сигурност, ИЗД. „За буквите – О писменехъ“, С., 2010.

[3] Национална стратегия за киберсигурност „Киберустойчива България 2023“: https://www.strategy.bg/PublicConsultations/View.aspx?lang=bg-BG&Id=5878 – проверен на 07.02.2023 г.

[4] Конкурс за назначаване на Главен експерт: https://obshtinaruse.bg/informatsia-za-konkurs-za-naznachavane-na-darzhaven-sluzhitel-na-dlazhnostta-glaven-ekspert-v-otdel-informatsionni-tehnolog - проверен на 07.02.2023 г.

- активно сътрудничество с държавните органи за прилагане на киберсигурността;
- поставяне на активни дългосрочни административно-електронни цели;
- повишаване на техническия капацитет в областта на противодействието на киберзаплахите;
- прецизиране на функционалната пригодност на текущия административен персонал;
- постигане на устойчивост при установени/констатирани кибератаки;
- засилване на научно-приложната дейност за налагане на устойчиви модели в областта на киберсигурността;
- осъвременяване на подхода за оценка на киберсигурността;
- полагане основите за усилена работа за създаване на киберрезерви;
- засилване на мониторинга над ситуацията на местно общинско ниво;
- установяване на механизми за провеждане на местно киберразузнаване;
- създаване на местна среда за споделяне на информация и взаимодействие в областта на киберсигурността, която да обхваща всички заинтересовани страни;
- полагане основите на местно публично-частно партньорство в областта на киберсигурността;
- сигурност, прозрачност и отвореност при предлаганите електронни административни услуги за гражданите.

На местно общинско ниво главен разпоредителен орган, под юрисдикцията на който попада и киберсигурността, това е Дирекцията „Обществен ред и сигурност“. Нейните задачи и правомощия са:

- организира и разработва мерки за действие при наличие на кризи;
- прави анализ на констатираната ситуация;
- защитава класифицираната информация в Общината съгласно действащата нормативна уредба;
- обезпечава технически работата в Общината в областта на информационните технологии;
- проследява новите тенденции и прави адекватни предложения на кмета на Общината за подобряване нивото на киберсигурността;
- участва активно в разработването и управлението на проекти, свързани с киберсигурността;
- контролира инфраструктурните обекти;

- изпълнява допълнителни задачи по информационното обслужване;
- предлага мотивирани решения на кмета на Общината при наличие на конфликт на интереси;
- извършва обществено полезна и координационна функция [5].

По време на пандемията от КОВИД-19 в Община Русе се приема Проект „Оперативна програма за електронно управление и техническа помощ 2021-2027“ [6]. Освен че крайната цел на този проект е да се постигне по-голяма цифровизация в предлагането на административни услуги в Общината, другото важно направление в областта на информационните технологии е да се гарантира мрежовата и информационната сигурност/киберсигурност.

Фиг. 2[7]. Приоритети за подобряване на киберсигурността в Община Русе.

В началото на настоящата 2023 година подадените проектни предложения за подобряване на киберсигурността в Общината са два пъти повече в сравнение с

[5] Дирекция „Обществен ред и сигурност“: https://obshtinaruse.bg/direktsia-obshtestven-red-i-sigurnost - проверен на 07.02.2023 г.

[6] Русе представи проекта на новата програма: https://obshtinaruse.bg/oits-ruse-predstavi-proekta-na-novata-novata-operativna-programa-za-elektronno-upravlenie-i-tehnicheska-pomosht-2021-202717952 - проверен на 07.02.2023 г.

[7] Адаптирана по: https://shortest.link/h27O - проверен на 07.02.2023 г.

отчетната 2022 година. Това показва засилена технологична модернизация и желание за напредък в областта на информационните технологии [8].

През последното десетилетие Община Русе има установени предимно следните киберзаплахи по вид:

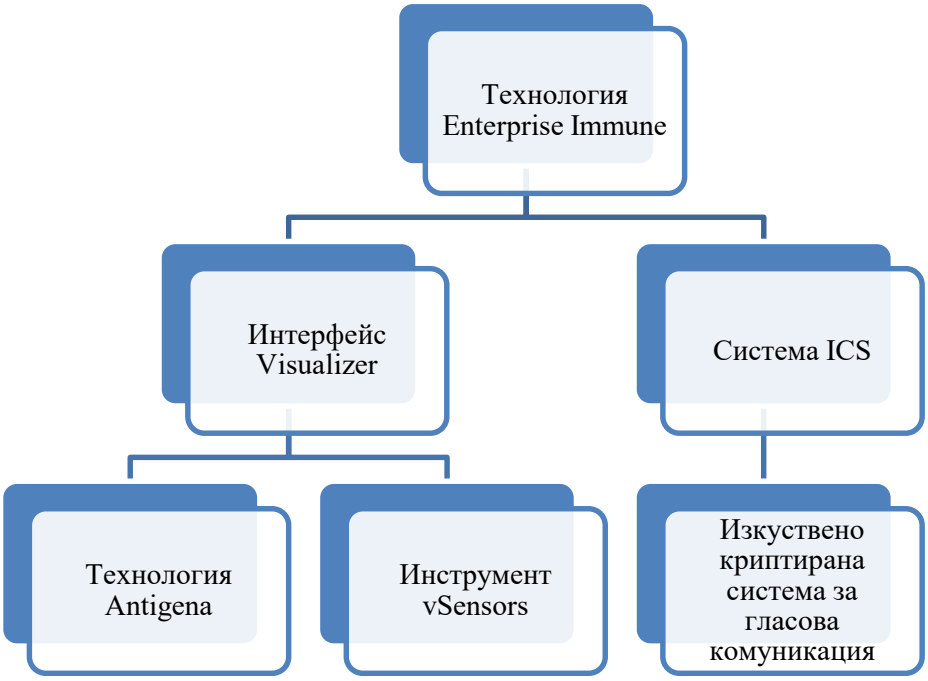
- атакуване на бази данни;
- мрежово базирани атаки;
- атаки чрез социалните мрежи;[9]
- изтичане на класифицирана информация;
- физическо въздействие върху материалната база;
- увреждане на съоръжения;
- непредумишлени престъпни въздействия [10].

Във връзка с пробива в системите – електронни, софтуер, хардуер, социални мрежи – Община Русе предприема активни действия през последните четири-пет години за особено подобряване и усъвършенстване на системата си за киберсигурност. Водена от своите административни цели и приоритети Община Русе все повече се насочва към прилагането на изкуствен интелект и приемането на интелигентни решения, като иновативен прийом за подобряване на киберсредата.

[8] Финансиране за киберсигурност: https://shortest.link/h2k6 - проверен на 07.02.2023 г.

[9] Павлов, М., И. Николова и др., Наръчник – обучение по киберсигурност, „Консорциум и обучения 2015“, С., 2015, с. 22-23.

[10] Димитров, Н., Колев, К., Информационни характеристики в интерес на сигурността на зоната критична инфраструктура, - В: Интегрирана информационна система за поддръжка управлението на бреговата зона, Варна, ВВМУ, „Н. Й. Вапцаров“, 2016, с. 57-60.



Фиг. 3[11]. Машинни технологии за изкуствен интелект.

Прилагането на изкуствен интелект и интелигентни решения в конкретно разглежданата Община е една изключителна иновация за самата нея. Тя ще донесе така чаканата фундаментална промяна на местно административно ниво. Работните екипи ще бъдат обучени и ще се съревновават с други конкурентни на база непрекъснато развиващите се и усъвършенствани киберзаплахи.

Кибератаките са безкомпромисни и изискват безапелационни решения. Поради това Общината проявява смелост и се насочва към наистина модерни решения, които могат да бъдат подкрепени и от държавните структури на по-високо ниво. Интелигентните решения стъпват на основата – самообучение. Съдържателно интелигентните решения се доближават до принципа на функциониране на човешката имунна система – когато тялото се зарази, имунната система открива заплахата и се опитва да я неутрализира, като предоставя сигурност на тялото. Тази способност за самообучение, подобно на човешките имунни клетки, позволява разкриване на редки и невиждани модели в областта на информационната сигурност. Тя различава приятел от враг, както и заплаха от атака. Самообучението позволява функциониране на системите в неопределена/несигурна среда и постепенно добиване на опит и компетенция. То се

[11] Адаптирана по: Йоцов, В., Информационна защита УНИБИТ, С., 2020.

впуска в неизвестна и дори рискова среда на базови знания. Следи се поведението при определени фиксирани стандарти за изпълнение. Те не могат да се променят към собственото поведение. Водещи мотиви са: поведение, реакции, действия. Прилага се вероятностен анализ и предсказване на поведението [12]. Самообучението се явява перспективно за сферата на сигурността в Общината.

Таблица 1[13]. Предимства и недостатъци на интелигентните решения в областта на киберсигурността.

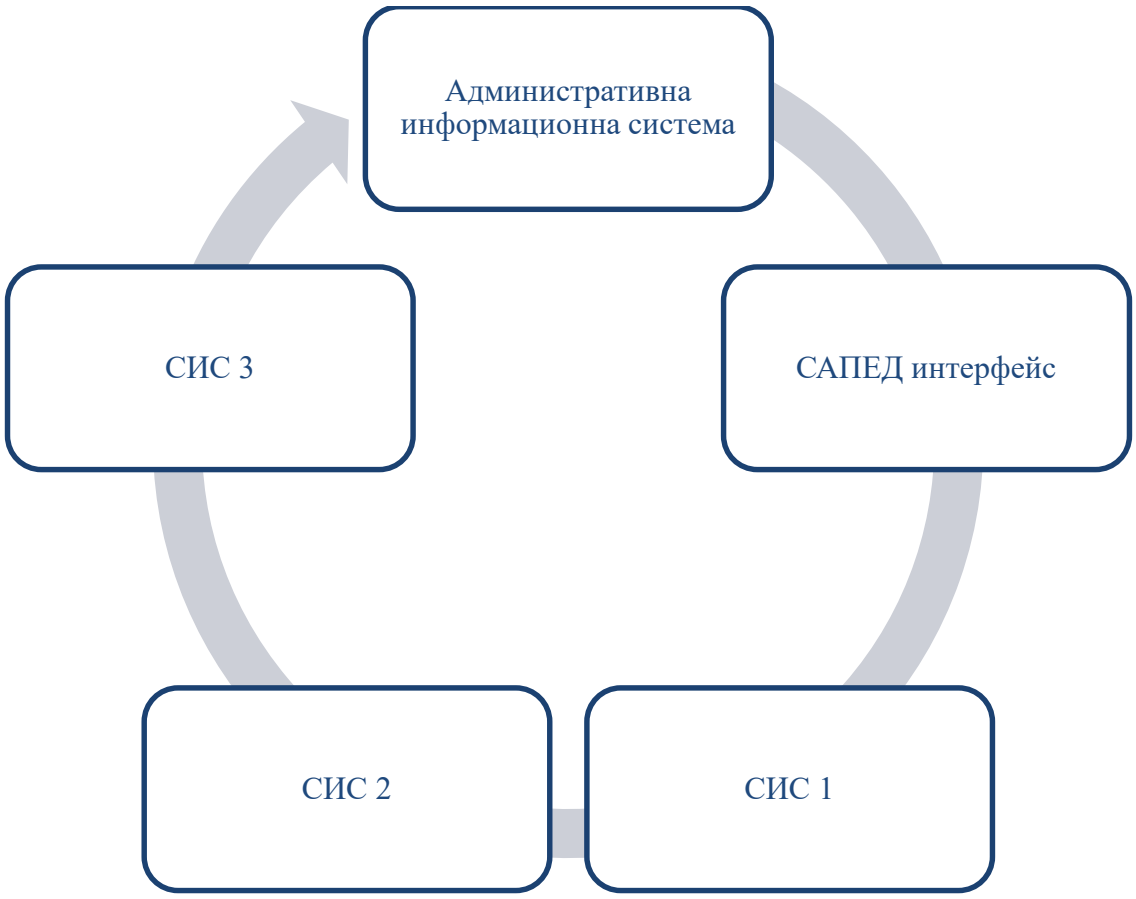
Плюсове	**Минуси**
Обучение – атестиране	Невъзможност за прогнозиране на резултатите
Идентификация, обработка и адекватна реакция срещу атаки	Нерегулярност на резултатите
Атестиране при вземане на решения	Потенциални рискове
Информационна сигурност	Много проекти – разливане на основната цел
Класически системи за сигурност	Вероятностни анализи
Постигане на ефективни крайни резултати	Недостиг на време
Решаване на сложни задачи	Използване на уязвими места
Ограничаване на човешки грешки	Минутни кибератаки
Еднаква защита на голям брой устройства	146 дни за организационна реакция
Защита от вътрешни заплахи	
Революция на новите технологии	

Благодарение именно на тези интелигентни решения, Общината може да си позволи да остави технологиите да се справят с по-трудните задачи, като по този начин отнема част от натовареността на административния персонал, която би могла да доведе до допускане на грешки. Но без значение колко добри са системите, тези на хакерите също еволюират мигновено бързо. Поради това управителните органи на общината

[12] Йоцов, В., Информационна защита, УНИБИТ, С., 2020.

[13] Съставена от автора.

следва да отчитат, че не съществува абсолютно надеждна защита от кибератаки. Но използването на интелигентни решения определено ще е в помощ за бърза и адекватна реакция, ако възникнат рискове и заплахи. Използването на изкуствен интелект е един много добър ход, тъй като и злонамерените хакери извършват изпреварващи действия, което затруднява установяването и отстраняването на кибератаките.



Фиг. 4[14]. Общински портал за единни административни услуги.

[14] Адаптирана по: Денчев, Ст., Информация и сигурност, ИЗД. „За буквите - О писменехъ“, С., 2019, с. 180.

Фиг. 5[15]. Укрепване доверието у общинската администрация в областта на киберсигурността.

ЗАКЛЮЧЕНИЕ И ПРЕПОРЪКИ

Въз основа на така получените резултати от проведеното проучване можем да заключим, че киберсигурността безспорно е сред задачите, стоящи на дневен за решаване в разглежданата Община, като взаимодействието в релацията *киберсигурност – киберзаплахи – противодействие – интелигентни решения на ниво Община* е двупосочна. Това твърдение не може да се отсъди нито като напълно вярно, нито като напълно грешно. Върху него сугестират редица външни фактори. Но като цяло Община Русе си остава сред най-модернистичните административни центрове и сред първите такива, които разработват и въвеждат нови проекти в областта на киберсигурността и затова вътрешната политика е в посока развитие сферата на електронните услуги. Повече

[15] Адаптирана по: Димитров, Н., Укрепване на доверието за използване на киберпространството, - В: Военен журнал, №2, 2014, с. 47-48.

от половината от икономиката на Общината се основава именно на административните услуги, защото те добавят стойност. А ако повечето преминат в електронни[16], то тогава добавената стойност ще се увеличи, но и ще има необходимост от увеличаване на киберзащитата.

Киберсигурността и киберзащитата са от първостепенно значение днес. Основни предимства на интелигентните решения са:

- обучението е непрекъснато и поради това адаптацията улеснена;
- осигуряват пълна видимост в критичната инфраструктура;
- благодарение на тях се откриват бързо атаки, преди да нанесат съществена вреда;
- инсталират се много бързо, без да изискват конфигурация.

Смятам, че всички промени, случили се до този момент в Общината и онези, които предстои да се случат, говорят за сигурна и продължаваща трансформация в тази насока и за в бъдеще. Ще продължават да се променят начинът ни на живот, естеството на работата ни, начинът, по който се извършват редица административни електронни услуги.

Изводите, които можем да направим в резултат на емпиричния анализ, са:

- синтезираната, интерпретирана и обобщена информация, показана за разглеждания проблем, е ефективна;
- разгледаната Община е добър нагледен пример за оптимизиране дейността в областта на киберсигурността и противодействието на киберзаплахите и за други общини в страната;
- Общината е на едно добро ниво на ефективност по отношение на киберсигурността, но има още много работа по отношение противодействието на киберзаплахите;
- киберзащитата е задължителна за Община Русе, защото тя ще продължава да дигитализира своите административни услуги.

Препоръки:

- Общината следва да използва целия си наличен потенциал за развитие на своята киберсигурност;

[16] Михалева, Св., Павлов, П., Концепцията „Електронно правителство – същност, проблеми и перспективи, УИ на ВСУ „Черноризец Храбър“, Варна, 2003.

- Общината следва да търси съдействието на държавните органи в подкрепа противодействието на киберзаплахите на местно ниво;
- Общината следва да използва своите налични инвестиционни възможности в подкрепа на кибепроектите;
- Общината следва да въведе електронна диверсификация на всички функционални административни услуги;
- Общината следва да въведе ефективна оценъчна система за измерване на риска и киберзаплахите;
- Общината следва да внедрява иновативните и модернистични административни технологични и технически нововъведения.

Въз основа на анализа се откроява значимостта на изследвания проблем. Практико-теоретичната актуалност и перспективност на изследвания проблем продължава своята интензивна въздейственост. Без съмнение неговото разширяване ще доведе до значителен по обем и съдържателен емпиричен масив от данни по темата. Формулираната цел на изследването се постигна, като доказателство за това е изследователският продукт на параметри и графични изображения на реални данни за интелигентните и информационните системи на Общината. Целта беше постигната поетапно, чрез решаване на формулираните изследователски задачи.

ИЗТОЧНИЦИ:

1. Боянов, Л., Съвременното дигитално общество, ИК ЛИК, С., 2014.
2. Денчев, Ст., Информация и сигурност, ИЗД. „За буквите - О писменехъ“, С., 2019.
3. Димитров, Н., Укрепване на доверието за използване на киберпространството, - В: Военен журнал, №2, 2014.
4. Димитров, Н., Колев, К., Информационни характеристики в интерес на сигурността на зоната критична инфраструктура, - В: Интегрирана информационна система за поддръжка управлението на бреговата зона, Варна, ВВМУ, „Н. Й. Вапцаров“, 2016.
5. Димитров, Н., Найденов, В., National security in Bulgaria – is it really a system? Theoretical foundations of security national and international security information security technical facilities for ensuring security., Scientific technical union of mechanical engineering industry, Vol. 3, Iss. 1 (5), 2019.
6. Димитров, Н., Управление на риска за сигурността в Център за компетентност „КВАЗАР“, – В: Военен журнал, №3-4, 2020.
7. Димитров, Н., Формулиране на оптимизационни задачи по управление на риска в ЦК „КВАЗАР“ чрез симулации, - В: Известия на Съюза на учените, Варна, 2020.
8. Йоцов, В., Информационна защита, УНИБИТ, С., 2020.
9. Йоцов, Вл., Интелигентни системи за информационна сигурност, ИЗД. „За буквите – О писменехъ“, С., 2010.
10. Михалева, Св., Павлов, П., Концепцията „Електронно правителство – същност, проблеми и перспективи, УИ на ВСУ „Черноризец Храбър“, Варна, 2003.
11. Павлов, М., И. Николова и др., Наръчник – обучение по киберсигурност, „Консорциум и обучения 2015“, С., 2015.
12. Русков, П., Информационни системи в бизнеса, Ч.1, С., 2010.
13. Семерджиев, Цв., Н. Митев, Информационна сигурност, ИЗД. „Софттрейд“, С., 2015.
14. Дирекция „Обществен ред и сигурност“: https://obshtinaruse.bg/direktsia-obshtestven-red-i-sigurnost - проверен на 07.02.2023 г.

15. Русе представи проекта на новата програма: https://obshtinaruse.bg/oits-ruse-predstavi-proekta-na-novata-novata-operativna-programa-za-elektronno-upravlenie-i-tehnicheska-pomosht-2021-202717952 - проверен на 07.02.2023 г.
16. https://shortest.link/h27O - проверен на 07.02.2023 г.
17. Национална стратегия за киберсигурност „Киберустойчива България 2023“: https://www.strategy.bg/PublicConsultations/View.aspx?lang=bg-BG&Id=5878 – проверен на 07.02.2023 г.
18. Конкурс за назначаване на Главен експерт: https://obshtinaruse.bg/informatsia-za-konkurs-za-naznachavane-na-darzhaven-sluzhitel-na-dlazhnostta-glaven-ekspert-v-otdel-informatsionni-tehnolog - проверен на 07.02.2023 г.
19. Финансиране за киберсигурност: https://shortest.link/h2k6 - проверен на 07.02.2023 г.