ISSN 1314-3379

НЯКОИ АСПЕКТИ НА КИБЕРСИГУРНОСТТА НА КРИТИЧНАТА ИНФРАСТРУКТУРА В КРАЙБРЕЖНАТА ЗОНА

Желязко Николов

MARITIME CRITICAL INFRASTRUCTURE CYBERSECURITY ASPECTS OVERVIEW

Zhelyazko Nikolov

Abstract: *The security of maritime critical infrastructure is of growing importance in the recent years. However, some trends in this area show that there are aspects of the security which are getting more significant. For example, Industrial Control Systems are becoming more exposed to cyber treats and in this paper some possibilities to increase their resistance are overviewed.*
Keywords: *critical infrastructure, cybersecurity.*

1. Въведение

Терминът „инфраструктура“ е въведен през XIX в. от швейцарския военен теоретик Антоан-Анри Жомини. Днес тази дума е с обогатено значение и се прилага широко в компютърните науки, икономическата география и в изследванията на сигурността. От друга страна, думата „критичност“ се дефинира в тълковните речници като „обозначаване на състояние, при което процес или система променят внезапно своите свойства“. Ако се свърже с инфраструктурата, понятието „критична инфраструктура“ се определя като тази част от инфраструктурата, която е изключително важна за функционирането на обществото.

Съвременната глобална инфраструктура може да се разглежда като непрекъснато усъвършенстваща се високотехнологична система, в която са съсредоточени значителна част от съвременните иновации. Паралелно с това се наблюдава и нейната роля в две неразривно свързани, но ясно разграничаващи се направления. От една страна глобалната инфраструктура благоприятства свободно движение на капитали, материални ценности, хора и информация, като по този начин стимулира развитието на световната икономика, а от друга, създава условия за развитието на миграционни вълни, организирана престъпност и прояви на тероризъм, включително киберпрестъпления [1, 2].

Зависимостта на управлението на инфраструктура в световен мащаб от високите технологии, и по-специално компютърните, създава условия за нарастване на уязвимостта на жизненоважни елементи. Ценните активи, които се контролират от тези системи представляват вероятна цел на технологични атаки и те могат да бъдат организирани в компютърните мрежи за управление на обекти на критичната инфраструктура с последствия от типа на нарушаване на управлението на системи за контрол на индустриални обекти, транспорт, доставки на горива, електроснабдяването и други [1, 2].

В настоящата разработка са представени някои аспекти на киберсигурността на критичната инфраструктура в крайбрежната зона.

2. Някои аспекти на киберсигурността на критична инфраструктура в крайбрежната зона

Сред обектите на бреговата критична инфраструктура на Република България могат да бъдат отбелязани:

- ТЕЦ “Варна” и ТЕЦ “Девня”;
- промишлена зона Девня;
- нефтохимически комбинат Бургас;
- пристанища – Балчик, Варна и Бургас;
- контейнерни терминали на пристанища Варна и Бургас;
- горивни терминали на пристанища Варна и Бургас;
- нефтен терминал “Бургас - Нефтохим”;
- летища – Балчик, Варна и Бургас;
- гранични полицейски пристанища Варна и Бургас;
- митници – Варна и Бургас;
- пътно-комуникационни съоръжения: крайморска фронтална магистрала “Север-Юг”,
- “Аспарухов мост”, проход “Дюлино”;
- водохранилища - язовири “Камчия” и “Цонево”, помпени станции, каптажи, главни и
- разпределителни водопроводи [3, 4].

От своя страна морската критична инфраструктура включва:

- товарни кораби, танкери, газовози и химикаловози на котва в пристанищата Варна и Бургас и в Териториалното море на Националните морски пространства;
- нефтени и газови терминали, тръбопроводи и морски платформи в Териториалното море на Националните морски пространства [3, 4].

В голяма част от изброените обекти, както и в глобален план, се прилагат софтуерно управляеми системи за контрол, и този факт е предпоставка за създаване на уязвимости. В тази връзка като съществена опасност по отношение на обектите на критичната инфраструктура през последните години се очертава кибертероризма. Множество примери днес свидетелстват за негативни икономически ефекти при въздействие върху разглежданите цели. Това променя характера на заплахите за инфраструктурата за бъдещ период и налага необходимостта от стратегия за ефективно реагиране. Решенията на проблема за повишаване на сигурността на инфраструктурата се усложняват и от факта, че значителна част от секторите на националното стопанство се оперира от частни организации, което предполага изработване и приемане на комплекс от мерки от юридически и организационен характер, регулиращи взаимоотношенията на държавните органи с частните компании [1, 2].

Зависимостта на основни функции на индустриални обекти, особено от групата на критичната инфраструктура, от популярните компютъризирани системи за дистанционен контрол, често ги превръща в цел на злонамерени атаки. Така изискванията към тези системи по отношение на киберсигурността постепенно се завишават и това се изразява и в необходимостта от непрекъснато усъвършенстване на използваните операционни системи и приложения. За съжаление и в тази сфера, усилията за подобряване на системите за дистанционен контрол действат като катализатор за развитието на кибертероризма. Освен това, не са рядкост и случаите при които, оценката на риска за сигурността на обекти на критичната инфраструктура е извършен неадекватно и това води до пропуски в защитата. Понякога този факт поставя сериозни предизвикателства пред екипите, отговорни за противодействието на кибер престъпленията. В близкото минало компютъризираните системи за дистанционен контрол в индустрията са били използвани изолирано от общодостъпни мрежи. Но потребностите на бизнеса от мрежови услуги като например наблюдение в реално време, дистанционна поддръжка и диагностика доведоха до интегрирането на

тези системи в Интернет на нещата и в Глобалната компютърна мрежа. И това в конкретния случай доведе до възможност за компрометиране на киберсигурността на обекти от критичната инфраструктура [5, 6, 7, 8, 9, 11, 12, 13].

Според [10] през последните години зачестяват киберпрестъпленията срещу обекти на критичната инфраструктура, особено в крайбрежната зона. Пример в това отношение е кибератаката срещу обект на петролна компания за добив на химикали в Саудитска Арабия през 2017 година, когато след използване на зловреден софтуер беше повлияно ефективно на системата за дистанционно управление, която регулира захранващото напрежение, налягането и температурата в процеса на производство на опасното вещество. Анализатори твърдят, че щастлива случайност е попречила на планираната експлозия и освен това, компрометирането на защитата на обекта „отваря“ врата за нови атаки срещу цели, които използват същия софтуер за дистанционно управление. Вече се наблюдават и примери за атаки с отложен във времето ефект, което още повече затруднява адекватното противодействие [14].

3. Изводи

Системите за дистанционен контрол на обекти от критичната инфраструктура придобиват все по-голяма популярност. Паралелно с тяхното значение нараства както броя на опитите, така и на успешните кибератаки срещу тях. Сред честите причини за тях са слабости в операционните системи и възможностите за неоторизиран достъп в компютърните мрежи за управление на критичната инфраструктура. В глобален план се засилват мерките за повишаване на киберсигурността, които се изразяват в разработването на адекватни на рисковете приложения, ограничаване на достъпа до мрежите и обектите, както и подготовка и привличане на квалифицирани специалисти.

Литература

1. Димитров, Н. Сигурност на морската критична инфраструктура. ВВМУ „Н. Й. Вапцаров”, Варна, 2010, ISBN 978-954-8991-65-0.

2. Димитров, Н. Системен подход към критичната инфраструктура. ВВМУ „Н. Й. Вапцаров”, Варна, 2019, ISBN 978-619-7428-41-4.

3. Медникаров, Б., К. Калинов, Н. Димитров. Аспекти на защитата на критичната морска инфраструктура. Шеста международна конференция ”Сигурността в Югоизточна Европа, публично-частното партньорство и критичната инфраструктура” 11-12 септември 2008, Академия на МВР, София, 2008.

4. Попов, Н. Класификация на критичната инфраструктура в крайбрежната зона на Р България. Известия на Съюза на учените – Варна, серия „Морски науки”, с. 22-27, Варна, Съюз на учените – Варна, 2011. ISSN 1314-3379.

5. Сивков, Й. Трансформиране на корабната мрежа от сензорно-базиран към информационно-базиран модел. ВВМУ „Н. Й. Вапцаров”, Варна, 2019, ISBN 978-619-7428-38-4.

6. Сивков, Й., К. Костадинов, М. Цветков. Система за предаване и приемане на данни от платформи със сензори. Интегрирана информационна система за поддръжка управлението на бреговата зона с. 89 – 96, Варна, ВВМУ „Н. Й. Вапцаров“, 2016. ISBN 978-954-8991-89-6.

7. Методика за оценка на риска за установените критични инфраструктури и обектите им в сектор „Отбрана“ в Република България. Министерство на отбраната на Република България, Военно-географска служба, Троян, 2017.

8. Grancharova V. New technologies used for automation of container handling at terminals. Journal of Marine Technology and Environment, p. 41-48, Constanta, Constanta Maritime University, Year VII, Vol. I/2014, ISSN 1844–6116,;

9. Grancharova V. The challenge of building greenfield terminals. Journal of Marine Technology and Environment, p. 33-36, Constanta, Constanta Maritime University, Year VII, Vol. II/2014. ISSN 1844–6116.

10. https://iecetech.org/index.php/Technology-Focus/2019-02/Cyber-attacks-targeting-critical-infrastructure - 15.11.2019.

11. https://www.gao.gov/assets/680/672973.pdf - 15.11.2019.

12. https://www.hsaj.org/articles/179 - 15.11.2019.

13. https://www.researchgate.net/publication/322909940_Cyber_Security_of_Critical_Infrastruc tures – 15.11.2019.

14. https://www.securitymagazine.com/articles/88818-saudi-arabia-investigating-critical-infrastructure-cyberattack - 15.11.2019.

За контакти:

доц. д-р Желязко Кирилов Николов
ВВМУ „Н. Й. Вапцаров”
e-mail: zhelyazko_nikolov@abv.bg