Модел на обучение в областта на киберсигурността (Ядрена сигурност)

Недко Тагарев*

Резюме: Проблемът, разглеждан в настоящата публикация, е нарастващата необходимост от адекватно и приложимо към съвременните условия обучение в областта на киберсигурността. Акцентът е поставен върху актуалните тенденции в ядрената сигурност и възходящия тренд на използване на ядрени технологии. Посочени са конкретни примери за кибератаки над ядрени обекти. Накратко е представена и магистърската програма „Икономика на отбраната и сигурността“ със специализация „Ядрена сигурност“. Важно е да се отбележи, че към момента цитираната програма е единствена в света. В публикацията намират място и конкретни примери за областите, в които могат да се развиват магистрите, преминали успешно обучителната програма.

Ключови думи: ядрена сигурност, киберсигурност, информационни технологии.

JEL: M150, D610; O21.

Въведение

Проблем на тази публикация е подходът при обучението в сферата на киберсигурността. Тук е мястото да се спомене, че различните програми в тази област изключително приоритизират технологичните или техническите аспекти на киберсигурността като криптография, програмен код и компютърни конфигурации. Този масово прилаган в практиката подход в обучението игнорира всички участници, които не са експерти в областта на информационните технологии или математиката. В следствие на това неглижиране, много често не се обръща внимание на управленските процеси или реалните процеси на експлоатация на информационните технологии. Съгласно с правилото, че сигурността е отговорност на всеки служител на организацията, обучението в областта на киберсигурността следва да е предназначено за всеки, който „експлоатира“ информационните мощности на организацията в административен или производствен аспект. Този пропуск в обучителните програми може дори да бъде причина за нанесени щети в огромни размери.

Тук е мястото да се отбележи, че през последните години има засилен интерес към приложението на ***ядрените технологии***. Редица държави проявяват интерес към разширяване или въвеждане на ***ядрена енергия*** на своята територия в резултат на собствената си оценка и нужди от енергийни доставки. Счита се, че това се дължи на изменението на климата и изискванията за икономическо развитие. Увелича-

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

ването на търсенето на ядрена енергия ще увеличи също и броя на ядрените реактори в световен мащаб. В съответствие с тази тенденция ще се увеличи и количеството използван ядрен материал. Тези промени се отразяват в засилено ползване на ядрени технологии с невоенно приложение. В резултат на това увеличение, необходимостта от експерти в областта на ядрената сигурност придобива огромно значение, защото ***възможните злоумишлени действия***, включващи ядрен или друг радиоактивен материал, са реална заплаха. Възможността да се използва ядрен или друг радиоактивен материал за злоумишлени цели не могат да бъдат изключени в сегашната глобална ситуация. За периода 2013-2016 г. са докладвани 514 инцидента, свързани с радиоактивни материали ('CNS Global Incidents and Trafficking Database | Analysis | NTI', accessed 17 December 2017, http://www.nti.org/analysis/reports/cns-global-incidents-and-trafficking-database/). За този период 188 от инцидентите са извън контрола на ядрените регулатори ('CNS Global Incidents and Trafficking Database | Analysis | NTI'). Държавите-членки на МААЕ отговарят на този риск, като се ангажират с колективен ангажимент за укрепване на защитата и контрола на този материал и да реагират ефективно на събития, свързани със сигурността в ядрената енергетика.

Всяка държава носи пълната отговорност за ядрената сигурност. В детайли трябва да гарантират сигурността на ядрените и други радиоактивни материали, свързаните с тях съоръжения и дейности; да се гарантира сигурността на такъв материал при употреба, съхранение или транспорт; за борба с незаконния трафик и случайното движение на такива материали, да бъдат подготвени да реагират на събитие за ядрена сигурност.

Един от основните проблеми, свързани с ядрената сигурност е ***киберсигурността***. В практиката са познати петнадесет случая, свързани с атаки срещу обекти от областта на ядрените технологии, като осем от тях са свързани с енергетиката. Въпреки това, всеки инцидент, свързан с ядрени материали, може да бъде свързан по смисъл с информационната сигурност. Един от модулите за обучение по „Ядрена сигурност" се занимава с ***киберсигурността в ядрените съоръжения***. Модулът се основава на националния опит и практики, както и публикации в областта на киберсигурността и ядрената сигурност.

1. Магистърска програма „Икономика на отбраната и сигурността" със специализация „Ядрена сигурност"

Катедра „Национална и регионална сигурност", към *„Университета за национално и световно стопанство"* предлага актуална магистърска програма *„Икономика на отбраната и сигурността"* със специализация ***„Ядрена сигурност"***. *Катедрата* е приет член на Международната мрежа за обучение по ядрена сигурност INSEN, в която членуват над 45 държави с повече от 120 организации.

Магистърската програма е резултат от споразумение между Международната агенция за атомна енергия (МААЕ) и Университета за национално и световно стопанство (УНСС), София. Програмата успешно се развива през последните четири години. През 2018 г. се приема третият випуск.

Програмата е структурирана в съответствие с изискванията на държавата за магистърска степен и Международна агенция за атомна енергия, Серия за ядрена сигурност № 12 („Nuclear Security", Nuclear Security, отворен на 28 октомври 2017, http://www.unwe.bg/nuclear-security/en.http://www.unwe.bg/nuclear-security/en). Тя е разработена и подкрепена от Международната мрежа за обучение по ядрена безопасност

(INSEN) и няколко български и международни институции.

Чрез програмата си за ***ядрена сигурност*** МААЕ подкрепя държавите за:

- създаване и поддържане на ефективен режим на ядрена сигурност. МААЕ е приела всеобхватен подход към ядрената сигурност.
- прилагането на съответните международни правни инструменти; *защита на информацията; физическа защита; материално счетоводство и контрол; откриване и отговор на трафик на ядрени материали; национални планове за действие; и извънредни мерки*.

Целта на магистърската програма *„Икономика на отбраната и сигурността“* със специализация ***„Ядрена сигурност“*** е да подготви висококвалифициран управленски персонал на средно управленско равнище за нуждите на ядрената индустрия.

Програмата е със следните характеристики:

- преподаване на английски език;
- продължителност 2 години – 4 семестъра, редовно обучение;
- 22 дисциплини – 12 задължителни и 10 избираеми.

Задължителните дисциплини обхващат въпроси и осигуряват необходимите знания в области като ядрени технологии, правна рамка на използването им, превенция и защита от криминални и злонамерени действия, разследване и анализ, радиационна защита и др. Избираемите дисциплини целят допълнителното профилиране на бъдещите мениджъри по сигурността в конкретни области (Георги Пенчев, „Икономика на отбраната и сигурността | 4 семестъра специализация „Ядрена сигурност“, E-DNRS (blog), 15 април 2015, http://www.e-dnrs.org/?magister=%d0%b8%d0%ba%d0%be%d0%bd%d0%be%d0%bc%d0%b8%d0%ba%d0%b0-%d0%bd%d0%b0-%d0%be%d1%82%d0%b1%d1%80%d0%b0%d0%bd%d0%b0%d1%82%d0%b0-%d0%b8-%d1%81%d0%b8%d0%b3%d1%83%d1%80%d0%bd%d0%be%d1%81%d1%82%d1%82%d0%b0-2).

Завършилите студенти намират своята професионална реализация в следните области:

- мениджъри и експерти по сигурността в ядрени обекти – ядрени централи, заводи, свързани с цикъла на ядреното гориво – мини, обогатителни станции, депа за ядрени материали, транспортни фирми с разрешение за работа с ядрени материали или лечебни заведения, използващи ядрени материали;
- специалисти по ядрена сигурност в държавната администрация, регулираща ядрената енергетика;
- разследващи и правоприлагащи органи – МВР, ДАНС, митническа администрация;
- фирми в областта на частната охранителна дейност;
- международни организации;
- научноизследователски организации в сектора на ядрената енергетика.

2. Методика на обучение в областта на киберсигурността (Киберсигурност и Ядрена сигурност)

Този курс на обучение осигурява въвеждането на информационните технологии (ИТ) и киберсигурността като цяло и със специален акцент върху ядрените съоръжения. Обучаваните научават терминологията, процесите и подходите за киберсигурност, основната архитектура на сигурността по отношение на ядрените съоръжения и разбират различията в мерките за сигурност, общите ѝ средства и основните специфични аспекти на сигурността по отношение на контрола на информационната среда и контрола върху ядрените съоръжения.

Лекционният материал е предназначен за хора, които нямат или имат малко опит в областта на информационните технологии. Трябва да се отбележи, че той е

насочен към управлението на киберсигурността, а не към техническото изготвяне на защитни механизми. В процеса на обучение се прави проблемен анализ на казуси, свързани с киберсигурността. За решение на тези казуси се прилагат различни методики за осигуряване на киберсигурността.

Лекционният материал е съставен от седем модула, които обхващат всеки от аспектите на киберсигурността. През 2018/2019 г. ще се направят промени в лекционния материал, като ще се отбележат бележките и препоръките на преподавателския екип.

2.1. Въвеждащ модул

Основната цел на обучението в областта на ***киберсигурността*** *е да се осъзнае важността за включване на компютърната сигурност като основна част от плана за цялостната сигурност за ядрени съоръжения.*

Киберсигурността играе все по-важна роля за постигането на тези цели. Използваната методика за обучение разглежда установяването и подобряването на програмите за защита на компютърните системи, мрежи и други цифрови системи, които са от решаващо значение за безопасната и сигурността на работа, както и за предотвратяване на кражби, саботажи и други злоумишлени действия (International Atomic Energy Agency, Computer Security at Nuclear Facilities: Technical Guidance, Reference Manual (Vienna: IAEA, 2011)).

В този контекст, злоумишлените действия с компютърни системи, свързани с ядрената сигурност, могат да бъдат групирани като:

– Атаки за събиране на информация, насочени към по-нататъшно планиране и изпълнение на злоумишлени действия;
– Атаки, целящи да деактивират или компрометират атрибутите на един или няколко компютри, важни за сигурността или безопасността на съоръженията;
– Компрометиране на един или няколко компютъра, комбинирани с други паралелни начини на атака, като например физическо навлизане в целевите местоположения (International Atomic Energy Agency).

Компютърната сигурност, както е дефинирана при обучението, е подклас на сигурността на информацията (според определението в ISO/IEC27000), с които тя споделя много от цели, методология и терминология („ISO_IEC_27001.pdf“, отворен на 28 октомври 2017, http://bcc.portal.gov.bd/sites/default/files/files/bcc.portal.gov.bd/page/adeaf3e5_cc55_4222_8767_f26bcaec3f70/ISO_IEC_27001.pdf).

2.2. Модул „Компютърна сигурност и контрол на достъпа“

Политиката за компютърна сигурност определя целите на компютърна сигурност на дадена организация. Политиката трябва да отговаря на съответните регулаторни изисквания. Изискванията на политиката за компютърна сигурност трябва да бъдат включени в документи от по-ниско ниво, които се използват за прилагане и контрол на политиката. Освен това, политиката трябва да бъде: *приложена; постижима; подлежаща на одит* (International Atomic Energy Agency, Computer Security at Nuclear Facilities).

Компютърните системи и мрежите в ядрените съоръжения, поддържащи операциите, включват много нестандартни компютърни системи, изисквания за архитектура, конфигурация или изпълнение. Тези системи могат да включват специализирани промишлени системи за контрол, системи за контрол на достъпа, алармени и проследяващи системи и информационни системи, отнасящи се до безопасността и сигурността и реагирането при извънредни ситуации. Те се отнасят за две категории: *Домейни, в които се използват информационни активи* (Бизнес процеси;

Информационни технологии; Инструменти и контрол) и *Информационни активи в бизнес процесите* (Хората, които имат съответните знания; Документи, необходими в работните процеси; Обмен на информация с бизнес партньори, регулатори, оператори на преносни системи;) („NS22.1 Comp Sec and Access Control.pptx“, без дата).

Контрол на достъпа се отнася до практиката за ограничаване на влизането в сграда и помещение или информационен масив на неупълномощени лица. Контролът на физическия достъп може да бъде постигнат чрез механични или технологични средства като системи за контрол на достъпа. В тези среди физическото управление на ключовете може да се използва и като средство за по-нататъшно управление и мониторинг на достъпа до ключови активи.

Електронният контрол на достъпа използва компютри за решаване на ограниченията на механичните ключалки и ключове. За подмяна на механични ключове може да се използва широк спектър от идентификационни данни. Електронната система за контрол на достъпа осигурява достъп на основа на представените данни. Когато бъде предоставен достъп, информацията е отключена за предварително определено време и транзакцията се записва.

Пример за такъв проблем, при който не са спазени правилата за достъп и идентификация е атаката към Изследователски център за водородни изотопи в Университета на Тояма (2015 г.) („University of Toyama's Hydrogen Isotope Research Center Hacked“, Best Security Search (blog), 18 октомври 2016, https://bestsecuritysearch.com/university-toyamas-hydrogen-isotope-research-center-hacked/), при която нападателят е успял да открадне досиета на два пъти, като и двете атаки засягат данни и личните данни на учени в областта на ядрените технологии. Атаката е извършена чрез фишинг, системата е заразена с малуер. Според служители на университета, атакуващите изпращат имейли с фиктивни копия на няколко изследователи, работещи в ядрената лаборатория.

Следователите проследяват първия злонамерен имейл до 24 ноември 2015 г. Компютърът на изследователя е бил компрометиран в края на ноември със сигнал за злонамерен софтуер, който събира данни от неговата работна станция и го е изпратил на онлайн сървър. Първият опит за изпращане на данни от мрежата на университета се осъществява през декември 2015 г. По време на атака са създадени над 1000 архивни файла, които са изпратени чрез кодиран канал на онлайн сървъра на нападателя. Тъй като файловете и трансферите са кодирани, следователите не знаят какво са откраднали нападателите по време на тази първоначална атака. След това нападателите събират друга серия от файлове, които също са компресирани в по-малки архиви и са претърпели ексфилтриране през март 2016 г. За този трансфер изследователите казват, че са успели да установят, че нападателите са събрали данни, свързани с изследване „Как да се премахне замърсената вода, изхвърлена от ядрена централа Fukushima No. 1?“. Когато нападателите крадат трета партида от файлове, през юни външна организация забеляза подозрителните прехвърляния на данни и уведоми изследователската лаборатория.

2.3. Модул „Криптография и удостоверяване“

Криптографията или криптологията е практиката и изследването на техниките за сигурна комуникация при присъствието на трети лица, наречени противници („NS22.2 Cryptography Authentication.pptx“, без дата). По-общо, криптографията е свързана с изграждането и анализирането на протоколи, които възпрепятстват трети страни или обществеността да четат частни съобщения. Това са важни аспекти

на информационната сигурност като: конфиденциалност на данните, целостта на данните, удостоверяване и неотказване в модерната криптография. Съвременната криптография съществува в пресечната точка на дисциплините по математика, компютърни науки, електротехника и комуникационна наука. Приложенията на криптографията включват електронна търговия, чип-карти, цифрови валути, компютърни пароли и военни комуникации (J. van Leeuwen, ред, Handbook of theoretical computer science (Amsterdam; New York: Cambridge, Mass: Elsevier; MIT Press, 1990)) (Mihir Bellare и Phillip Rogaway, "Introduction to modern cryptography", Ucsd Cse 207 (2005): 207) (A. J. Menezes, Paul C. Van Oorschot, и Scott A. Vanstone, Handbook of applied cryptography, CRC Press series on discrete mathematics and its applications (Boca Raton: CRC Press, 1997)).

2.4. Модул „Архитектура на компютърната сигурност"

Всички дисциплини на сигурността (включително персонална, физическа, информационна и компютърна) взаимодействат и взаимно се допълват, за да се установи положението за сигурност на съоръжението. Съответно се провеждат лабораторни упражнения в тези направления. Сигурността на обекта е основно отговорност на ръководството, по-специално на висшето ръководство, за да се гарантира, че законовите и регулаторните изисквания са напълно изпълнени чрез изпълнението на плана за сигурност.

Провалът в който и да е от елементите на сигурността може да повлияе върху другите области, има каскаден ефект и води до допълнителни изисквания към останалите аспекти на сигурността. Компютърната сигурност е елемент, който взаимодейства с всички други области на сигурност в ядрено съоръжение („NS22.3 Comp Sec Architecture.pptx", без дата). Планът за сигурност на обекта би трябвало да бъде разработен, като се има предвид компютърната сигурност. В този случай отговорността на ръководството също е да осигури правилна координация на различните области на сигурността и интеграцията на компютърната сигурност.

Заплахите и уязвимостите са дефинирани предварително в „База данни на основните заплахи" (DBT). Тя е подчинена на следните принципи:

- ***Вътрешни/външни противници.***

  Един потенциален противник е всеки индивид или група от хора, включително както външни противници, така и вътрешни лица, за които се смята, че имат намерение/способности да извършат злонамерено действие.

- ***Връзка между злоумишлени действия и неприемливи последствия.***

  Някои злоумишлени действия, като например неоторизиран достъп до компютърни системи и манипулиране с тях, могат да доведат до неприемливи последствия и следователно трябва да бъдат предотвратени.

- ***Атрибути и характеристики.***

  Съответните атрибути и характеристики на потенциалните противници описват тяхната мотивация, намерение и способност да извършат злонамерен акт.

  Мотивацията може да бъде икономическа, политическа или идеологическа.

  Намеренията могат да включват неразрешен достъп до поверителна информация или саботаж чрез промяна и/или предотвратяване на използването на съществена информация.

  Възможностите на противниците се определят от техния състав, включително техния брой, групиране, евентуално включване на вътрешни лица и тайни споразумения и тяхната организация; както и способностите и активите им, включително тактики, инструменти, ниво на достъп и умения на противника.

- ***Проектиране и оценка.***

База данни на заплахите (DBT) е инструмент, който се използва, за да се установят изисквания за производителност при проектирането и оценката на системите за физическа защита. Възможностите на противниците в тази област помагат на операторите и властите да определят съответните критерии и защита („NS22.3 Comp Sec Architecture.pptx“).

Защитните механизми, които се изучават в модула, се базират на следните принципи:

- Ограничения на действията на удостоверени потребители;
- Най-малка привилегия;
- Принцип на четирите очи;
- Класификация на активи;
- Подход на надграждане;
- Защита в дълбочина;

Пример за атака, която показва слабости в архитектурата на защитните механизми е атаката над Атомната електроцентрала в Монджу (2014 г.) („Malware based attack hit Japanese Monju Nuclear Power Plant“, Security Affairs, 10 януари 2014, http://securityaffairs.co/wordpress/21109/malware/malware-based-attack-hit-japanese-monju-nuclear-power-plant.html), при която ИТ администраторът в атомната електроцентрала в Монджу открива, че атака, основана на зловреден софтуер, заразява система в контролната зала на реактора.

Вторият от осемте компютъра в контролната зала в атомната електроцентрала в Монджу е компрометиран. ИТ администратор е открил, че системата в контролната зала на реактора е била достъпна над 30 пъти през последните пет дни, след като служител е актуализирал безплатно приложение на една от машините в обекта. Смята се, че компютърът е бил заразен с вируса, когато програма за възпроизвеждане на видеоклипове се опитва да извърши редовна актуализация на софтуера. Първата информация, налична за инцидента, потвърждава, че повече от 42 000 съобщения за електронна поща и обучение на персонала са на разположение в компрометираната система в атомната електроцентрала.

Специалистите по сигурността, които разследват инцидента, заключават, че това е атака, основана на злонамерен софтуер, възможно вектор на инфекцията може да бъде софтуерна актуализация на компрометираната машина, злонамереният код е откраднал някои данни, изпращайки го на сървър Command & Control, в Южна Корея, според мрежата, регистрирала извънредния трафик.

2.5. Модул „Мрежова сигурност“

Оборудване за работа в мрежа

В тази част на модулното преподаване се разглеждат различните устройства в мрежата, тяхното устройство и ролята им, като защитни механизми. Съответно се провеждат и лабораторни упражнения, свързани с разглеждания материал. Някои от разглежданите устройства са: Медийни конвертори; Мостове, маршрутизатори, хъбове; Шлюзове („NS22.4 Network Sec.pptx“, без дата); Защитна стена; Диоди за данни; Системи за мрежово криптиране. *На този етап от обучението се прилагат практически примери, чрез специализиран софтуер за наблюдение и контрол на трафика. На базата на тези упражнения се преминава към заплахите и мерките за защита на мрежата.*

Основни заплахи при мрежовата сигурност („ISO_IEC_27001.pdf“), които се изучават и се упражнява противодействие срещу тях по време на упражнения са – *Проби; Надушване; „Човек в средата“; Отказ от услуги („наводняване“); Злонамерен софтуер; Червеи; Троянски коне*. Съответно на заплахите се разглеждат и защитните механизми.

Като пример за успешна мрежова атака може да се покаже атаката срещу Търгов-

ска мрежа на Korea Hydro и Nuclear Power Co. (2014 г.) („Korea Hydro and Nuclear Power Co. Hacked“, отворен на 29 октомври 2017, http://www.powermag.com/korea-hydro-and-nuclear-power-co-hacked/). През декември 2014 г. хакери инфилтрират и откраднат данни от търговската мрежа на Korea Hydro и Nuclear Power Co., която управлява 23 ядрени реактора в Южна Корея. Хакерите получават достъп чрез изпращане на фишинг имейли до служителите на собственика-оператор, някои от които щракват върху връзките и изтеглят злонамерения софтуер. Хакерите са получили чертежите и ръководствата на два реактора, най-вероятно принадлежащи към атомните електроцентрали „Гори“ и „Волсонг“, както и графики за потока на електроенергия, лични данни, принадлежащи на около 10 000 служители на компанията, и оценки на излагането на радиация на жителите в околността. Данните са изтеглени от Twitter от профил, за който се твърди, че принадлежи на ръководителя на анти-ядрена група в Хавай; хакерите също предупреждават „Корея Хидро и ядрена енергетика“ да затворят три реактора или ще се „разрушат“. Собственикът-оператор пренебрегна ултиматума, който се оказа напразна заплаха.

Допълнителни чертежи и данни от тестовете са изтеглени през Twitter през март 2015 г., като хакерите настоявали за пари, за да не се освободят повече данни и да се убеди, че други страни са проявили интерес към закупуването на данните. Вместо да реагира, Южна Корея излиза със съобщение, официално обвиняващо Северна Корея за атаката, като посочи като доказателство, че IP адресите, използвани при фишинг атаките, са свързани с режима; Северна Корея категорично отрече обвиненията.

Инцидентът илюстрира нарастването на изнудването в ядрената индустрия. Интервюираните за проекта съобщават, че такива инциденти, са относително чести.

2.6. Модул „Откриване на проникване и възстановяване на информация“

По време на обучението в този модул се разглежда Системата за установяване на пробиви (СУП). По време на практическите занятия се изпробват широка гама от механизми, вариращи от антивирусен софтуер до йерархични системи, които следят трафика на цялата мрежа. Системата е от голямо значение при управлението и вземането на решения при изграждането на архитектурата на информационната система. Най-често срещаните класификации са Системите за откриване на проникване в мрежата (СОПМ) и Системите за откриване на проникване на базата на хост (СОПБХ). Система, която следи важни файлове на операционната система, е пример за СОПМ, докато система, която анализира входящия мрежов трафик е пример за СОПБХ. Също така е възможно да се класифицира СУП чрез откриване, като най-известните варианти са детектирането на базата на подпис (откриването на лоши модели като злонамерен софтуер) и откриването на аномалии се основава на машинно обучение. Някои СУП имат способността да реагират на открити прониквания. Системите с възможности за реагиране обикновено се наричат система за предотвратяване на проникване.

Във втората част от този модул се разглеждат принципите на *„Възстановяване при бедствия“*. От икономическа гледна точка това е най-интересният елемент от гледна точка на икономическия анализ. Разходния модел се определя от избрания подход.

2.7. Модул „Практика за управление на мрежата“

В този раздел се изучават и упражняват добрите практики от стандартите ISO 27002:2005 по отношение на „мениджмънт

на промяната". Тези практически упражнения могат да се обобщят в следните групи:

- Идентифициране и записване на значителни промени;
- Планиране и тестване на промените;
- Оценка на потенциалните въздействия, включително въздействието върху сигурността, на такива промени;
- Официална процедура за одобрение на предложените промени;
- Съобщаване на подробности за промените на всички съответни лица;
- Процедури за възстановяване, включително процедури и отговорности за прекратяване и възстановяване от неуспешни промени и непредвидени събития („ISO-IEC_27002-.pdf", без дата).

Установяване на уязвимостите на мрежата е процес на прилагане на всички получени знания в процеса на обучение по киберсигурност. Целите могат да се определят като:

- Идентифициране или проверка на оформлението на мрежата;
- Подпомагане идентифицирането на потенциални уязвими места, идващи от конфигурацията и настройките на оборудването;
- Разбирането на начина, по който атакуващият използва тези техники, за да заснеме информация и да открие допълнителни уязвимости за експлойта („NS22.6 NetworkMgnt.pptx", без дата).

Заключение

В публикацията е засегнат проблемът с необходимостта от комплексно обучение в областта на киберсигурността. Накратко е представена магистърска програма *„Икономика на отбраната и сигурността"* със специализация ***„Ядрена сигурност"***.

Показана е методиката за обучение в областта на киберсигурността. Посочени са модулите и основните елементи на компютърната и мрежовата сигурност, и възстановяването след аварии. За илюстрация са приложени казуси от реални атаки срещу обекти от ядрената индустрия.

Цитирани източници:

Пенчев, Георги, Икономика на отбраната и сигурността | 4 семестъра специализация „Ядрена сигурност". E-DNRS (blog), 15 април 2015. http://www.e-dnrs.org/?magister=%d0%b8%d0%ba%d0%be%d0%bd%d0%be%d0%bc%d0%b8%d0%ba%d0%b0-%d0%bd%d0%b0-%d0%be%d1%82%d0%b1%d1%80%d0%b0%d0%bd%d0%b0%d1%82%d0%b0-%d0%b8-%d1%81%d0%b8%d0%b3%d1%83%d1%80%d0%bd%d0%be%d1%81%d1%82%d1%82%d0%b0-2.

(Penchev, Georgi, 2015. Ikonomika na otbranata i sigurnostta | 4 semestara spetsializatsia „Yadrena sigurnost" E-DNRS (blog), 15 April 2015. http://www.e-dnrs.org/?magister=%d0%b8%d0%ba%d0%be%d0%bd%d0%be%d0%bc%d0%b8%d0%ba%d0%b0-%d0%bd%d0%b0-%d0%be%d1%82%d0%b1%d1%80%d0%b0%d0%bd%d0%b0%d1%82%d0%b0-%d0%b8-%d1%81%d0%b8%d0%b3%d1%83%d1%80%d0%bd%d0%be%d1%81%d1%82%d1%82%d0%b0-2)

Bellare, Mihir, и Phillip Rogaway, 2005. Introduction to modern cryptography. *Ucsd Cse* 207 (2005): 207.

'CNS Global Incidents and Trafficking Database | Analysis | NTI', accessed 17 December 2017,

International Atomic Energy Agency. 2011. *Computer Security at Nuclear Facilities: Technical Guidance, Reference Manual.* Vienna: IAEA.

„ISO_IEC_27001.pdf". Отворен на 28 Октомври 2017. http://bcc.portal.gov.bd/sites/default/files/files/bcc.portal.gov.bd/page/adeaf3e5_cc55_4222_8767_f26bcaec3f70/ISO_IEC_27001.pdf.

„ISO-IEC_27002-.pdf“, без дата.

„Korea Hydro and Nuclear Power Co. Hacked“. Отворен на 29 октомври 2017. http://www.powermag.com/korea-hydro-and-nuclear-power-co-hacked/.

Leeuwen, J. van, 1990. peg. *Handbook of theoretical computer science*. Amsterdam; New York: Cambridge, Mass: Elsevier; MIT Press.

„Malware based attack hit Japanese Monju Nuclear Power Plant“. Security Affairs, 10 януари 2014. http://securityaffairs.co/wordpress/21109/malware/malware-based-attack-hit-japanese-monju-nuclear-power-plant.html.

Menezes, A. J., Paul C. Van Oorschot, u Scott A. Vanstone, 1997. *Handbook of applied cryptography.* CRC Press series on discrete mathematics and its applications. Boca Raton: CRC Press.

„NS22.1 Comp Sec and Access Control.pptx“, без дата.

„NS22.1 Comp Sec and Access Control.pptx“, без дата.

„NS22.2 Cryptography Authentication.pptx“, без дата.

„NS22.3 Comp Sec Architecture.pptx“, без дата.

„NS22.4 Network Sec.pptx“, без дата.

„NS22.6 NetworkMgnt.pptx“, без дата.

„Nuclear Security“. Nuclear Security. Отворен на 28 октомври 2017. http://www.unwe.bg/nuclear-security/en.

„University of Toyama's Hydrogen Isotope Research Center Hacked“. 2016. *Best Security Search* (blog), 18 октомври 2016. https://bestsecuritysearch.com/university-toyamas-hydrogen-isotope-research-center-hacked/.