Механика Транспорт Комуникации

ISSN 1312-3823 (print)
ISSN 2367-6620 (online)
том 15, брой 3, 2017 г.

Научно списание http://www.mtc-aj.com **статия № 1471**

АКТУАЛНИ ВЪПРОСИ И ИНОВАЦИИ, СВЪРЗАНИ С ОБУЧЕНИЕТО НА СТУДЕНТИ В СФЕРАТА НА МРЕЖОВАТА И ИНФОРМАЦИОННА СИГУРНОСТ

Димитър Димитров[1], Мария Христова[1], Венцислав Трифонов[2]
ddimitrov@vtu.bg, mhristova@vtu.bg, vencislav.trifonov@gmail.com

[1]ВТУ „Тодор Каблешков", ул. „Гео Милев" ,158, София
[2]Технически Университет, бул. „Климент Охридски" 8, София
БЪЛГАРИЯ

Ключови думи: *мрежови и информационни системи, мрежова и информационна сигурност, интернет, компютърни системи и мрежи, обучение.*

Резюме: *Мрежовата и информационна сигурност имат съществено значение както за обществения, така и за частния сектор на икономиката и за защитата на критичните управленски информационни инфраструктури. В последните години мрежовите и информационните системи на организациите са потенциално засегнати от все по-чести, по-мащабни и по-сложни инциденти по отношение на сигурността. С цел да допринесе за осигуряването на високо ниво и култура на мрежова и информационна сигурност в Европейския Съюз, Европейската Общност създаде Европейска агенция за мрежова и информационна сигурност.*

В настоящата публикация са разгледани актуални въпроси, свързани с мрежовата и информационна сигурност, поставени в Директивата на Европейския парламент относно мерки за гарантиране на високо общо ниво на мрежова и информационна сигурност в Европейския Съюз. Налага се изводът, че най-слабото място в областта на киберсигурността засега остава човешкият фактор, поради което все повече нараства значимостта на подготвеността на кадрите в тази сфера. Обусловена е изключителната актуалност и необходимост от разкриване на магистърска програма „Мрежова и информационна сигурност"(МИС), за да се отговори на изискванията на Националната стратегия и националния план за сътрудничество за МИС. Акцентира се върху иновативни визии, идеи и практики в програмата, които гарантират нейната стратегическа актуалност и в бъдеще.

ПОСТАНОВКА НА ПРОБЛЕМА

Мрежовите и информационните системи и услуги имат изключително важна роля в съвременното общество. Тяхната надеждност и сигурност са от основно значение за стопанските дейности и обществото благополучие. Съвременните информационни системи се характеризират с висока степен на дигитализация, логически зависимости, развитие на изкуствения интелект и цели подпомагане на потребителите с адекватни решения, чрез които да подобрят качеството на извършваната от тях работа. Това от своя страна води до нов подход, основаващ се на

интуитивното мислене и действие при работа с тези системи. В общия случай основната цел на дизайнерите и разработчиците на информационните системи е да заложат такива механизми, които да предотвратяват опасностите и своевременно да информират потребителите за потенциалните проблеми.

Информацията и знанията се превръщат в основни продукти и определят характера на развитието на цивилизацията. Като резултат от тази фундаментална обвързаност с информационните инфраструктури и ресурси, информацията се превръща в обект на множество *заплахи и посегателства,* което налага да се изведе на преден план проблемът с информационната сигурност. Мащабите на нарочно предизвиканите или случайно настъпили инциденти в сигурността и честотата, с която те се появяват, се увеличават и представляват сериозна заплаха пред функционирането на мрежите и информационните системи [1].

Още през 2001 г. в Съобщението си *„Мрежова и информационна сигурност (МИС): предложение за създаване на европейска политика“* Европейската Комисия (ЕК) очертава засилващото се значение на МИС. Това съобщение е последвано през 2006 г. от приемането на Стратегия за сигурно информационно общество [2], поставяща си за цел да създаде култура на МИС в Европа. Европейската общност създава Европейската агенция за мрежова и информационна сигурност (*ENISA*) [3] като експертен център в областта на кибернетичната сигурност в Европа. Агенцията помага на ЕС и страните членки да бъдат по-добре подготвени за предотвратяване, откриване и реакция на проблеми в сферата на информационната сигурност.

През 2009 г. ЕК приема Съобщение относно защитата на критичната информационна инфраструктура, посветено основно на защитата на Европа от кибернетични смущения чрез подобрена сигурност. Със съобщението се обявява план за действие, който да подпомага усилията на държавите членки да гарантират превенция и отговор. В съобщение „Постижения и предстоящи стъпки за постигане на сигурност в световното кибернетично пространство“ от 2011 г. (CIIP) [4] ЕК прави преглед на постигнатите резултати от приемането на плана за действие за CIIP през 2009 г. и стига до заключението, че изпълнението на плана показва, че само национални подходи за справяне с предизвикателствата пред сигурността и устойчивостта не са достатъчни и че Европа следва да продължи да полага усилия да изгради последователен и кооперативен подход на територията на целия ЕС. Обявени са редица действия, като ЕК призовава държавите членки да изградят капацитет за МИС и трансгранично сътрудничество.

На 6 юли 2016 г. е приета *Директива (ЕС) 2016/1148* на Европейския Парламент и на Съвета относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в ЕС [5]. Целта на предлаганата директива е да гарантира високо общо ниво на МИС. Това означава повишаване на сигурността на интернет и на частните мрежи и информационни системи, които са в основата на функционирането на нашите общества и икономики. За постигането на тази цел от държавите членки ще се изисква да повишат своята готовност и да подобрят сътрудничеството помежду си, а от операторите на критична инфраструктура, като енергетика и транспорт, от ключовите доставчици на услуги на информационното общество (платформи за електронна търговия, социални мрежи и др.), а също така от публичните администрации — да предприемат подходящи стъпки за управление на рисковете пред сигурността и да докладват на националните органи за сериозните инциденти. ENISA следва да оказва подкрепа на държавите членки и на Комисията, като предоставя на разположение своите експертни познания и консултации и улеснява обмена на най-добри практики.

Непрекъснато се увеличават сигналите за нарушения в интернет. Повече от 230 са обработените през февруари 2017 г от Националния Център за действие при

инциденти в информационната сигурност към Държавна агенция „Електронно управление“ (CERT-България)[6]. сигнали за нарушения в интернет пространството, като над 5100 са засегнатите IP адреси. От общия брой на подадените сигнали 157 са определени като инциденти, съгласно определението на ENISA. CERT България констатират, че продължава ръстът на атаките от типа „отказ от услуга“ (DDoS), които са 64 на сто от инцидентите или с 20 на сто по-голям дял на атаките от този тип спрямо предходния месец. Следват ги атаките със зловреден софтуер (14%) и тези, свързани с фишинг сайтове (12%).

За един месец в света са извършват над 100 милиарда опита за кибератаки към индивиди, частни и държавни организации. По данни на Gartner 46% от компаниите сериозно повишават инвестициите си в киберсигурност. МИС са в топ приоритетите в съвременните компании и организации. До края на 2017 г. повече от 20% от предприятията ще имат цифрови услуги, свързани със сигурността, предназначени за защита на техните бизнес инициативи, както и интелигентни (smart) устройства и услуги, използващи концепцията „*Интернет на нещата“* (Internet of Things**,** IoT). „Интернет на нещата“ вече е навсякъде около нас - включва всички устройства, които ползваме и които имат постоянна връзка с интернет мрежата. Това води до значителни предизвикателства пред киберсигурността и поражда особена необходимост от създаване на широкоспектърни интернет специалисти-консултанти, които трябва да се грижат, както за сигурността на данните, така и за цялостния процес по използване на IT системите и устройствата.

Според експерти от CERT-България най-слабото звено в системата на МИС е човешкият фактор, който волно или неволно е причина за редица инциденти. Защитата на трансфера на информация и съхраняването на данните изискват създаването на специални способности за активно противодействие на всякакъв вид атаки. Трябва да се говори и мисли за понятието „култура на сигурност“.

МАГИСТЪРСКА ПРОГРАМА „МРЕЖОВА И ИНФОРМАЦИОННА СИГУРНОСТ“ (МИС)

Независимо от големите предизвикателства за осигуряване на информационната сигурност, този въпрос традиционно се решава чрез физическа и логическа сегментация на интернет мрежата (корпоративна, домашна, публична и др.) и инсталиране на необходимия инструментариум за анализ и защита на мрежовия сегмент и най-вече чрез качествено подготвени IT специалисти, отговарящи за сигурността и безопасността на информационните системи и тяхното ползване. Напоследък се оформи и свободна ниша за необходимостта от компютърни специалисти със „специално предназначение“, имащи за цел да обследват и защитават информационните сегменти, както и да консултират потребителите за безопасна работа с информационните системи. Това са т.нар. консултанти по информационна сигурност, работещи в съответните корпоративни и други мрежови сегменти.

За да отговори на необходимостта от специалисти в областта ма мрежовата и информационна сигурност, ВТУ „Т. Каблешков“ разкри магистърска програма „Мрежова и информационна сигурност“. Програмата е разработена в съответствие с Националната квалификационна рамка на Р България, съгласувана с Европейската квалификационна рамка като стандарт на Европейското образователно пространство и тя отговаря на европейските стандарти за обучение, като обхваща съвременните направления в сигурността и защитата на информацията. Специалността осигурява знания и умения за откриване, разпознаване, оценка и анализ на всяка атака и инцидент в киберпространството и справяне с нея. Обучаемите получават специализирани теоретични познания по технологиите за информационната сигурност в държавната администрация, сигурността и отбраната, бизнеса, транспорта и енергетиката,

финансите и счетоводството, банковото дело, науката и образованието, правната система, здравеопазването и др. Разглеждат се съвременните концепции за мрежова структура, осигуряваща нужната надеждност и ефективност, техническите и програмните методи за осигуряване на защита на информацията в информационните системи. Придобиват се умения за разработка и прилагане на различни методи, техники и технологии за организационни, програмни, технически, криптографски и икономически цели; за проектиране разработване и внедряване на защитени информационни системи в киберпространството; за работа със стратегически системи за подпомагане вземането на решения и пр.

Завършилите могат да работят като експерти, аналитици, администратори по сигурността, консултанти и специалисти в службите за сигурност и обществен ред, структурите за управление при кризи и други държавни институции и частни фирми, разработващи и поддържащи софтуер на системите за информационна сигурност, защита на комуникации, защита на класифицираната информация и в други области за приложения по киберсигурността, както и да извършват изследвания в областта на информационните системи, електронното управление, мениджмънт на знанията и др.

ОБОБЩЕН МОДЕЛ НА ОБУЧЕНИЕТО

Основната цел на магистърската програма „МИС“ е свързана с изграждането на теоретичен и практически фундамент в знанията и уменията за изграждане на мрежова и информационна сигурност, както и умения за решаване на казуси от практиката.

Според Michael E. Whitman и Herbert J. Mattord [7] учебният план за обучение, по мрежова и информационна сигурност може да се изгражда като се използват различни подходи. Специалистът по МИС трябва да има добро математическо образование с акцент върху онези дялове от математиката, които са приложими за проектиране и разработване на системи за зашита на информацията и софтуерни системи за осигуряване на информационна сигурност. Той трябва да познава стандартите в тази област и техните изисквания. Да има познания за организацията на системите за информационна сигурност, които включват: *политиката* – съвкупност от формални правила, регламентиращи механизмите за информационна безопасност, идентификацията и автентификацията: *одита* и *мониторинга* – проследяване на събитията в процеса на обмен на информация: *управление на риска* и пр.

Предлага се един обобщен модел на обучението по МИС във ВТУ „Т. Каблешков“, чрез който се търси съвкупността от теоретични знания по МИС:

$$(1)\ \text{МИС}^{\text{знания}} = f\{\text{ИУКМ, НБКС, ИЗ, СДИ, НСМИС, КС}^1\text{, ОИС}^1\text{, РЕРКИ,МСА, ИУИС, ИАЗС, АОРИС, УСЧР, ЗССС}^2\text{, ВЧМБЗ}^2\text{, ИСМАОИСПП}\} \geq min$$

, където

$\text{МИС}^{\text{знания}}$ са натрупаните знания в областта на мрежовата и информационна сигурност, което е в зависимост от заложените учебни дисциплини, както следва [11]:

- ИУКМ – *Изграждане и управление на компютърни мрежи;*
- НБКС – *Надеждност и безопасност на компютърните системи;*
- ИЗ – *Информационна защита;*
- СДИ – *Системи за детектиране на интрузия;*
- НСМИС – *Нормативи и стандарти за мрежова и информационна сигурност;*
- КС^1 – *Корпоративна сигурност*(първа избираема група);
- ОИС^1 – *Одит на информационни системи* (първа избираема група);
- РЕРКИ – *Работа на екипи за реагиране при компютърни инциденти;*
- МСА – *Мрежова и системна администрация;*
- ИУИС – *Интелигентно управление на информационната сигурност;*
- ИАЗС – *Информационни атаки и злонамерен софтуер;*

- АОРИС – *Анализ и оценка на риска на информационните системи;*
- УСЧР – *Управление и сигурност на човешките ресурси;*
- ЗССС[2] – *Защитни стени и специализиран софтуер*(втора избираема група);
- ВЧМБЗ[2] – *Виртуални частни мрежи и безопасни зони*(втора избираема група);
- ИСМАОИСПП – *Използване на системи за мониторинг, анализ и оценка на информационните събития и потенциални проблеми;*

при ограничение – натрупаните знания за всяка от дисциплините в (1) да са ≥ от необходимите минимални знания.

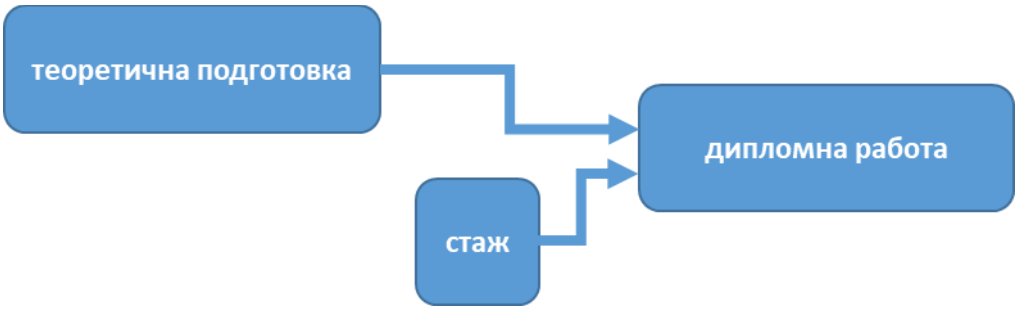
За създаване на практически умения се предвижда стаж по специалността в размер на минимум 2 седмици:

(2) $\text{МИС}^{\text{стаж}} = f(t) = 2$ седмици

Завършителната част на обучението предвижда разработване и защита на дипломна работа в областта на мрежовата информационна сигурност:

(3) $\text{МИС}^{\text{ДР}} = f(t) = 1$ семестър

Задължително условие е да се спазва технологичната последователност на обучението, показано на фиг. 1.



Фиг.1. Технологична последователност на извършване на обучението по МИС

Показаното на фиг.1 гарантира систематичността на провежданото теоретично обучение, практическия опит, натрупан по време на стажа и самостоятелната работа по изграждането и защитата на проект в областта на МИС.

ТЕМАТИЧЕН ОБХВАТ НА ТЕОРЕТИЧНОТО И ПРАКТИЧЕСКО ОБУЧЕНИЕ

Тематичният обхват на теоретичното обучение включва следните теми за отделните дисциплини:

- ИУКМ – Представят се основните понятия, същността и видовете компютърни мрежи – кабелни и безжични, мрежовите устройства и мрежовия софтуер, както и най-разпространените стандарти за мрежова архитектура, топология на мрежите и протоколи за работа на слоевете. Разглеждат се в теоретичен аспект същността и слоевете на мрежовите модели OSI и DoD (TCP/IP) и за най-разпространените протоколи на протоколния стек TCP/IP. Изграждат се умения за конфигуриране на мрежови устройства и компоненти. Прави се обзор на приложните системи и софтуер за проектиране, конфигуриране, тестване и мониторинг на мрежи, както и изграждане на реални мрежи, работа с помощни програми и др. Използват се приложни инструменти за проектиране и мониторинг на компютърните мрежи. Разглеждат се въпроси за технико-икономическо планиране и развитие на капацитета на мрежите.
- НБКС – Представят се основните моменти от теорията на надеждността и безопасността. Разглеждат се принципите за изграждане и методите за оценка на безопасността на компютърни системи. Изучават се анализ и моделиране на

надеждността и безопасността на отказоустойчиви компютърни системи. Разглеждат се основните методи за изграждане на високонадеждна и безопасна след откази система. Изучават се методите за анализ на надеждността и безопасността на системите и свързания с тях риск.

- ИЗ – Разглеждат се съвременните системи за откриване на неправомерни действия и защита от нарушения при работа в мрежите, комплекс от мерки за защита на информация и криптография. Осигуряват се основни знания и практически умения от областта, засягаща всички потребители на компютърната техника и на различни уеб приложения. Дисциплината има пряка връзка с други дисциплини, свързани с програмиране, мрежови защити, киберсигурност, приложения на теория на вероятностите, Теория на числата, теоретични основи на информатиката, логическото програмиране и др.
- СДИ – Представят се основни понятия в областта на детектиране на интрузии и видовете атаки в мрежите, срещу които ще се прави защита според различните слоеве на OSI модела. Анализират се съществуващи системи за детектиране на интрузии в компютърни мрежи и системи за детектиране на интрузии в крайни системи (сървъри и потребителски компютри). Разглежда се най-известната система за детектиране на интрузии в компютърни мрежи SNORT. Разглеждат се методи за планиране на защитни архитектури. Третира се и проблемът за проактивна автономна работа на IDS в локална мрежа. Анализират се различни видове интелигентни имунни системи за защита от интрузии и се разглеждат видове модели и методи за прилагането им. Представят се различни варианти за анализ на интрузии чрез използване на поведенчески модели и прилагането им в сървърни и потребителски системи. Разглежда се метод за защита от интрузии чрез въвеждане на контрол върху интегритета на файлови системи и файлове. Обясняват се архитектура на система за превенция на интрузии. Акцентира се върху проблеми на детектиране на интрузии в реално време. Представят се съвременни нерешени проблеми в методи за детектиране на интрузии в крайни системи (end host).
- НСМИС – Включва теми по основните понятия и терминология от нормативната рамка и уредба в областта на МИС, стандарти за изграждане на безжични мрежи; международни стандарти за системи за детектиране и защита от интрузия в комуникационни мрежи, стандарти при разработването на софтуер и хардуер; персонална идентификация; идентификационни карти и устройства; електронен подпис и карти, както и свързани с тях системи и дейности; стандарти за захранване на съобщителни системи; безопасност на електронни устройства от областта на аудио/видео и информационни и съобщителни технологии; системи за дома и сгради; далекосъобщителен обмен на информация между системи; свързване на съоръжения за обмен на информация; съоръжения за офис. Обръща се внимание на възможностите и ограниченията, които налага законовата рамка и стандартите при изграждането на сигурни комуникационни системи.
- КС[1] – Разглежда се специфичната нормативна база, чрез която се регулира корпоративната сигурност. Определя се структурен модел на сигурността. Прави се анализ на средата на управление и управляващата и изпълняваща система. Изучават се проблеми при идентификация на ценностите, корпоративните интереси и отговорности. Идентифицират се рисковете за корпоративната сигурност.
- ОИС[1] – Одитът на информационните системи включва описание на модела за изграждане на система за сигурност на информацията, определят се заплахите, уязвимостите, оценява се рискът и мерките, предприети за снижаването му, разглеждат се методи за анализ на управлението на риска. Излагат се базови понятия за одит по сигурността и се дават характеристики на целите на неговото провеждане. Анализират се основните стандарти, използвани при провеждането на одита, разглеждат се и се

анализират основните контроли от *Annex A* на международния стандарт за управление на информационната сигурност, както и подходът при даването на препоръки по прилагането му. Формират се основни понятия за одит на системи за управление.

- РЕРКИ – Описва процеса на създаване на екипи за реагиране при компютърни инциденти (CERT) във всички свързани с това аспекти като бизнес управление, управление на процеси, както и от техническа гледна точка. Разглеждат се въпроси свързани със създаването, израстването и работата на Националния център за реакция при инциденти в МИС. Студентите се запознават с мисията, целите и задачите, законовата рамка и услугите, които се предлагат, процедурите за обработка на инциденти; анализа и съхраняването на артефактите. Обсъждат се най-интересните случаи от статистиката на българския център и превантивните мерки необходими за ограничаване на щетите или повторното им появяване. Изучава се процедурата за обработка на инциденти и артефакти и се прави разлика между събитие, атака и инцидент. Придобиват знания как да се приоритизират и класифицират инцидентите се анализират инциденти със значително въздействие.
- МСА – Представят се основните принципи на системната и мрежовата администрация. Разглеждат се методите и средствата за изграждане на политики за управление на правата на потребителите и ресурсите на системите (AD, LDAP и др.). Изучават се основните методи за управление на рутирането OSPF и RIP. Представят се и основните елементи, структура и конфигуриране на DHCP и DNS сървърите. За администриране на Windows и Linux базирани мрежи се дават се знания и се формират умения за същността и работа със сървъри за електронна поща (mail), интернет страници (www), за обмен на файлове (ftp), за SQL бази данни, както и достъп до мрежови ресурси чрез Active Directory, LDAP, Samba Sharing и др. Отделя се внимание на мониторинга на IP базираните мрежи, чрез използване на SNMP. Важен акцент се дава и на средствата и способите за изграждане и управление на CLOUD информационни структури.
- ИУИС – Интелигентно управление на информационната сигурност дава теоретически и практически знания по изграждане и работа с модела на проблемната област, по отстраняване на неточности или непълноти, по придобиване и формализация на знания за целите на интелигентните приложения, по изграждане на класически и съвременни машини за извод или за разсъждение с използване на модерни, често интердисциплинарни теории от областта. Дават се знания за модерните логически приложения, невронните мрежи, многоагентни системи и други разпространени изследователски области с по-голям теоретически или практически интерес на икономическите приложения. Една от целите е запознаването с многобройните термини, понятия и сложни синтетични методи от областта и придобиването на стратегическо мислене при проектиране на жизнения цикъл на интелигентните системи и при практическите приложения.
- ИАЗС – Анализират се функционалната и интрузионната устойчивост на TCP/IP комуникационния стек. Разглеждат се най-използваните операционни системи като Windows OS, Linux OS, Android OS и iOS. За тях се разглеждат видовете атаки и слаби места за проникване. Анализара се интрузионната устойчивост, видове сценарии за атаки, анализ на последствията, индикатори за наличие на атаки в системата и варианти за противодействие. За компютърните мрежи и крайни системи се разглеждат атаки в ETHERNET комуникационните протоколи, атаки в TCP/UDP, IP слоя и др. Основен акцент се поставя и върху начините за провеждане на атаки в Wi-Fi мрежи. Представят се методи за проследяване на потребителска активност в интернет и събиране на данни за социален инженеринг. Дефинират се индикатори за наличие на атаката, както и методи за противодействие. Разглеждат се още видовете атаки срещу разплащателни

системи и подмяна на идентичност и се прави анализ на различни сценарии за провеждане, както и на методи за противодействие. Представя се анализ на видове програми за преодоляване на сигурността на компютърни системи, както и класификация и ефекти от използването им. Анализират се програми за преодоляване на криптографски системи, и сценарии за провеждане на атаки и противодействие.

- АОРИС – Изучават се вероятностни твърдения и модели, случайни величини и основни теоретични разпределения. За статистическия анализ на данни се изучават основни статистически понятия, величини и характеристики. Разглеждат се различни начини за представяне на данни и пресмятане на техни средни стойности. Правят се проверки за достоверност на направените прогнози и хипотези. Изучават се и основни понятия за риска, управлението му и неговите фази. Студентите се запознават и с конкретни вероятностни модели за анализ и оценка на риска на информационните системи.
- УСЧР – Разглеждат се основни понятия в областта на управлението на човешките ресурси: стратегия, политика, програма и план за управление на човешките ресурси. Анализират се различни модели и начини за тяхното реализиране в управлението, ръководството и работата на дадена организация. Акцентира се върху съвременните подходи за подбор на човешки ресурси и за избягване на грешки в управлението им. Разграничават се понятията „човешки ресурси“ и „човешки капитал“. Акцентира се върху съвременните подходи за развитие на човешкия капитал. Сигурността на човешките ресурси (персонална сигурност) разглежда основните понятия в областта на управлението на риска, превенцията и неутрализирането на т.нар. „заплаха от вътрешен човек (insider threat)“. Разясняват се предпоставките за възникване, наличие и развитие на заплахата от вътрешен човек. Разясняват се изискванията на персоналната сигурност и различните етапи за идентифициране и преодоляване на потенциална заплаха от вътрешен човек.
- ЗССС^2 – Разглеждат се общи понятия в защитните стени. Дефинира се принципна структура на функциите на защитната стена, както и теоретичния модел на работата на защитна стена. Разглеждат се три генерации защитни стени. Анализ на функционалността на първа генерация защитни стени от тип „пакетни филтри“; анализ на производителността и проблеми при интрузионни атаки. Анализ на функционалността на втора генерация защитни стени от анализиращи цялостна връзка от сокет до сокет; функционален модел; анализ на производителността и проблеми при интрузионни атаки. Анализ на функционалността на трета генерация защитни стени от тип „анализатори на приложни протоколи“; функционален модел, анализ на производителността и проблеми при интрузионни атаки. Представят се различни видове архитектури на защитни стени при проектиране на мрежова сигурност. Дават се принципите за проектиране на сигурността на компютърни мрежи чрез използване на защитните стени. Представя се начинът за работа с прокси сървъри и методи за конфигурирането им. Представят се методи за използване на защитни стени за управление на сигурността в Cloud базирани информационни архитектури. Анализират се начините за реализиране на защитни стени в Windows OS и Linux OS. Анализират се комбинирани решения на защитни стени и антивирусни програми.
- ВЧМБЗ^2 –дават се основни понятия във VPN мрежите. Разглеждат се видове архитектури, софтуерни и хардуерни реализации. Представят се методи за сигурна автентификация и осигуряване на надеждност на връзките. Прави се анализ на методите за генериране и обмен на ключовете и управление на SSL/TSL конфигурации. Обяснени са принципите за създаване на демилитализирани зони. Разгледани са формите за създаване на CA (certificatedauthority) структури и основни понятия, и елементи на CA. Разглеждат се и основни елементи на OpenVPN решението, елементи

на клиентския и сървърния софтуер, както и метод за генериране на ключовете и сертификати. Разглежда се използване на KERBEROS за изграждане на автентификационни системи в ИНТЕРНЕТ и локални мрежи, използване на PGP за изграждане на автентификационни системи в ИНТЕРНЕТ и локални мрежи. Представени са варианти за инсталиране, конфигуриране и използване при планиране на защитени локални и интернет зони. Разгледани са алтернативни подходи чрез използване на методи за скриване на IP адресите на крайните системи.

- ИСМАОИСПП – Използването на системи за мониторинг, анализ и оценка на информационните събития и потенциални проблеми дискутира методите за създаване на модели за откриване на интрузионни следи в комплекси комуникационни мрежи и информационни системи. Предлагат се методи за оценка на качеството на обучение на системите с изкуствен интелект за откриване на интрузии. Демонстрира се метод за използване на машинно обучение за изграждане на системи за защита на комуникационни мрежи и информационни системи. Обсъждат се формите за изграждане на проактивни системи за интрузионна защита.

ЗАКЛЮЧЕНИЕ

Настоящата публикация представя обобщен модел, технологичната последователност и тематичния обхват на теоретичното и практическо обучение по новата магистърска специалност „Мрежова и информационна сигурност“ във ВТУ „Тодор Каблешков“. Въпреки, че това е динамична задача, която изисква постоянно актуализиране на знанията в тази област, основната цел се постига чрез изграждането на теоретичен и практически фундамент от знания и умения за проектиране и изграждане на МИС, както и решаване на казуси от практиката. Този фундамент е солидна основа за анализиране и справяне с най-новите заплахи и предизвикателства пред информационната сигурност, каквито са заплахите в киберпространството. Основната цел е създаването на експерти, аналитици, администратори по сигурността, консултанти в службите за сигурност и обществен ред, в структурите за управление при кризи, държавни институции и частни фирми – задача със стратегическа актуалност и в бъдеще.

ЛИТЕРАТУРА:

[1] ПОЗИЦИЯ НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ, приета на 13 март 2014 г. с оглед приемането на Директива 2014/./ЕС на Европейския парламент и на Съвета относно мерки за гарантиране на високо общо ниво на мрежова и информационна сигурност в Съюза http://www.europarl.europa.eu/sides/getDoc.do?type=TC&reference=P7-TC1-COD-2013-0027&format=PDF&language=BG

[2] http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0251en01.pdf

[3] https://europa.eu/european-union/about-eu/agencies/enisa_bg

[4] http://eur-lex.europa.eu/legal-content/BG/ALL/?uri=CELEX:52011DC0163

[5] http://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX%3A32016L1148

[6] https://govcert.bg/

[7] Michael E. Whitman, Herbert J. Mattord CISM, CISSP CISM, Principles of Information Security, Fourth Edition, 2011, Kennesaw State University , Library of Congress Control Number:, 2010940654, ISBN-13978, Course Technology, Channel Center, Boston, MA, 02210, USA

[8] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:321:0001:0004:BG:PDF

[9] Bradley Bogolea, Information security curriculum creation: a case study, 2004, ACM

New York, NY, USA, ISBN:1-59593-048-5
[10] Димитров Д., Лабораторна база за обучение и експериментални изследвания в областта на информационните и интернет технологиите във ВТУ „Т. Каблешков“, Научно списание „Механика Транспорт Комуникации“, 1, IV-1 IV-6, 2015, ст. № 1107Саркисян А., Обучение на български специалисти с висше образование по информационна безопасност, Списание, Диалог, 3, 2011
[11] [12] Учебен план, програми и документация на обучението по „Мрежова и информационна сигурност“ във ВТУ „Тодор Каблешков“
[13] Христова М. Софтуер за критични по безопасност системи: проблеми и решения. Монография, Издателство ВТУ „Т. Каблешков”, София, ISBN 978-954-12-0240-1, 2016
[14] Hristova M.,Potentialities of Modern Information and Communication Technologies in Logistics and Transport, Technology and Art, Research and Topicalities, ISSN 2029-400X, Vilnius College of Technologies and Design, Vilnius, Lithuania, pp. 104-110, 2015

CURRENT ISSUES AND INNOVATIONS RELATED TO THE TRAINING OF STUDENTS IN THE FIELD OF NETWORK AND INFORMATION SECURITY

Dimitar Dimitrov[1], Maryia Hristova[1], Vencislav Trifonov[2]
ddimitrov@vtu.bg, mhristova@vtu.bg, vencislav.trifonov@gmail.com

[1]Todor Kableshkov University of Transport, 158 Geo Milev Str., Sofia,
[2]Technical University,.8 Kliment Ochridski Blvd.
BULGARIA

Key words: *Network and Information systems, Network and Information Security, Internet, Computer Systems and Networks, training*

Abstract**:** *Network and information security is essential for both the public and the private sectors of the economy and for the protection of critical management information infrastructures. In recent years, network and information systems of various organizations are potentially affected by increasingly frequent security incidents, that are more complex and on a larger scale. To promote a more sophisticated culture of network and information security in the European Union, the European Community has established the European Network and Information Security Agency (ENISA).*

The present paper addresses relevant network and information security issues raised by the European Parliament's Directive on measures to ensure a high level of network and information security in the European Union. The human factor remains the weakest part of cybersecurity, therefore the importance of the preparedness of the work force in this field is increasing. We focus on the exceptional relevance and necessity of creating a new Master of Science (MS) program "Network and Information Security" (NIS) to meet the requirements of the National Strategy and the National NIS Cooperation Plan. We share some innovative visions, ideas and practices in the program that ensure its strategic relevance in the future.