Кратки резюмета
на научните публикации, научните трудове и другите научни разработки
на майор гл. ас. д-р инж. Линко Г. Николов

| № | Наименование, резюме |
|---|---|
| 1 | Линко Николов, **Киберсигурност на КИС – монография**<br>В тази монография, структурирана в 4 глави, са съсредоточени конкретни резултати от изследвания върху сигурността на комуникационно-информационна система, осигурявана от междинни устройства (маршрутизатори и комутатори), и върху уязвимостите на приложенията, работещи в крайните информационни системи (клиентски станции, сървъри и др.). Изследванията са проведени в контролирани условия, като мрежовите ресурси са собственост на Националния военен университет. В глава първа „Киберзаплахи за съвременните комуникационно-информационни системи“ са разгледани заплахите, експлоатационните пробиви и злонамерените действия в една КИС, както и преглед на наличните Инструменти и техники за изследване на киберсигурността. В глава втора „Анализ на уязвими мрежови процеси и възли в комуникационно-информационните системи“ са извършени действия по проверка на сигурността на мрежовата инфраструктура, като са използвани както речникови атаки, така и атаки с „пълно комбиниране“ след ограничаване на някои параметри на паролните стрингове. В глава трета „Системни и програмни уязвимости“ е извършен преглед на слабостите в операционните системи и анализ на сигурността в използваните приложения. В глава четвърта „Осигуряване на киберзащита в комуникационно-информационните системи“ е предложена Политика за киберсигурност както и методология и административно-технически дейности по защита на междинните и крайните устройства. |
| 2 | Линко Николов, **Възможности за динамично разпределение на трафика към паралелни безжични мрежи –част I**<br>Тази публикация е първата от серията два доклада за възможности в обработката на клиенти при безжична мрежова среда. Тук се представя математическата теория на вероятността на обслужване на крайните устройства от централно управляващо устройство. Публикацията представлява обобщение от преглед на съществуващи литературни източници и основополагащи математически теории в областта на статистиката. В разглежданите модели за тест се посочва обстоятелство по ограничаване на информацията относно текущото състояние на трафика в различните направления, които централното устройство управлява. |
| 3 | Линко Николов, **Възможности за динамично разпределение на трафика към паралелни безжични мрежи –част II**<br>Тази публикация е втората от серията два доклада за възможности в обработката на клиенти при безжична мрежова среда. Поради разтегателното представяне на моделите за изследване и теоретичните аспекти, е необходимо разделянето на изследването в две публикации. В този доклад са посочени проверки за възможност за обслужване или за отказ от обслужване от страна на централно управляващо устройство по динамичен принцип. Числовите експерименти, след тестовете за обслужване, са представени в няколко таблици и една композитна графика, съдържаща теоретично представяне и две представяния с при ограничена информация за наличие на трафик – алгоритми на Бейс о „JSQ“ (Join the shortest queue). Резултатите показват, че въпреки изследваната система да разполага с по-малко информация в сравнение с напълно проучена система, частичното проучване не прави значителен компромис с времето на живот на заявките (задачите) и обслужването на клиенти с безжичен достъп. |
| 4 | Линко Николов, Красимир Славянов, **Развитие на анонимните мрежи и аспекти на сигурността в бъдещите мрежи** |

| | |
|---|---|
| | Желанието да се запази сигурността и тайната в киберпространството подтиква изследването в областта на анонимните мрежи. Всяка единица, работеща в киберпространството, е податлива на кибер атаки. Интернет днес е невероятно ефективно и неконтролирано оръжие за подслушване и шпиониране. С кибер атаките, целящи да получат разузнавателна информация и да прекъсват комуникацията, се задава нова ера на война. В този доклад се посочва, че тайната и анонимността в комуникационно-информационните системи са въпроси с нарастваща важност. Изброени и разтълкувани са шест кабелни и единадесет безжични анонимни мрежи. Като заключение се посочва, че в състояние на постоянна кибервойна, анонимността може да намали уязвимостта и да защити собствените мрежови и информационни ресурси чрез осуетяване на неприятелските способности за събиране на информацията и разстройване на комуникацията. |
| 5 | Лора Ралева, Теодор Тодоров, Линко Николов, **Съображения за сигурност при сесиите с „бисквитки" в интернет браузърите**<br>Тук са посочени функционалните особености на информационните „бисквитки" (кукита, „cookies") в интернет браузърите и потенциалните заплахи и уязвимости, които предоставят. Дефинирани са съображения за сигурност, необходими от страна на потребителите и методи за защита в домейн-сървърите, като технически устройства. За да бъдат преодолени уязвимостите по сигурността на данните в бисквитките, трябва на първо място потребителят да е добре информиран за тяхната полза, как те да бъдат правилно управлявани и кога е необходимо използването на бисквитките. Също така, при програмирането на даден сайт трябва да се вземат под внимание параметри на бисквитките като съкратена давност, реална необходимост от реклами и определяне на разрешаваните домейни. Потребителят би трябвало да е наясно с разрешаването или забраняването определенията от него сайтове да използват бисквитки. На второ място може да се посочи осигуряването на метод на защита. Използването на криптографски сигурен алгоритъм, осигуряващ достатъчна сложност на алгоритъма за криптиране би осуетило евентуална заплахата от атака. Като съображение за сигурност не на последно място може да се отбележи отговорността на потребителите да съхраняват или изтриват излишни бисквитки, запазени на компютъра като история на посещенията и други, които биха допринесли за нежелан несанкциониран достъп до данни. |
| 6 | Линко Николов, Красимир Славянов, **Ефективност на софтуер за комуникационно разузнаване**<br>Един софтуер за сигнално разузнаване може да се състои от няколко модула с различни функции за радионаблюдение и радиолокация. В този доклад се посочва, че разузнавателната информация се придобива след извършването на няколко стъпки от кръгов процес, включващ планиране/насочване, събиране, обработване, анализ и разпространяване на информация, като всички тези стъпки трябва да са предвидени от разработчиците на софтуера, с цел да се постигне пълен обхват от мероприятия. Кръговият процес определя обратна връзка, чрез която се оценява степента на ефективност на сигналното разузнаване и до каква степен са изпълнени поставените изисквания. В доклада са посочени различни функционалности на стратегически системи „COMINT" и тактически системи „CESM". Оперативните изисквания за една CESM система трябва да отговарят на възможните средства за комуникация. Понякога обаче се налага наличната система за комуникация да бъде заменена с по-мощна, за да отговаря на все по-строгите оперативни изисквания за радиомониторинг. Софтуерната част на една такава система се определя като позволяваща широколентови сензори, които от своя страна създават големи обеми от данни, които да от своя страна е необходимо да бъдат дистанционно управлявани с използване на нискоскоростни комуникационни канали. |
| 7 | Линко Николов, **Еволюция към 4G широколентови комуникации**<br>В този доклад е направен анализ на развърнатите за своето време клетъчни комуникационни инфраструктури и е посочена тенденцията за преминаване към системи от следващо поколение. Следващо поколение означава повишени възможности от гледна точка на капацитет за предаване на данни, брой свързани мобилни устройства и улеснено управление на комуникационните канали от страна на контролерите в базовите станции. Чрез фигуративни графики са показани пазарните тенденции, като на фигура 2 е показано и прогнозно развитие. Посочени са предимствата на новоопределената форма на радиосигнала – тази с ортогонално честотно мултиплексиране. Разгледан |

| | |
|---|---|
| | е и аспект за оптимизиране натоварването с мрежови трафик чрез преразпределение между умален в пространството обем, но повишено като количество брой клетки и контролери (Radio Resource Control-RRC) в лицето на крайни устройства – мобилни терминали. |
| 8 | Юлия Матева, Линко Николов, **Алтернативата IPv6 за компютърните мрежи**<br>Интернет протокол версия 6 (Internet Protocol version 6 – IPv6) се явява еволюция на версия 4 (IPv4). IPv6 предвижда по-лек механизъм на обработване на хедъра, защото всеки отделен пакет може да бъде с различна дължина. Значително е увеличено адресното пространство, а методите за автентикация са усъвършенствани. Новият протокол предлага увеличаване на количеството битове, отредени за един адрес – 128 бита. Това предполага около $3{,}403.10^{38}$ броя адреси. При IPv4, адресите се записват с 32 бита, т.е този протокол определя $2^{32}$ уникални адреса, почти всички от които вече са заети), докато при IPv6 броят уникални адреси е $2^{128}$. Предвидени са домакински уреди, автомобили, смартфони, е-книги, таблети, лаптопи, „wearables“ и други (IoT) устройства да използват свързаност към Интернет. Всички те ще могат да работят с IPv6. В този доклад са представени в резюмиран и съкратен вид най-важните функционалности на протокол IPv6. Във военната сфера беше представен войника на бъдещето с приблизително 50 мрежови устройства в униформата си, ползващи IP адрес. Поради този факт, както и поради изискването за повишаване скоростта на предаване на данни по компютърните мрежи, специалистите в тази област предложиха новата версия на мрежовия протокол. Като подобрение от изключителна важност може да се посочи възможността за по-голям брой уникални адреси. Пред разработчиците са предявявани изисквания за опростеност, повече гъвкавост и по-висока ефективност от гледна точка на функциите, с които новият мрежов протокол трябва да разполага. |
| 9 | Linko Nikolov, Nikolay Kulev, **A survey on the quality of digital images**<br>В този доклад е направен литературен обзор на експерименти по компресиране на изображения, като се изследва качеството на картината, спектралните характеристики и степента на загуба на информация. Като параметри за сравнителен анализ са използвани корелационни характеристики между оригинално и компресирано изображение, както и средно квадратично отклонение в стойностите на цветова гама за два еднакви обекта в съответните оригинално и компресирано изображение - MSU-BM (MSU – Blocking Measure – оценка за блокиране движението на артефакти при MPEG компресия); VQM (Video Quality Measure) и SSM (Structural Similarity Metric). |
| 10 | Линко Николов, **Засекретяване предаването на данни в CDMA2000 1xEVDO**<br>Един от няколкото реализирани стандарта на клетъчната система с кодово разделяне на каналите CDMA2000 е „1XEV-DO“, който е изцяло с пакетна обработка на цифровите данни. В тази система, пакетите с данни биват засекретявани (криптирани) на няколко етапа посредством протоколи, работещи в обособен слой за сигурност от затворения мрежовия модел по стандарт CDMA. Тук е разгледан слоят за сигурност с неговите функционални възможности, определени от внедрените стандарти и протоколи за мрежова сигурност. Посочени са и йерархията и стъпките при генерирането на ключове между кореспондентите. Като резултати от анализа се посочва, че използваните протоколи са надеждни и процесорната им обработка не усложнява в голяма тежест потока от инструкции. Не се получава ненужно забавяне на пакетите, а латентността е в границите на приемливото за потребителя. Недостатък в изследваните процеси по засекретяване се посочва ниската криптографска устойчивост на ключовете при налична частична информация, включена в процеса на генериране. С цел да не бъдат натоварвани процесорите в базовите станции и терминалите, протоколите за криптиране не генерират ключове с достатъчна дължина и криптографски свойства. Това се явява уязвимост в сигурността на системата, но тя се открива само при специализирани преднамерени атаки и криптоанализ. |
| 11 | Krasimir Slavyanov, Linko Nikolov, **An algorithm for ISAR image classification procedure**<br>В този доклад е предложена архитектура за автоматично разкриване на обекти при цифрови радари |

| | |
|---|---|
| | с обратна синтезираща апертура чрез софтуерна обработка от алгоритъм на невронна мрежа. Алгоритъмът на изследваната двуслойна невронна мрежа притежава свойство за оптимизация на изображението с висока ефективност, което се доказва с графики след изчисляване обема на целеви елементи. За обучение на алгоритъма са проведени 72 епохи, а за качеството на алгоритъма се определя средно квадратична грешка в изчисленията за обем равна на $1.10^{-1}$ . В доклада се посочва, че този алгоритъм е подходящ само за класа обекти, които са предварително известни и за които корелацията е възможна. Особено важна характеристика при изграждане изображението на радиолокационната цел е пикселното съотношение. То участва в разпознаването на целите, дори в условията на силни смущения, характерни за радиолокационния канал. Друг резултат след анализа в този доклад е високата скорост в изчислението и обработката на изображенията на целите. Този алгоритъм се оказва подходящ и при използването му за други задачи, свързани с машинно обучение, но приемащи същите ограничения за предварителна информация и приложимост на желаното крайно състояние. |
| 12 | Linko Nikolov, Dyanko Hubenov, **BER performance for WCDMA signal in a jammed radio environment**<br>В тази публикация са представени резултати от симулационно изследване приемането на радиосигнали в радиокомуникационен канал от стандарт WCDMA в усложнена радиокомуникационна среда чрез симулационен софтуер. Стандартът е 3GPP WCDMA, а каналът е низходящ, с честотно разделяне (FDD, Release99). Симулационният софтуер има възможност за изчисляване вероятността за възникване на цифрова грешка, като изследваните обекти са блокове с пакети, трафик канала и контролния канал, а параметрите са съответно „BLER“, „DTCH BER“ и „DCCH BER“. Резултатите са представени в табличен вид, а на графика е изобразена формата на предадения и на приетия сигнал. Предложен е модел на широколентов смутител симулиращ мощност на смущаващия сигнал 5W. Недостатък се явява краткото симулирано време на работа на системата поради ниската изчислителна мощност на процесора, който обработва симулационния софтуер, но получените резултати дефинират ориентировъчни стойности с достатъчна точност за определяне на минималното необходимо съотношение сигнал-шум в приемника за осигуряване на непрекъсваемост на комуникационните услуги. |
| 13 | Linko Nikolov, Krasimir Slavyanov, **On the contemporary cybersecurity threats**<br>След приемането на обстоятелството, че петата област на бойното поле ще е киберпространството, въпросите по киберсигурността нараснаха неимоверно. В този доклад са разгледани тенденциите на киберзаплахите от гледна точка на компютърната, мрежова и облачна сигурност. Посочени са актуалните посоки на кибератака, най-известните, най-широко използваните и най-често срещаните атаки, главните уязвими точки в компютърните системи и мрежи, както и топ 10 на уеб рисковете според световни източници. Посочен е конкретен пример за уязвимост в система за база данни, както и пример за атаки чрез техниките за социално инженерство. Като техники за защита са посочени оперативни насоки за системните и мрежовите администратори. |
| 14 | Линко Николов, **Ролята на Европейския съюз в осигуряването на Киберсигурност**<br>Този обзорен доклад разглежда насоките, разисквани от Европейската комисия и от Европейската агенция за мрежова и информационна сигурност по изграждане на единен систематичен подход при справянето с проблемите на киберсигурността. Посочва се, че Република България, със своите новосъздадени стратегически документи, а именно Закон за киберсигурност и Национална стратегия за киберсигурност, представя пред европейската общност готовност за спазване на ценностите и принципите за осъществяване на качествен и ефективен контрол при възникване на кибер инциденти. Властите и компетентните органи в Република България, като пълноправен член на Европейския съюз, имат идея за създаване на Национална координационно-организационна мрежа за кибер сигурност НКОМКС по модела на публично-частните партньорства, чрез която ще може да се интегрират единните европейски директиви и документи по мрежова и информационна сигурност. Като резултат от този обзорен доклад може да се заключи, че перманентното обучение на персонала, работещ в киберпространството, трябва да стане задължителен елемент. Трябва да бъдат установени |

| | |
|---|---|
| | специализирани изследователски и приложни центрове с уникални компетентности и технологична база за симулации, обучение, изпитване и активна защита на IT-системи, системи за управление в индустрията и критични инфраструктури. Посредством новоизградените координационни центрове, следването на единна рамка за сертифициране и постигането на защитен общ електронен пазар в Европейския съюз, а в това число и в България, ще бъде адекватно отговорено на съвременните предизвикателства пред киберсигурносттта. |
| 15 | Линко Николов, **Същност, роля, място и задачи на кибер защитата в сигурността и отбраната**<br>В този обзорен доклад са разгледани основните принципи и методи за осигуряване на киберсигурност. Дефинирани са и ориентировъчни понятия за направлението Киберсигурност, като се посочват същността, ролята, мястото и задачите, изпълнявани в процеса на осигуряване на защита на електронната информация в компютърните системи и мрежи. Постигането на едно желано крайно състояние на кибер устойчивост е свързано с всеобхватно преосмисляне на проблемите на сигурността, формиране на адекватни на съвременните реалности концепции и осъществяване на система от взаимосвързани практически действия, водещи към изграждане на качествено „нова архитектура“ на системата на национална сигурност. Главното в това преосмисляне е възприемането и утвърждаването на формулираната теза, че „основа“ и „изграждаща конструкция“ на „новата архитектура“ на сигурността в комуникационното общество е киберсигурността, разглеждана във всичките й измерения - технологично-информационно, правно-институционално и политическо. Архитектурата на кибер защитата ще отразява моментното (актуалното) състояние на потребностите, и ще има възможност за преминаване към ново, по-съвършено и в по-голяма степен отговарящо на целите на системата, състояние. Кибер защитата трябва ше покрива целия спектър от уязвими места и критични точки. Информацията, независимо от носителя, върху който се съхранява, и вида на нейното представяне в преносната среда (масиви от данни, глас, видео, телефония и др.), ще бъде надеждно защитена. Все още обаче не е конкретизиран най-старшия, най-главния отговорник за изпълнението на всички тези дейности по кибер защита. В политически аспект, в Република България трябва да се въведе единоначалие и единен подход за управление на киберсигурността, който към момента на написване на този доклад липсва. |
| 16 | Линко Николов, **Анализ на уязвимостта на безжична компютърна мрежа, защитена с криптографски протокол WPA2**<br>В една КИС, потенциален вход за атака е безжичната точка за мрежов достъп. Въпреки защитаването й със стрингова парола, по метода на отгатване с пълно комбиниране е възможно злонамерено лице да осъществи нерегламентиран достъп. В този изследователски доклад са представени времената за разбиване на няколко модела на пароли чрез инструменти за атака с пълно комбиниране и атака с помощта на стрингови пароли от речник. За провеждане на изследванията е използвано мултифункционално устройство за осигуряване на безжичен достъп и маршрутизиране на пакетите с данни: „Huawei HG530“; мобилен телефон с операционна система Андроид версия 4.2.2, а като атакуваща система е използван компютър с 2GB RAM памет и операционна система KALI LINUX. В топологията за изследване на уязвимостта е ползван всеизвестния похват „Man-in-the-Middle, MITM“. Атакувана е функцията „WPA-2 Personal“ в протокола WPA. Създаваната мрежа е контролирана и не са компрометирани лични данни. Условията за провеждане на изследването са лабораторни, като ресурсите са ограничени. Процеса на разбиване на парола изисква използването или на сравняване на хеш-стойности, произведени от пароли, подредени в речник, или чрез корелация на псевдослучайно генерирани стрингове с хеш-стойността на текущата парола за мрежата. От свободното пространство в Интернет е изтеглен речник „BIG WPA LIST“, който е в текстов формат и има размер около 16 GB. Времената за разбиване на пароли са показани в таблица 1, като особено внимание може да се наблегне на паролния стринг „ 1qaz!QAZ “, който много често бива използван като заместител на криптографски устойчива парола, но той присъства в световноизвестния речник и времето за отгатване, с определените в тази изследователска постановка ресурси, е около 5600 секунди. В доклада се посочва, че функцията „WPA-2 Enterprise“ не се поддава на така предложения похват „MiTM“, с което се повишава нивото на киберзащита. |

| | |
|---|---|
| 17 | Linko G. Nikolov, Vasil O. Slavyanov, **Network infrastructure for cybersecurity analysis**<br>За осъществяване на изследвания в областта на киберсигурността е необходимо създаването на лабораторни условия, максимално близки до реалните комуникационно-информационни инфраструктури. Този изследователски доклад има за цел да представи на широката аудитория примерен модел на реално развърната мрежова инфраструктура за извършване на коректни тестове за киберсигурност. В мрежовата топология са предвидени кабелни и безжични устройства, работещи с най-известните и най-широко разпространените операционни системи. Посочени са и най-функционалните, от гледна точка на възможности, инструменти и тестови рамки, чрез които са се посочват адекватни резултати при кибер изследванията. Демонстрирано е използването на няколко инструмента като : „nmap“, „lynis“ и рамката „OpenVas web app test“. Предложената мрежова инфраструктура е подходяща за широк набор от използвни в световен мащаб приложения, но при наличие на специфични задачи и конкретизирани услуги, е необходима допълнителна конфигурация и инсталиране на нови софтуерни инструменти, отговарящи на специфичните за даден клиент изисквания. След киберанализ в този доклад, резултатът от използването на предложените комплект инструменти и инфраструктура е посочването на политики за повишаване на киберсигурността. |
| 18 | Nikolov, L., Fetfov, O., Borisova, A., **Съображения за сигурност при писането на кодове с JavaScript**,<br>Една силно уязвима точка при използването на програмен код в широкомащабните приложения по целия свят е внедряването на функционалност чрез езика JavaScript. От една страна, това е добре за потребителите и се приветства от гледна точка на интерактивността. От друга страна обаче, в този доклад са посочени рискове за киберсигурността и скрити заплахи, породени от синтаксиса на JavaScript. В този доклад са представени някои от най-известните заплахи, като са посочени и техники за избягване на уязвимостите. В този обзорен доклад се представят възможностите за кражба на данни при атакуване на слабостите в програмния код на уеб-сайтове, HTTP заявки и сесии с бисквитки. За избягване на слабостите и намаляване на рисковете от гледна точка на киберсигурността, в този доклад са обобщени насоките при писането на кодове с JavaScript. Посочени са и специализирани инструменти-анализатори в помощ на разработчиците при програмиране с езика JavaScript: „Crawljax“, „ESLint“, „Esprima“ и „Iroh.js“. |
| 19 | Linko G. Nikolov, **Wireless network vulnerabilities estimation**<br>Този изследователски доклад доразвива предходно започнатия анализ на протокола WPA-2 по защита на безжичните мрежи. В предложената безжична топология за изследване се анализира и протокол WPS, с възможност за кражба на числовия PIN код. Представен е и литературен обзор за анализ на известни вече уязвимости в безжичните мрежи. Посочва се, че при използването на протокол WPS с PIN код, нивото на сигурност е значително занижено, а при използването на протокол „WPA-2 Enterprise“, отговорността за защита на безжичната мрежа се прехвърля към защитата на централното устройство, управляващо обмена на криптографски ключове. |
| 20 | Валентин Т. Атанасов, Линко Г. Николов, **XCPU симулатор като обучаващо приложение**<br>Публикацията представя една реализация на Уеб базирано приложение с интеграция на модел на обучавания за целите на цифрово-базиран учебен процес. Изложени са подходи за синтез на компонентни модели, предназначени за симулации на процесорна обработка, базирана на архитектурен набор от инструкции „CISC“. Представеният подход за кодиране на инструкции позволява широк кръг от кодови отрязъци, които биха допринесли за по-доброто разбиране работата на процесорното устройство от страна на обучаваните. Реализацията на приложението следва възприятията на т.н. високоинтерактивно поколение, което обстоятелство би довело до по-висока ефективност на процеса на обучение. |
| 21 | Линко Г. Николов, Валентин Т. Атанасов, **Похвати за пробиване на пароли в безжичните мрежи**<br>Тази изследователска публикация е продължение от серията изследвания за сигурността на безжичните мрежи. В нея се представят различни инструменти и съответстващите програмни команди за атакуване на пароли, защитаващи безжичните мрежи. Посочено е използване и на специализиран автоматизиран софтуер „WiFi Bruteforcer“, чрез който се проверява възможността за достъп до |

| | |
|---|---|
| | безжична мрежа от мобилен терминал. Като резултат от изследванията се заключава, че уязвима точка в безжичните мрежи е дължината на паролата и използваната семантика на символите в нея. Сложността на генерирания ключ за криптиране, при съвременните изчислителни мощности на атакуващите машини, може да се окаже слаба и този ключ да бъде отгатнат. Също така, с развитието на технологиите по защита на безжичните мрежи расте и популяризацията на инструментите, които я изследват. Цели операционни системи и софтуерни инструменти могат лесно и свободно да се набавят, което прави въпроса по защита на безжичните мрежи силно належащ. |

Съставил:

м-р гл. ас. д-р инж. Линко Николов

Short summaries
of the scientific papers and works
of major, chief assistant, engineer Linko Nikolov, PhD

| № | Title, summary |
|---|---|
| 1 | Linko Nikolov, **Cybersecurity of CIS - monograph**<br>In this monograph, structured in 4 chapters, concrete results are concentrated over security and vulnerability research of communication and information systems with network devices (routers and switches) and end devices (PCs, servers and etc.). The physical network attacks are performed in a controlled laboratory owned by National Military University. In chapter 1 "Cyberthreats for contemporary CIS", the attacks, exploitation tools and malicious activities are described, as well as instruments for cyber forensics and cyber analysis. In chapter 2 "Network processes and nodes vulnerability assessment" security test actions are performed with dictionary and brute force attacks. In chapter 3 "Application and system vulnerabilities" a review of weaknesses and operating systems' vulnerabilities and applications' security is performed. Chapter 4 "Providing CIS cybersecurity" proposes tactics, techniques, procedures and policies for developing the network devices' and end systems' cybersecurity. |
| 2 | Linko Nikolov, **Capabilities for on-time traffic division in parallel wireless nodes – part** I.<br>This publication is the first in a series of two reports on the ability to handle wireless clients. Here the mathematical theory of the probability of servicing the terminal devices from a central control device is presented. The publication is a summary of a review of existing literature sources and fundamental mathematical theories in the field of statistics. In the considered test models a circumstance for limiting the information is indicated on the current state of traffic in the various directions managed by a central unit. |
| 3 | Linko Nikolov, **Capabilities for on-time traffic division in parallel wireless nodes – part II**<br>This publication is the second in a series of two reports on the ability to handle wireless clients. Due to the expansive presentation of research models and theoretical aspects, it is necessary the results to be presented in two series. This report identifies tests for service availability or for denial of service by a central control unit on a dynamic basis. The numerical experiments, after the service tests, are presented in several tables and one composite graph containing a theoretical presentation and two presentations with limited traffic information – Bayes algorithm and JSQ (Join the shortest queue) algorithm. The results show that despite the fact that the studied system has less information than a fully studied system, the partial study does not make a significant compromise with the lifetime of requests (tasks) and customer service with wireless access. |
| 4 | Linko Nikolov, Krasimir Slavyanov, **Anonymous networks development and security aspects of future computer networks**<br>The desire to maintain security and secrecy in cyberspace spurs research on anonymous networks. Every node, working in the cyber domain, is susceptible to cyber attacks. The Internet today is an incredibly effective and uncontrolled weapon for eavesdropping and spying. Cyber attacks aimed at gaining intelligence and disrupting communication are ushering in a new era of war. This report states that secrecy and anonymity in communication and information systems are of growing importance. Six wired and eleven wireless anonymous networks are listed and interpreted. In conclusion, in a state of constant cyber warfare, anonymity can reduce vulnerability and protect one's own network and information resources by thwarting hostile information-gathering capabilities and disrupting communication. |
| 5 | Lora Raleva. Teodor Todorov, Linko Nikolov, **Security considerations for cookie sessions in Internet browsers** |

| | |
|---|---|
| | Here are the functional features of the information cookies and the potential threats and vulnerabilities they provide. Security considerations required by users and security methods in domain servers, such as technical devices, are defined. In order to overcome vulnerabilities in the security of data in cookies, the user must first be well informed about their benefits, how to properly manage them and when to use cookies. Also, when programming a website, one must take into account the parameters of cookies such as reduced state of limitations, the real need for advertising and determining the permitted domains. The user should be aware of the permission or prohibition of the sites designated by him to use cookies. Secondly, the provision of a method of protection may be mentioned. Using a cryptographically secure algorithm that provides sufficient complexity for the encryption algorithm would thwart the potential threat of an attack. Last, as a security consideration, the responsibility is led to users to store or delete unnecessary cookies like history of visits and others that could contribute to unwanted unauthorized access to data. |
| 6 | Linko Nikolov, Krasimir Slavyanov, **Effectiveness of a COMINT software**<br>A communication intelligence software may consist of several modules with different functions for radio surveillance and radiolocation. This report states that intelligence is acquired after several steps in a circular process, including planning / targeting, collecting, processing, analyzing and disseminating information, while all these steps must be foreseen by the software developers in order to achieve a full range of activities. The circular process determines the feedback, which assesses the degree of effectiveness of signal intelligence and the extent to which the requirements are met. This report identifies various functionalities of the COMINT strategic systems and the CESM tactical systems. The operational requirements for a CESM system must meet the available communication paths. However, sometimes the existing communication system needs to be replaced with a more powerful one in order to meet the increasingly stringent operational requirements for radio monitoring. The software part of such a system is defined as allowing broadband sensors, which in turn create large amounts of data, which in turn need to be remotely controlled using low-speed communication channels. |
| 7 | Linko Nikolov, **Evolution towards 4G wideband telecommunications**<br>This report analyzes the deployed cellular communication infrastructures and highlights the trend towards next generation systems. Next generation means increased capabilities in terms of data transmission capacity, number of connected mobile devices and easier management of communication channels by controllers at base stations. Figurative graphs show market trends, and Figure 2 shows the forecast development. The advantages of the newly defined form of the radio signal are indicated - orthogonal frequency multiplexing. An aspect for optimizing the load of network traffic by redistribution between reduced in space volume, but increased in number of cells and controllers (Radio Resource Control-RRC) in the face of terminal devices - mobile terminals is also considered. |
| 8 | Yulia Mateva, Linko Nikolov, **The IPv6 alternative for computer networks**<br>Internet Protocol version 6 (IPv6) is an evolution of version 4 (IPv4). IPv6 provides a lighter header processing mechanism because each packet can be a different length. Address space has been significantly increased and authentication methods have been improved. The new protocol proposes an increase in the number of bits allocated to one address - 128 bits. This predicts about $3{,}403.10^{38}$ number of addresses. In IPv4, addresses are written with 32 bits, i.e. this protocol defines $2^{32}$ unique addresses, (almost all of which are already occupied), while in IPv6 the number of unique addresses is $2^{128}$. Home appliances, cars, smartphones, e-books, tablets, laptops, wearables and other (IoT) devices are designed to use Internet connectivity. All of them will be able to work with IPv6. This report summarizes and summarizes the most important features of the IPv6 protocol. In the military sphere, the soldier of the future was represented with approximately 50 network devices in his uniform using an IP address. Due to this fact, as well as the requirement to increase the speed of data transmission over computer networks, experts in this field have proposed a new version of the network protocol. The possibility of a larger number of unique addresses can |

| | |
|---|---|
| | be mentioned as an extremely important improvement. Developers are required to be simple, more flexible and more efficient in terms of the features that the new network protocol should have. |
| 9 | Linko Nikolov, Nikolay Kulev, **A survey on the quality of digital images**<br>In this report, a literature review of image compression experiments is made, examining picture quality, spectral characteristics, and the degree of information loss. Correlation characteristics between original and compressed image, as well as standard deviation of color gamut values for two identical objects in the respective original and compressed image - MSU-BM (MSU - Blocking Measure) were used as parameters for comparative analysis (artifacts in MPEG compression); VQM (Video Quality Measure) and SSM (Structural Similarity Metric). |
| 10 | Linko Nikolov, **Data transfer encryption in CDMA2000 1xEVDO**<br>One of the few implemented standards of the CDMA2000 code division multiple access cellular system is "1XEV-DO", which is entirely packet-processed digital data. In this system, data packets are classified (encrypted) in several stages by means of protocols operating in a separate security layer of the closed network model according to the CDMA standard.The security layer with its functionalities determined by the implemented standards and protocols for network security is considered here. The hierarchy and steps in generating keys between correspondents are also indicated. The results of the analysis indicate that the protocols used are reliable and their processing does not complicate the flow of instructions. There is no unnecessary packet delay, and the latency is within acceptable limits for the user. A shortcoming in the studied classification processes is the low cryptographic stability of the keys in the presence of partial information included in the generation process. In order not to load the processors in the base stations and terminals, the encryption protocols do not generate keys with sufficient length and cryptographic properties. This is a security vulnerability in the system, but it is only detected in specialized deliberate attacks and cryptanalysis. |
| 11 | Krasimir Slavyanov, Linko Nikolov, **An algorithm for ISAR image classification procedure**<br>This paper proposes an architecture for automatic detection of objects in digital radars with reverse synthesizing aperture through software processing by a neural network algorithm. The algorithm of the studied two-layer neural network has the property of optimizing the image with high efficiency, which is proved by graphs after calculating the volume of target elements. 72 epochs have been conducted for the training of the algorithm, and for the quality of the algorithm an average square error is determined in the calculations for a volume equal to $1.10^{-1}$ . The report states that this algorithm is only suitable for the class of objects that are known in advance and for which correlation is possible. A particularly important feature in the construction of the image of the radar target is the pixel ratio. It participates in the recognition of targets, even in the conditions of strong disturbances, characteristic of the radar channel. Another result after the analysis in this report is the high speed in the calculation and image processing of the targets. This algorithm also proves to be suitable for other machine learning tasks, but accepting the same limitations of prior information and the applicability of the desired end state. |
| 12 | Linko Nikolov, Dyanko Hubenov, **BER performance for WCDMA signal in a jammed radio environment**<br>This publication presents the results of a simulation study of the reception of radio signals in a radio communication channel of the WCDMA standard in a complex radio communication environment using simulation software. The standard is 3GPP WCDMA, and the channel is downlink, with frequency division multiplexing (FDD, Release99). The simulation software has the ability to calculate the probability of digital error, as the studied objects are packet blocks, traffic channel and control channel, and the parameters are "BLER", "DTCH BER" and "DCCH BER". The results are presented in tabular form, and the graph shows the form of the transmitted and received signal. A model of a broadband jammer simulating the power of the 5W interference signal is proposed. The disadvantage is the short simulated operating time of the system due to the low computing power of the processor that processes the simulation software, but the results define |

| | |
|---|---|
| | indicative values with sufficient accuracy to determine the minimum required signal-to-noise ratio in the receiver to ensure continuity of communication services. |
| 13 | Linko Nikolov, Krasimir Slavyanov, **On the contemporary cybersecurity threats**<br>After accepting the fact that the fifth area of the battlefield will be cyberspace, cybersecurity issues have grown exponentially. This report examines cyber threat trends in terms of computer, network and cloud security. The current directions of cyber attacks, the most famous, most widely used and most common attacks, the main vulnerabilities in computer systems and networks, as well as the top 10 web risks according to global sources are listed. A specific example of vulnerability in a database system is given, as well as an example of attacks through social engineering techniques. Operational guidelines for system and network administrators are listed as security techniques. |
| 14 | Linko Nikolov, **The role of the European Union in ensuring cybersecurity**<br>This review report examines the guidelines discussed by the European Commission and the European Network and Information Security Agency on building a unified systematic approach to tackling cybersecurity. It is stated that the Republic of Bulgaria, with its newly created strategic documents, namely the Cyber Security Act and the National Cyber Security Strategy, presents to the European community readiness to respect the values and principles of quality and effective control of cyber incidents. The authorities and competent bodies in the Republic of Bulgaria, as a full member of the European Union, have an idea to create a National Coordination and Organizational Network for Cyber Security NCOMCS on the model of public-private partnerships, which will integrate single European directives and documents. network and information security. As a result of this review report, it can be concluded that the ongoing training of staff working in cyberspace should become a mandatory element. Specialized research and application centers with unique competencies and technological bases for simulations, training, testing and active protection of IT systems, industrial management systems and critical infrastructures must be established. hrough the newly established coordination centers, following a single framework for certification and achieving a secure common electronic market in the European Union, including Bulgaria, will adequately address today's challenges to cybersecurity. |
| 15 | Linko Nikolov, **Definition, role, place and tasks of cyber defense over national security and ministry of defense**<br>This review report outlines the basic principles and methods for ensuring cybersecurity. Indicative concepts for the Cybersecurity area are also defined, indicating the nature, role, place and tasks performed in the process of ensuring the protection of electronic information in computer systems and networks. Achieving a desired state of cyber resilience is associated with a comprehensive rethinking of security issues, the formation of adequate to modern realities concepts and the implementation of a system of interrelated practical actions leading to building a qualitatively "new architecture" of the national security system. The main goal in this rethinking is the perception and affirmation of the formulated thesis that the "basis" and "building structure" of the "new architecture" of security in the communication society is cybersecurity, considered in all its dimensions - technological-informational, legal-institutional and political. The cyber security architecture will reflect the current state of needs, and there will be an opportunity to move to a new, more perfect and more relevant to the system's goals. Cyber security must cover the full range of vulnerabilities and critical points. The information, regardless of the medium on which it is stored and the type of its presentation in the transmission medium (data sets, voice, video, telephony, etc.), will be reliably protected. However, the senior, chief responsible for the implementation of all these cyber security activities has not yet been specified. In the political aspect, the Republic of Bulgaria must introduce a single leadership and a unified approach to cybersecurity management, which at the time of writing this report is lacking. |
| 16 | Linko Nikolov, **Vulnerability analysis of a wireless computer network protected by the WPA2 cryptographic protocol** |

| | |
|---|---|
| | In a CIS system, a potential port of attack is the wireless network access point. Despite its protection with a string password, by the method of guessing with full combination it is possible for a malicious person to gain unauthorized access. This research report presents the times for cracking multiple password models using full-combination attack tools and dictionary-based string password attacks. A multifunctional device for providing wireless access and routing of data packets was used to conduct the research: "Huawei HG530"; mobile phone with Android operating system version 4.2.2, and a computer with 2GB of RAM and KALI LINUX operating system was used as an attack system. The well-known "Man-in-the-Middle, MITM" technique was used in the vulnerability research topology. The WPA-2 Personal feature in the WPA protocol has been attacked. The created network is controlled and personal data are not compromised. The conditions for conducting the research are laboratory and the resources are limited. The password cracking process requires the use of either comparing hash values derived from passwords arranged in a dictionary or by correlating pseudo-randomly generated strings with the hash value of the current network password. The "BIG WPA LIST" dictionary, which is in text format and has a size of about 16 GB, has been downloaded from the free space on the Internet. Password cracking times are shown in Table 1, with particular emphasis on the password string "1qaz! QAZ", which is often used as a substitute for a cryptographically strong password, but it is present in the world-famous dictionary and guessing time, with the resources identified in this research setup, is about 5600 seconds. The report states that the "WPA-2 Enterprise" feature does not lend itself to the proposed "MiTM" technique, which increases the level of cybersecurity. |
| 17 | Linko G. Nikolov, Vasil O. Slavyanov, **Network infrastructure for cybersecurity analysis**<br>In order to carry out research in the field of cybersecurity, it is necessary to create laboratory conditions as close as possible to the real communication and information infrastructures. This research report aims to present to the general public an exemplary model of a truly deployed network infrastructure to perform accurate cybersecurity tests. The network topology includes wired and wireless devices that work with the most well-known and widespread operating systems. The most functional, in terms of capabilities, tools and test frameworks are indicated, through which adequate results in cyber research are indicated. The use of several tools has been demonstrated, such as nmap, lynis and the OpenVas web app test framework. The proposed network infrastructure is suitable for a wide range of applications used worldwide, but in the presence of specific tasks and specific services, additional configuration and installation of new software tools is needed to meet customer-specific requirements. Following the cyber analysis in this report, the result of using the proposed set of tools and infrastructure is the identification of policies to increase cybersecurity. |
| 18 | Nikolov, L., Fetfov, O., Borisova, A., **Security concerns in JavaScript coding**<br>One very vulnerable point in the use of program code in large-scale applications around the world is the implementation of functionality through the JavaScript language. On the one hand, it is good for users and is welcomed in terms of interactivity. On the other hand, this report identifies cybersecurity risks and hidden threats posed by JavaScript syntax. This report presents some of the most well-known threats, as well as techniques for avoiding vulnerabilities. This overview report presents the possibilities for data theft when attacking vulnerabilities in the program code of websites, HTTP requests and cookie sessions. To avoid vulnerabilities and reduce cybersecurity risks, this report summarizes guidelines for writing JavaScript code. There are also specialized analytics tools to help developers with JavaScript programming: "Crawljax", "ESLint", "Esprima" and "Iroh.js". |
| 19 | Linko G. Nikolov, **Wireless network vulnerabilities estimation**<br>This research report builds on the previously launched analysis of the WPA-2 protocol for the protection of wireless networks. The proposed wireless topology for research also analyzes the WPS protocol, with the possibility of stealing the numeric PIN code. A literature review for the analysis of already known vulnerabilities in wireless networks is also presented. It is stated that when using WPS with PIN, the level of security is significantly reduced, and when using WPA-2 Enterprise, the responsibility for protecting the |

| | |
|---|---|
| | wireless network is transferred to the protection of the central device that controls the exchange of cryptographic keys. |
| 20 | Valentin T. Atanasov, Linko G. Nikolov, **XCPU simulator as a learning application**<br>This publication presents an implementation of a Web-based application with the integration of a learner model for the purposes of a digital-based learning process. Approaches to the synthesis of component models designed for simulations of CPU processing based on the CISC. The presented approach for instruction coding allows a wide range of code snippets that would contribute to a better understanding of the operation of the processor device by the trainees. The implementation of the application follows the perceptions of the so-called highly interactive generation, which circumstance would lead to higher efficiency of the learning process. |
| 21 | Linko G. Nikolov, Valentin T. Atanasov, **Techniques for password cracking in wireless networks**<br>This research publication is a continuation of a series of studies on wireless network security. It presents various tools and the corresponding program commands for attacking passwords that protect wireless networks. The use of specialized automated software "WiFi Bruteforcer" is also mentioned, which checks the possibility of access to a wireless network from a mobile terminal. As a result of research, it is concluded that a vulnerable point in wireless networks is the length of the password and the semantics of the symbols used in it. The complexity of the generated encryption key, with the modern computing power of attacking machines, may be weak and this key can be guessed. Also, with the development of wireless network protection technologies, the popularity of the tools that study it is growing. Entire operating systems and software tools are easily and freely available, making the issue of wireless security very pressing. |