Р Е З Ю М Е

НА НАУЧНИТЕ ТРУДОВЕ

на д-р Ангел Генчев

Научните трудове са в областта на автоматизираните системи за управление, методите за обработка на информацията, изкуствения интелект, съвременните информационни системи и технологии, моделиране и подпомагане вземането на решения, системите за групова работа, киберсигурност, цифрови комуникации и др. Разработките включват внедрени информационни задачи, комплекси, подсистеми и системи за нуждите на отбраната в областта на оперативно-бойното осигуряване, комуникационно-информационна поддръжка, системи за подпомагане вземането на решения, системи за автоматизация на управлението на войските, системи за моделиране и др. Научно-изследователските проекти са свързани с проектиране на информационни и комуникационни системи за нуждите на ръководния състав на Министерство на отбраната и Българската армия и подчинените им структури, както и надведомствени проекти по подпомагане управлението на страната при кризи, природни бедствия и др.

Научните трудове са представени в три категории:

I. Монографични трудове

II. Научни статии и доклади

III. Научно-изследователска и развойна дейност

I. МОНОГРАФИЧНИ ТРУДОВЕ

1.1 Р. Илиев, А. Генчев **СЪВРЕМЕННИ ЦЕНТРОВЕ ЗА ДАННИ (ИЗИСКВАНИЯ, ТЕХНОЛОГИИ, ИЗГРАЖДАНЕ).** Монография, Издание на Институт по отбрана „Професор Цветан Лазаров”, ISBN 978-619-90024-3-8, София, 2021 г., 273 стр. (рецензенти: проф. д.т.н. Веселин Целков – Университет по библиотекознание и информационни технологии и полк. доц. д-р инж. Марио Ангелов – Институт по отбрана)

Монографията разглежда съвременните центрове за данни – невидимата за потребителите на информационни и комуникационни услуги съвкупност

от инфраструктура, технологии, системи, софтуер и компютърни устройства. В книгата е направен преглед на историческото развитие и етапите през които преминават центровете за данни, още от възникването на електронни изчислителни машини, като е обърнато внимание и на първите изчислителни центрове в България (известни под това име до 90-те години на XX век). Анализирани са развитието и основните типове съвременни центрове за данни, общите им архитектурни особености, както и последователността на изграждането им. Направени са оценка и изводи от изследването на най-използваните технологични платформи за изграждане на центрове за данни, предлагани от Vmware и Microsoft, както и на много Linux-базирани решения, като Red Hat Virtualization, Xen Cloud platform, Proxmox virtual environment и др. Предложени са основни критерии за избор на софтуерна платформа за виртуализация, като цена за притежание, необходим брой виртуални машини, поддържани операционни системи, системи за осигуряване на висока достъпност до услугите и ресурсите, оценка на степента на натоварвания и други.

В монографията са представени основните стандарти и добри практики за изграждане на центрове за данни, на изискванията и препоръките на американската Асоциацията на телекомуникационната индустрия (TIA) и нейния стандарт ANSI/TIA-942, насочен към телекомуникационната инфраструктура на центровете за данни.

Представени са някои иновативни решения на компании от областта за създаване на различни типове центрове за данни – модулни, мобилни, екологични, като е обърнато внимание и на бързото разрастване и изграждане на нови центрове за данни не само на сушата, но и под водата (експериментален център за данни на Майкрософт), особено след разрастването на епидемиологичната обстановка през 2020 – 2021 г., когато отдалечената комуникация, учене и работа от вкъщи беше масово практикувана.

Съществена част от монографията е отделена на създаването на концептуален модел за изграждане на система от центрове за данни за нуждите на сигурността и отбраната, с включени голям брой оперативни, функционални, технически, технологични, информационни, организационни и др. изисквания към нея.

Описаният модел, изискванията и технологията на работа по реализацията на системата от центрове за данни са в резултат от изследвания и експерименти на авторите с популярни софтуерни платформи за виртуализация, както и на опита с различни хардуерни устройства за конфигуриране на системата, добит благодарение на изградения от тях работещ прототип на облачен център за данни в Института по отбрана.

II. НАУЧНИ СТАТИИ И ДОКЛАДИ

II.2.1 Н. Стоянов, А. Генчев, Р. Илиев **НЯКОИ АСПЕКТИ ПРИ АНАЛИЗА НА РИСКА В ИНФОРМАЦИОННИ СИСТЕМИ ЗА СИГУРНОСТ И ОТБРАНА**. Научна конференция на Шуменски университет „Епископ Константин Преславски", Сборник трудове, 2009 г., стр. 200-209

В доклада са представени някои аспекти от анализа на риска в информационните системи. Разгледани са дефиниции, източници и други параметри, които влияят върху риска на системите C4I. Резултатите от това изследване са използвани в изграждани комуникационни системи за Българската армия.

II.2.2**.** Р.Илиев, Н. Стоянов, А. Генчев. **Един архитектурен подход при създаване на информационна среда за съвместна работа**, Научна конференция на Шуменски университет „Епископ Константин Преславски", Сборник трудове, стр. 214-221, 2009 г.

В доклада е предложен един подход за създаване на информационна среда за съвместна работа, основан на прилагането на три типа архитектурни изгледи – функционален (оперативен), системен и технически. Предложен е вариант за създаване на такава среда за съвместна работа на длъжностни лица в една организация (тестван успешно в структури от Министерство на отбраната) чрез приложение на съвременни информационни технологии и технически решения.

II.2.3. А.Генчев, Р.Илиев, Н. Стоянов**. Изследване на възможността за приложение на бездискови работни станции в информационните системи на Българската армия**, Научна конференция на Шуменски университет „Епископ Константин Преславски", Сборник трудове, стр. 210-213, 2009 г.

В доклада са представени резултати от изследване, основано на използването на информационна мрежа от бездискови работни станции за обмен на класифицирана информация, в която са интегрирани съвременни методи, средства и системи за информационна защита. Представени са изследваните технологични решения за създаване на такава мрежа и са направени изводи за тези от тях, които позволяват съществено да се подобри сигурността на ин-

формацията, обработвана в информационните системи на Българската армия при спазване на заложените в закона и разпоредбите към него изисквания.

II.2.4. Генчев А., **Перспективни технологии и решения за интелигентна отбрана**. Научна конференция с между-народно участие„MT&S-2011”, ISBN 978-619-90024-1-4, София, 2012, Сборник доклади, 101 - 105 стр.

В доклада е извършен анализ на инициативата за интелигентна отбрана (Smart Defence) на секретаря на НАТО, представена в речта му на Мюнхенската конференция за сигурност и отбрана (04.02.2011 г.). От нея са извлечени концепциите и са адаптирани към съвременните ИТ технологии. Предложени са примери за решения, реализиращи тези концепции.

II.2.5. Генчев А., **Анализ на системи за виртуализация при изграждане на облачни архитектури**. Научна конференция с международно участие „MT&S-2013”, ISSN 2367-5942, София, 2014, Сборник доклади, II-25 - II-40

Докладът отразява резултатите от проучване, извършено в хода на работата по системен проект „Развитие и модернизация на Интегрираната информационна инфраструктура на БА“. Разгледани са възможностите и ограниченията на съвременните системи за управление на виртуализация и облачна инфраструктура от водещи производители и такива с отворен изходен код с оглед резултатите да бъдат използвани при избор на подходяща платформа за нуждите на проекта.

II.2.6. Генчев А., **Оптимизиране на използването на хардуерни ресурси**. Списание „ЦИО“ брой от 2015 г – Юли.

В доклада в много сбита форма са представени резултатите от извършено проучване, експериментиране и разработка на системи, позволяващи съвместното използване на една компютърна система от няколко потребителя. Разработената система разчита на виртуализация за да създаде пълна илюзия за собствен хардуер на всеки от потребителите, като при това осигурява защита на неговата информация от останалите потребители и защита на решението за виртуализация от достъп с администраторски права. Реализира икономия на компютърен хардуер и на RAM памет посредством имплементация на подсистемата за KSM (kernel same page merging), съществуваща

от известно време в ядрото на ОС Linux. Реализацията е успешно експериментирана в две конфигурации в дирекция „Административно и информационно осигуряване“ в МО-1, като е предоставен дистрибутивен носител (DVD) за администратора на системата.

II.2.7. Колев А, Генчев А. **Институтът по отбрана приложи хибриден модел на ИС във виртуална среда**. Списание „ЦИО“ брой от 2018 г – Юли.

В доклада са изследвани проблеми, свързани с присъщи ограничения при съхранението на големи обеми от данни. Предложен е усъвършенстван, наречен от авторите „хибриден“ модел на организация на подсистемата за съхранение на данни. Докладът демонстрира идеята за съвместяване на използването на виртуализация на част от ресурсите на компютърната система – там, където от това има желан ефект (като изолация на отделните приложения) със използване на не виртуализирани ресурси като дискова памет. Идеята е реализирана и практически - като информационна система – електронна библиотека за нуждите на ИО.

II.2.8. Илиев, Р., А. Генчев. **ИЗГРАЖДАНЕ НА СИСТЕМА ОТ ЦЕНТРОВЕ ЗА ДАННИ ЗА НУЖДИТЕ НА ОТБРАНАТА.** Международна научна конференция „Хемус 2018”, Сборник доклади, II-189 - II-195, Пловдив, 2018 г.

В доклада са разгледани някои съвременни решения за изграждане на центрове за данни и са анализирани различни критерии за избор на платформи за виртуализация и създаване на облачни среди с насоченост към използването им за нуждите на отбраната. Представени са възможностите за изграждане на система от центрове за данни за нуждите на отбраната, както и някои специфични изисквания на които те трябва да отговарят.

II.2.9. Генчев А., Р. Илиев. **ПРИДОБИВАНЕ НА СЕНЗОРНА ИНФОРМАЦИЯ ОТ БЕЗПИЛОТНИ ЛЕТАТЕЛНИ СРЕДСТВА ПРИ ОЦЕН-**

КА НА КРИЗИСНА ОБСТАНОВКА. Международна научна конференция „Хемус 2018”, Сборник доклади, II-153 - II-162, Пловдив, 2018 г.

В доклада са разгледани срещаните проблеми при събиране на сензорна информация от безпилотни летателни средства в условията на кризисна обстановка и са предложени способи за тяхното преодоляване.

II.2.10. Генчев, А., Р. Илиев. **ЗАЩИТА НА ИНФОРМАЦИЯТА И КИБЕРСИГУРНОСТ НА КОРПОРАТИВНИТЕ ИНФОРМАЦИОННИ СИСТЕМИ**. Международна научна конференция „Хемус 2018”, Сборник доклади, II-163 - II-173, Пловдив, 2018 г.

В доклада е извършен обзор на възможни съвременни кибератаки, на методи и средства за защита от тях, приложими към корпоративните информационни системи. Предложени са схеми на защита на корпоративни системи от различни типове въздействия чрез прилагане на съществуващи софтуерни продукти.

II.2.11. Генчев А. **Сензори и сензорни технологии използвани при безпилотни летателни средства**. . Международна научна конференция „Хемус 2018”, Сборник доклади, , II-174 - II-188, Пловдив, 2018 г.

Докладът отразява част/поредна стъпка от работата по проучване и разработка на система за придобиване и визуализация на сензорна информация по програми 7.1, 7.2 и 1.7.7 на МО. Разглежда типовете сензори, използвани при безпилотните летателни средства, поставят се изискванията към тях и към техните комуникационни интерфейси с оглед построяване на система за събиране и предаване на данни в реално време от мястото на кризисно събитие.

II.2.12. П. Николова, Генчев, А. **Анализ и визуализация при вероятни кибератаки**. 2018, Международна научна конференция „Хемус 2018”, Сборник доклади, II-107 - II-114, Пловдив, 2018 г.

Докладът съдържа анализ на средства за установяване и предотвратяване на кибератаки. На база на този анализ е предложен релационен модел за система за управление на бази от данни за съхранение на информацията за възникналите кибератаки срещу специално приготвен сензор - honeypot. Разгледани са способите за гео-реферирane на източниците на кибератаките и на тази база е предложено решение за визуализирането им върху електронна географска карта.

II.2.13. Iliev, R., A. Genchev. **POSSIBILITIES FOR USING UNMANNED AERIAL VEHICLES TO OBTAIN SENSORY INFORMATION FOR ENVIRONMENTAL ANALYSIS**. Information & Security: An International Journal 46, no. 2 (2020): 127-140, https://doi.org/10.11610/isij.4609

Тази статия представя някои възможности за добиване на сензорни данни от околната среда (като метеорологични данни, ниво на замърсяване, инфрачервено излъчване и др.), с използване на безпилотни летателни апарати (БЛА). Обръща се внимание на специфични изисквания към БЛА, използвани като летящи платформи за събиране на сензорни данни. Анализира се процесът на създаване на прототип на система за събиране и предаване на данни в реално време от мястото на кризисно събитие с използване на БЛА. Предлага се да се използва специализирана невронна мрежа, настроена за идентифициране на наполовина скрити (полузатрупани от бедствие) хора, когато се анализират изображения, получени от сензори на БЛА, прелитащи над мястото на кризисното събитие.

II.2.14. Genchev, A., R. Iliev. **USING UNMANNED AERIAL VEHICLES FOR COLLECTION AND TRANSMISSION OF DATA IN REAL TIME FROM THE PLACE OF CRISIS EVENT**. SPRINGER 2021 Communications in Computer and Information Science (series), ISSN: 1865-0929, 2020 (под печат)

Докладът анализира възможностите за използване на безпилотни летателни апарати (БЛА) за получаване на сензорни данни от мястото на кри-

зисно събитие чрез оценка на техните полетни, комуникационни и сензорни възможности. Предложен е подход за използване на БЛА за превенция и помощ на спасителните екипи при оценка на кризисната ситуация чрез оборудване на такъв апарат с подходяща система от сензори, комуникации, средства за първична обработка на данни и др. Докладът предлага да се използва специализирана невронна мрежа, която да се приложи за идентифициране на полускрити (полузатрупани от бедствие) хора след анализ на техни изображения, като представя и някои от получените резултати.

II.2.15. Генчев А. **Изграждане на бюджетно-ориентирани решения за IP телефония, предназначени за военните формирования на БА.** Международна научна конфе-ренция „Хемус-2020“, Сборник доклади, II-165 - II-172, Пловдив, 2020 г.

В доклада се представят резултатите от разработката на прототип на полева цифрова IP централа, базирана на софтуерни решения с отворен изходен код. Дадена е блокова схема на взаимодействието на софтуерните компоненти и примерна схема на свързване на инстанции (екземпляри) от централата в една по-голяма мрежа за IP-телефония. Извършено е проучване на възможността за привързване на IP централата към съществуваща ISDN инфраструктура чрез изграждане на мост към ISDN-E1 линия както посредством допълнителен компонент, така и чрез вграждане на E1 интерфейсен модул в хардуера на централата.

II.2.16. Iliev, R., A. Genchev. **GENERALIZED NET MODEL OF THE DECISION MAKING PROCESS IN THE CRISIS MANAGEMENT.** Journal 'Advanced Studies in Contemporary Mathematics', South Korea, 335/839(39.9%) in the category of mathematics (The 2011 SJR in SCOPUS for Advanced Studies in Contemporary Mathematics is 0.043 with a ranking) (for print)

Статията представя непубликуван досега модел на процеса на вземане на решения при управление на кризи с помощта на обобщена мрежа, реализирана с пет прехода. За оценка на осъществимостта на решението, при последния преход се взема предвид фактът, че не всички генерирани решения за управление на кризи могат да бъдат успешно приложени. При оценка на пара-

метрите на отделните ядра е предвидена възможността да се използват размити и интуиционистки размити стойности за по-точно моделиране на процеса и по-ясно представяне на чисто човешкият начин на изразяване.

II.2.17. A. Genchev. **A CONCEPTUAL MODEL FOR WEB PAGE MONITORING SOLUTION**. 2021, International Conference on Advanced Research and Technology for Defence (ARTDef).
В борбата с киберпретъпленията и конкретно обезобразяването на WEB страници се налага да се осъществява наблюдение и своевременно известяване. Докладът представя анализ на проблема и подходи за решаването му с използване на средства с отворен изходен код. Предложеният подход включва употребата на ядро на WEB browser за осигуряване на правилното възпроизвеждане на съдържанието на WEB страниците, които разчитат на AJAX и Javascript за да се визуализират.

II.2.18. A. Genchev. **Визуализация на сензорна информация, получена от безпилотни летателни системи в център за управление на кризи**. 2021, International Conference on Advanced Research and Technology for Defence (ARTDef).

Докладът отразява пореден етап от серия разработки, започнала със проучване, избор на подходяща летателна платформа, анализ на необходимите сензори и решения за определяне на местоположението в 3-D пространството. Разгледани са решенията за визуализация, използвани в центъра за управление, което включва изграждане на видеостена и софтуерно WEB приложение за визуализация на 3-D модел на местността и данните от сензорите.

II.2.19. Генчев А. **Адаптивен алгоритъм за динамично разпределение на честотните ресурси, приложим в клетъчни комуникационни мрежи със**

специално предназначение. International Conference on Advanced Research and Technology for Defence (ARTDef).

В хода на изследвания върху адаптивните алгоритми за динамично разпределение на честоти за повторно използване в клетъчните радиомрежи, е установено, че има необходимост от създаване на адаптивен спрямо преднамерени смущения и едновременно с това, децентрализиран алгоритъм. Освен това е необходимо алгоритъма да продължава да функционира при загуба на част от съседните клетки или на комуникацията с тях. Настоящия доклад представя едно предложение за подобен алгоритъм.

II.2.20. Vasilis Katos, Angel Genchev, Maya Bozhilova and Nikolai Stoianov, **Cybersecurity user requirements analysis: the ECHO approach.** 2021, "Lecture Notes in Networks and Systems" (ISSN: 2367-3389) Vol. 344 (MODS-2021 June 28-July 1, 2021)

Докладът представя структуриран подход за идентифициране на знанията за киберсигурността и извличане на нуждите на потребителите въз основа на разработването на специфични случаи на употреба. Дадени са примерни описания на случаи на използване (use cases) на атаките в обща компютърна мрежа. Предложените случаи на употреба са анализирани в платформата CAIRIS. Процесът на моделиране потвърждава, че CAIRIS е мощен инструмент за обогатяване на контекста на моделите на заплахи и UML клас диаграми. Също, моделирането с CAIRIS може да поддържа използването на принципи за сигурност по дизайн. Изследването се провежда в рамките на дейностите на проект „Европейска мрежа от центрове за киберсигурност и център за компетенции за иновации и операции“ (ECHO).

II.2.21. A. Genchev, M. Bozhilova, N. Stoianov. **Multi-sector cyber security analysis methodology – the ECHO approach**. 2021, DIGILIENCE 2021

Докладът представя структурирана методология за идентифициране на секторните знания за киберсигурността, анализиране на нуждите на потребителите и извеждане на специфични за сектора случаи на употреба, създадена за решаване на задача 2.5 от проект ECHO. Даден е пример в областта

на отбраната за прилагане на предложената методология, както и подход за проверка. Изследването е проведено в рамките на проект „Европейска мрежа от центрове за киберсигурност и център за компетенции за иновации и операции" (ECHO).

III. НАУЧНО-ИЗСЛЕДОВАТЕЛСКА И РАЗВОЙНА ДЕЙНОСТ

А. Приложни разработки

3.1. Информационна система за командване и управление

Автоматизираната информационна система за командване и управление е с надведомствен обхват и е предназначена за подпомагане управлението при кризи от различен характер. Включва няколко подсистеми и осигурява над 60 информационно-комуникационни услуги, базирани в четири основни компютърни мрежи. Разработена от Р. Илиев (ръководител), Н. Стоянов, А. Генчев, Х. Радев, Д. Желязков, Н. Лазарова, А. Цолова. Внедрена научно-изследователска и приложна разработка, приета в БА през 2008 г.

Б. Проекти, описания на системи, ръководства

3.2. Информационна система. Информационно оборудване на оперативни помещения

Документът е технически проект за оборудване на помещения за работа на оперативен състав със съвременни информационно-технически и програмни средства за работа. Включена е и техническа спецификация. Проектът е разработен на основата на проведени научни изследвания и експерименти от областта на АСУ и приложение на съвременни IT-технологии и решения, от колектив в състав: Р. Илиев (ръководител), Н. Стоянов, А. Генчев, Х. Радев, АГК, 2009 г.

3.3. Информационна мрежа „АИМ-АГК”

Технически проект за изграждане на автоматизирана информационна мрежа на АГК за работа на длъжностни лица, предоставяща широк спектър от информационни и комуникационни услуги (съвместна работа с ел. документи, ел. календар и времеви график, средства за планиране на дейности, IP-видео телефония, ел. поща и др.). В проекта е включена и техническа спецификация. Проектът е разработен на основата на проведени научни изследвания и експерименти по приложението на съвременни IT-технологии и решения от: Р. Илиев, Н. Стоянов и А. Генчев, АГК, 2008 г.

3.4. АИС на БА. Информационно-комуникационна среда за съвместна работа и подпомагане на управленския процес

Документът е работен проект за развитие на Автоматизираната информационна система на БА. Проектът е разработен с цел развитие на АИС на БА и осигуряване на длъжностните лица от МО и БА със съвременни информационни и комуникационни услуги за подпомагане на управленския процес и във връзка с интегрирането на системи, разработени от външни за МО разработчици. Той е приложение на съвременни информационни и комуникационни технологии, изследвани, анализирани и експериментирани от колектива, разработчик на проекта. Описва изграждане на информационно-комуникационна среда са съвместна работа на длъжностните лица, която включва следните по-важни подсистеми: подсистема за групова работа; комуникации и видеоконференции; географска информационна подсистема; подпомагане управлението при извънредни ситуации; подпомагане вземането на решения; подсистема за съобщения и оповестяване. Проектът е разработен през 2011 г. от Р. Илиев в основната си част (както е отбелязано в увода), а отделни точки са дело и на: И. Христозов, Н. Стоянов, А. Генчев, А. Борисов, Г. Георгиев, К. Андреев, А. Атанасов, Д. Караколев. Проектът е приет на Съвет по въоръжения за изпълнение.

3.5. Развитие и модернизация на Интегрираната информационна инфраструктура на Министерството на отбраната (МО)

Документът е системен проект за развитие и модернизация на Интегрираната информационна инфраструктура на МО чрез внедряване на съвременни информационни и комуникационни технологии и решения за изграждане на сървърни архитектури. Проектът е приложение на проведени редица изследвания и анализи на съвременните достижения на IT-технологиите и тяхното приложение в практиката. Проектът е разработен през 2011 г. от Н. Стоянов (ръководител), Р. Илиев, И. Иванов, С. Стойков, А. Генчев, М. Божилова, А. Колев. Проектът е приет на Съвет по въоръжения за изпълнение.

3.6. Развитие и модернизация на Интегрираната информационна инфраструктура на българската армия (БА)

Документът е системен проект за развитие и модернизация на Интегрираната информационна инфраструктура на БА чрез внедряване на съвременни информационни и комуникационни технологии и решения за изграждане на сървърни архитектури. Проектът е приложение на проведени редица изследвания и анализи на съвременните достижения на IT-технологиите и тяхното

приложение в практиката. Проектът е разработен през 2011 г. от Н. Стоянов (ръководител), Р. Илиев, И. Иванов, С. Стойков, А. Генчев, М. Божилова, А. Колев. Проектът е приет на Съвет по въоръжения за изпълнение.

3.7. Център за научни изследвания и развитие на ИКИС и системите С4I. Лаборатория „Кибератаки и информационна сигурност"

С проекта се цели да се осигури научно съпровождане, изграждане, изпитване и развитие на информационните и комуникационни системи и системите С4I за нуждите на отбраната и сигурността на страната. Той е предназначен за осигуряване на научно-изследователска и лабораторна база за анализ, изследване, обучение и прилагане на кибератаки, както и за повишаване на сигурността на комуникационно-информационните системи и мрежи за нуждите на ИКИС и системите С4I, в съответствие с приоритетните инвестиционни проекти от Дългосрочния инвестиционен План-програма на МО. Проектът е реализиран на основата на изследване и анализ на перпективните IT-технологии в световен мащаб, които да се експериментират и на тяхна основа да се правят бъдещи разработки за нуждите на МО и БА. Проектът е разработен през 2011 г. от Н. Стоянов (ръководител), И. Иванов, Р. Илиев, А. Генчев, М. Божилова.

3.8. Център за научни изследвания и развитие на ИКИС и системите С4I. Лаборатория „Учебно-тренировъчен полигон по КИС, защита на информацията и системи за командване и управление"

С проекта се цели да се осигури научно съпровождане, изграждане, изпитване и развитие на информационните и комуникационни системи и системите С4I за нуждите на отбраната и сигурността на страната. Той е предназначен за осигуряване на научно-изследователска база за обучение и провеждане на тренировки по КИС, системите за защита на информацията и С2-системите от състава на ИКИС и от състава на С4I-системите в приоритетните инвестиционни проекти от Дългосрочния инвестиционен План-програма на МО. Проектът е реализиран на основата на изследване и анализ на перпективните IT-технологии в световен мащаб, които да се експериментират и на тяхна основа да се правят бъдещи разработки за нуждите на МО и БА. Проектът е разработен през 2011 г. от И. Иванов (ръководител), Н. Стоянов, Р. Илиев, А. Генчев, А. Колев.

3.9. Възможности за използване на офис-пакети с отворен код в Българската армия

С изследването се цели да се проучат и тестват различни софтуерни офис-продукти (с безплатни лицензи), които да се използват в Българската армия. Документът включва: идентификация на софтуерните пакети с лиценз freeware, които да бъдат алтернативи на комерсиалните офис-пакети; анализ на съвместимостта с Microsoft Office по отношение на потребителския интерфейс и по отношение на файловите формати; анализ на общата функционалност на приложенията; тестване за стабилност; проучване на начините, по които се поддържа и перспективите за развитие на всеки от продуктите; анализ на опита на страните от ЕС и предложения за бъдещи изследвания.

Проучването е извършено от работен колектив в състав: А. Генчев, Р. Илиев, М. Божилова.

В. УЧЕБНО-МЕТОДИЧЕСКИ ТРУДОВЕ (ТИД, ТТЗ, програми, методики и др.)

В този раздел са включени учебно-методически трудове, свързани с участие на автора при разработване на технико-икономически доклади, тактико-технически задания, програми и методики за изпитване и приемане на автоматизирани информационни задачи, комплекси, подсистеми и системи, както и на други изходни документи, необходими за придобиване на компютърни продукти за нуждите на Министерство на отбраната, Българската армия и подчинените им структури. Общо 23 документа, разработвани през периода: 1990 – 2020 г.

През 2013 г. е разработен технико-икономически доклад за развитие на корпоративната информационна система за отбрана (387 стр.), с включено обстойно изследване на съществуващи системи, технологии, решения и световни тенденции в изграждането на такива системи и модернизирането им върху облачна инфраструктура.

Документът е разработен от: Г. Велев (ръководител), Р. Илиев, А. Генчев, Н. Стоянов, М. Ангелов, И. Иванов, И. Христозов, Й. Йорданов, Г. Грънчаров.

През 2014 г. беше изготвено тактико-техническо задание (121 стр.) за изграждане на системата (от Г. Велев, А. Генчев и Р. Илиев), базирано на прилагане на съвременни облачни технологии и информационни среди за съвместна работа (прието от Съвета по въоръженията).