

ИНФОРМАЦИОННА СИГУРНОСТ В СЪВРЕМЕННИТЕ ОРГАНИЗАЦИИ: ЗАПЛАХИ, УЯЗВИМОСТИ И МЕХАНИЗМИ ЗА ЗАЩИТА

Сергей Модев, Николай Атанасов,
Мирослав Шалев, Бойко Велков

Университет по библиотекознание и информационни технологии

Резюме: В условията на ускорена цифрова трансформация информационната сигурност се утвърждава като стратегически фактор за устойчивото функциониране на съвременните организации. Интензивното използване на информационни и комуникационни технологии създава нови възможности за развитие, но едновременно с това поражда значителни рискове, свързани с кибератаки, изтичане на данни и компрометиране на организационни ресурси. Целта на изследването е да анализира концептуалните основи на информационната сигурност, да систематизира основните заплахи и уязвимости в цифровата среда и да представи ефективни организационни, технически и нормативни механизми за защита, като е приложена методология, основана на сравнителен анализ, системен подход и анализ на документи. Основните изводи показват, че ефективната информационна сигурност не може да бъде постигната чрез изолирани технически решения, а изисква интегриран, многослоен подход, в който централна роля играе човешкият фактор. Резултатите имат приложим характер за ръководители, специалисти по информационна сигурност и разработчици на политики.

Ключови думи: информационна сигурност; киберсигурност; управление на риска; информационни системи; цифрова трансформация

ВЪВЕДЕНИЕ

Дигиталната трансформация е сред най-значимите процеси, определящи развитието на съвременното общество. Информационните и комуникационните технологии проникват във всички сфери на обществения и икономическия живот, като информацията се превръща в стратегически ресурс, чиято защита е пряко свързана с ефективността, конкурентоспособността и устойчивостта на организациите (Whitman, Mattord, 2022; Andress, 2020). развитието на облачните технологии, мобилните комуникации, интернет на нещата и изкуствения интелект значително разширява повърхността за атака и увеличава сложността на средата за сигурност, а киберпрестъпността се превръща в глобален проблем, засягащ държавните институции, бизнеса и гражданите (World Economic Forum, 2024; ENISA, 2024).

В този контекст информационната сигурност следва да се разглежда не само като технологичен въпрос, а като комплексна управленска дейност, включваща политики, процедури, технически решения, правни механизми и организационна култура. Съществуващата литература предлага солидна теоретична база по отделни аспекти на сигурността (Whitman, Mattord, 2022; Stallings,

Brown, 2018; Pfleeger, Pfleeger, 2015; Andress, 2020; Von Solms, Van Niekerk, 2013; Cherdantseva, Hilton, 2013; Alberts, Dorofee, 2003), допълнена от актуални институционални доклади (ENISA, 2024; World Economic Forum, 2024; SANS Institute, 2023), но голяма част от публикациите разглеждат технологичните, организационните, човешките и нормативните измерения поотделно, без интегрирана рамка – именно тази празнина определя приноса на настоящото изследване.

Основният изследователски проблем е фрагментираният подход към управлението на информационната сигурност, при който техническите, организационните и нормативните мерки често се прилагат изолирано. Целта на изследването е да анализира концептуалните основи на защитата, заплахите и уязвимостите в цифровата среда, механизмите за противодействие и управление на риска, както и актуалните тенденции пред организациите. Изследователските задачи включват: 1) систематизиране на концептуалните основи на информационната сигурност; 2) идентифициране и класифициране на основните заплахи и уязвимости; 3) анализ на организационните, техническите и нормативните механизми за защита; 4) очертаване на актуалните тенденции и предизвикателства пред организационната сигурност.

МЕТОДОЛОГИЯ НА ИЗСЛЕДВАНЕТО

Изследването е реализирано чрез комплексен анализ на научна литература, международни стандарти и актуални доклади в областта на информационната сигурност и киберсигурността, като са използвани методите на сравнителния анализ, системния подход и анализа на документи. Използвани са вторични източници: рецензирани научни публикации (предимно от 2000–2024 г.), официални документи на международни организации по стандартизация (ISO/IEC, NIST, ENISA, EC) и актуални доклади на водещи институции (World Economic Forum, SANS Institute). Аналитичната рамка съчетава дескриптивен преглед на литературата със структуриран подход, изграден върху триадата конфиденциалност – цялостност – достъпност (CIA) и утвърдените модели за управление на риска.

РЕЗУЛТАТИ

КОНЦЕПТУАЛНИ ОСНОВИ НА ИНФОРМАЦИОННАТА СИГУРНОСТ

Информационната сигурност представлява съвкупност от организационни, технически и правни мерки, насочени към защита на информацията от неразрешен достъп, промяна, унищожаване или неправомерно използване, и се разглежда като стратегическа функция на управлението (Whitman, Mattord, 2022). Развитие на цифровите технологии променя разбирането за сигурност – от защита предимно на физически носители към широк спектър от механизми за електронни данни, комуникационни мрежи, облачни среди и интелигентни системи, което налага интегриран подход, обединя-

ващ технологични решения, организационни политики и нормативна регулация (Andress, 2020).

Информационната сигурност и киберсигурността често се използват като взаимозаменяеми, но между тях има съществени разлики: първата обхваща защитата на информацията независимо от нейния носител, а втората е насочена предимно към цифровите системи и комуникационните мрежи (Von Solms, Van Niekerk, 2013). Информацията се разглежда като ценен организационен актив, чиято загуба или компрометиране може да доведе до сериозни финансови, правни и репутационни последици (Pfleeger, Pfleeger, 2015). Централно място заема понятието „риск“ – вероятността определена заплаха да използва уязвимост и да причини вреда, а управлението на риска включва идентифициране на активите, анализ на заплахите и уязвимостите и прилагане на подходящи мерки (Alberts, Dorofee, 2003; Gibson, 2022).

Фундаментален модел е триадата CIA (Confidentiality, Integrity, Availability) (Bishop, 2018; Stallings, Brown, 2018). Конфиденциалността гарантира достъп само за упълномощени лица чрез криптиране, управление на достъпа и автентикация. Целостността осигурява точност и непроменимост на информацията чрез цифрови подписи, контролни суми и хеширащи алгоритми. Достъпността гарантира навременен достъп на упълномощените потребители чрез резервиране на ресурси, архивиране, аварийно възстановяване и защита срещу DDoS атаки (Stallings, Brown, 2018). Съвременните модели допълват триадата с автентичност, отчетност, надеждност и неотричане на действията (Gollmann, 2011).

Особено внимание заслужава човешкият фактор – значителна част от инцидентите се дължат на човешки грешки, недостатъчна осведоменост или неспазване на политиките, а социалното инженерство и фишингът остават сред най-успешните методи за компрометиране именно поради тази уязвимост (Siponen, 2000; SANS Institute, 2023). Затова изграждането на култура на сигурност, съчетана с обучение и повишаване на осведомеността, е ключов елемент от ефективното управление на информационната сигурност и предпоставка за успешно противодействие на съвременните заплахи.

ЗАПЛАХИ И УЯЗВИМОСТИ В СЪВРЕМЕННИТЕ ОРГАНИЗАЦИИ

Развитието на цифровите технологии и нарастващата зависимост на организациите от информационните системи водят до значително увеличаване на рисковете за сигурността. Заплаха е всяко събитие, което може да наруши конфиденциалността, целостността или достъпността на информацията, а уязвимост е слабост, която може да бъде използвана за причиняване на вреда (Cherdantseva, Hilton, 2013). Идентифицирането и анализът на заплахите и уязвимостите са сред най-важните елементи на управлението на информационната сигурност (Whitman, Mattord, 2022).

Външни заплахи

Външните заплахи произхождат извън организацията и се реализират

най-често чрез интернет или компрометирани системи. Сред тях са кибератаките от организирани престъпни групи и държавно подкрепяни структури, насочени към кражба на информация, финансови измами или саботаж (ENISA, 2024). Особено опасни са атаките тип DDoS, при които компрометирани устройства претоварват инфраструктурата, както и атаките Zero-Day, използващи неизвестни уязвимости (Kizza, 2024). Тревожна тенденция е моделът Cybercrime-as-a-Service, който позволява дори на неопитни лица да извършват сложни кибератаки (World Economic Forum, 2024).

Вътрешни заплахи

Значителна част от инцидентите се дължат на вътрешни лица с легитимен достъп – служители, мениджъри или партньори (Peltier, 2016). Вътрешните заплахи могат да бъдат умишлени (кражба, злоупотреба, саботаж) или неумишлени (човешки грешки, неправилна конфигурация, загуба на устройства). Особен риск представляват лицата с привилегирован достъп, поради което управлението на привилегированите акаунти е основна задача на съвременната сигурност (Kim, Solomon, 2021).

Социално инженерство

Социалното инженерство обхваща техники за психологическо манипулиране с цел получаване на достъп до информация или системи (Siponen, 2000). Най-разпространена форма е фишингът, при който съобщения имитират комуникация от банки или институции (SANS Institute, 2023), а по-усъвършенствани форми, като spear phishing и whaling, са насочени към конкретни лица чрез персонализирана информация. Изкуственият интелект допълнително повишава ефективността на подобни измами чрез генериране на убедителни текстове, изображения и аудио (ENISA, 2024).

Зловреден софтуер

Зловредният софтуер включва вируси, червеи, троянски коне, шпионски програми и ransomware (Stallings, Brown, 2018). Ransomware криптира данните на жертвата и изисква откуп, като се превърна в една от най-значимите заплахи за публичния сектор, здравеопазването и бизнеса (World Economic Forum, 2024). Шпионският софтуер събира информация без знанието на потребителя, най-често чрез електронна поща или компрометирани уебсайтове.

Уязвимости в информационните системи

Уязвимостите са слабости в хардуера, софтуера, мрежите или процесите, които могат да бъдат използвани за атака (Shostack, 2014). Сред най-честите технически уязвимости са остарели операционни системи, липса на актуализации, слаби пароли, неправилна конфигурация, липса на криптиране и недостатъчен контрол на достъпа. Организационните уязвимости включват липса на политики за сигурност, недостатъчно обучение и неясно разпределение на отговорностите (Peltier, 2016). Съвременните атаки обикновено комбинират технически средства, социално инженерство и организационни слабости по логиката на веригата на кибератаката (cyber kill chain) (Cherdantseva, Hilton, 2013; Yadav, Rao, 2015).

Междинен извод

Анализът показва, че средата за сигурност е динамична и непредвидима, а външните атаки, вътрешните злоупотреби, социалното инженерство и техническите слабости формират сложна система от рискове, изискваща цялостен и интегриран подход към защитата на информационните ресурси.

МЕХАНИЗМИ ЗА ЗАЩИТА НА ИНФОРМАЦИЯТА И УПРАВЛЕНИЕ НА СИГУРНОСТТА

Ефективната защита изисква комплексна система от организационни, технически и правни мерки, тъй като не съществува универсално решение, способно самостоятелно да гарантира сигурност. Устойчивата защита се постига чрез многослоен подход, при който различни механизми функционират едновременно и взаимно се допълват (Humphreys, 2016), а организациите преминават от реактивен към проактивен модел, изграждащ превенция, ранно откриване и своевременно противодействие (NIST, 2024).

Организационни мерки за сигурност

Организационните мерки формират основата на системата за сигурност, като определят правила, отговорности и процедури (Peltier, 2016). Ключов инструмент са политиките за информационна сигурност – официални документи, определящи принципите и изискванията за защита (Tipton, Krause, 2016). Съществено значение имат ясното разпределение на отговорностите и програмите за обучение и повишаване на осведомеността, които намаляват риска от човешки грешки (SANS Institute, 2023).

Управление на достъпа

Контролът на достъпа гарантира, че всеки потребител получава достъп само до необходимите му ресурси, съгласно принципа на минималните привилегии (Kim, Solomon, 2021). Многофакторната автентикация (MFA) изисква повече от един метод за удостоверяване и значително намалява риска от неоторизиран достъп (NIST, 2024), а системите за управление на идентичността и достъпа (IAM) автоматизират създаването, промяната и прекратяването на потребителски права.

Криптографска защита

Криптографията осигурява конфиденциалност, цялостност и автентичност чрез преобразуване на информацията в защитена форма (Gollmann, 2011). Прилага се както при съхранение, така и при предаване на данни, като протоколи като TLS осигуряват защитен обмен на информация, а цифровите подписи и инфраструктурите за публични ключове (PKI) гарантират автентичността на комуникацията.

Защита на мрежовата инфраструктура

Защитните стени контролират мрежовия трафик според предварително дефинирани правила (Stallings, Brown, 2018), а системите IDS/IPS осигуряват наблюдение в реално време и автоматично блокиране на атаки. Сегментирането на мрежите ограничава разпространението на атаки между отделните части

на организацията, а виртуалните частни мрежи (VPN) осигуряват защитен отдалечен достъп.

Архивиране и аварийно възстановяване

Архивирането е задължителен елемент на всяка система за сигурност, тъй като загуба на данни може да възникне от кибератаки, технически повреди или човешки грешки. Препоръчва се правилото 3-2-1 – три копия на данните на два различни носителя, едно от които на отделна локация (Andress, 2020), допълнено от редовно тествани планове за аварийно възстановяване.

Международни стандарти и рамки за управление

Управлението на информационната сигурност все по-често се основава на международно признати стандарти. Най-разпространен е ISO/IEC 27001:2022, който определя изискванията за система за управление на сигурността чрез риск ориентиран подход (ISO/IEC 27001:2022). Рамката NIST Cybersecurity Framework 2.0 структурира дейностите в пет направления: идентифициране, защита, откриване, реагиране и възстановяване (NIST, 2024), а COBIT и CIS Controls предоставят допълнителни практически насоки.

Концепцията Defense in Depth

Концепцията Defense in Depth се основава на множество взаимно допълващи се слоеве на защита – физически мерки, контрол на достъпа, криптиране, защитни стени, мониторинг и организационни политики, така че, ако един слой бъде преодолян, останалите продължават да ограничават риска (Humphreys, 2016).

Изводи

Анализът показва, че ефективната информационна сигурност изисква интегриран подход, обединяващ организационни политики, технологични средства, обучение на персонала и международни стандарти, чрез многослойна система за защита.

СЪВРЕМЕННИ ТЕНДЕНЦИИ И ПРЕДИЗВИКАТЕЛСТВА ПРЕД ИНФОРМАЦИОННАТА СИГУРНОСТ

Дигиталната трансформация променя начина, по който организациите функционират и управляват информационните си ресурси, а средата се характеризира с динамичност, глобална свързаност и усложняване на киберзаплахите (World Economic Forum, 2024). Организациите вече са част от сложни цифрови екосистеми – облачни услуги, мобилни технологии, социални мрежи и интелигентни устройства, което разширява повърхността за атака (Whitman, Mattord, 2022).

Облачни технологии и сигурност на данните

Облачните технологии намаляват разходите и улесняват достъпа до ресурси (NIST, 2024), но пораждат рискове от неоторизиран достъп, загуба на контрол върху инфраструктурата, зависимост от външни доставчици и проблеми с юрисдикцията на данните. За тяхното ограничаване се прилагат криптиране, MFA, постоянен мониторинг и хибридни облачни модели (Andress, 2020).

Изкуствен интелект и информационна сигурност

Изкуственият интелект предоставя нови възможности за автоматизирано откриване на аномалии и прогнозиране на заплахи (NIST, 2024), но се използва и от киберпрестъпниците за автоматизиране на атаки и генериране на убедително фалшиво съдържание (ENISA, 2024). Особено предизвикателство представляват технологиите deepfake, използвани за измами и манипулиране на общественото мнение (World Economic Forum, 2024).

Интернет на нещата (IoT)

Свързаните устройства се използват широко в индустрията, здравеопазването и енергетиката (Kizza, 2024), но много от тях имат ограничени механизми за сигурност и фабрични пароли, което ги прави лесни цели за изграждане на ботмрежи, DDoS атаки и неототоризиран достъп до вътрешни системи.

Концепцията Zero Trust

Традиционните модели предполагат доверие вътре в мрежата, но развитието на облачните услуги и дистанционната работа поставя това под съмнение (NIST, 2024). Концепцията Zero Trust изисква непрекъсната проверка на самоличността, минимални привилегии, сегментиране на мрежите и постоянен мониторинг на поведението на потребителите, като постепенно се утвърждава като водещ модел за защита.

Регулаторна среда и нормативни изисквания

Регулацията се превръща в ключов фактор за изграждане на ефективни системи за защита (Schneier, 2015). Общият регламент за защита на данните (GDPR) поставя изисквания за защита на личните данни, прозрачност, управление на съгласието и уведомяване при нарушения (Regulation (EU) 2016/679), а Директива NIS2 разширява изискванията към организациите с критична инфраструктура.

Дистанционна работа и нови рискове

Пандемията от COVID-19 ускори дистанционните модели на работа, при които служителите използват домашни мрежи и лични устройства, което увеличава риска от незащитени комуникации, компрометирани крайни устройства и неототоризиран достъп. В отговор организациите инвестират във VPN решения и технологии за наблюдение на крайните устройства.

Бъдещи направления на развитие

Очаква се информационната сигурност да бъде все по-тясно свързана с изкуствения интелект, автоматизацията и квантовите технологии, като развитието на квантовите компютри налага нови подходи в постквантовата криптография (Gollmann, 2011).

ИЗВОДИ/ДИСКУСИЯ

Проведеният анализ потвърждава, че информационната сигурност е сред ключовите фактори за устойчивостта и конкурентоспособността на съвременните организации. Традиционният подход, основан предимно на технически средства, вече не е достатъчен за противодействие на съвременните кибер-

рискове, поради което се наблюдава ясна тенденция към интегриране на технологични, организационни и управленски механизми в рамките на единна система – с нарастващо значение на международните стандарти, риск ориентирани модели и концепциите за защита в дълбочина и Zero Trust.

Дискусията показва, че най-сериозните рискове произтичат не от техническите уязвимости сами по себе си, а от комбинирането им с човешкия фактор и организационните слабости – социалното инженерство и фишинг кампаниите продължават да демонстрират висока ефективност, което потвърждава необходимостта от инвестиции в обучение и организационна култура на сигурност. Изкуственият интелект има двойствена роля – подпомага откриването на заплахи, но и повишава сложността на атаките, включително чрез deepfake манипулации, а регулаторната рамка (GDPR, NIS2) стимулира организациите да интегрират управлението на риска в стратегическото планиране.

ЗАКЛЮЧЕНИЕ

Информационната сигурност се утвърждава като един от най-важните фактори за устойчивото функциониране на съвременните организации, а информацията – като стратегически ресурс, чиято защита е пряко свързана с конкурентоспособността и общественото доверие (Whitman, Mattord, 2022). Изследването показва, че средата на сигурност се характеризира с висока динамичност – облачните услуги, изкуственият интелект и интернет на нещата пораждат нови заплахи, докато кибератаките, социалното инженерство и вътрешните заплахи остават сериозно предизвикателство независимо от размера и сферата на дейност на организациите (ENISA, 2024; World Economic Forum, 2024).

Принципите за конфиденциалност, цялостност и достъпност остават фундамент на всяка система за защита, допълнени от изисквания за автентичност, отчетност и неотричане на действията (Bishop, 2018; Gollmann, 2011). Управлението на риска и концепцията за защита в дълбочина осигуряват устойчивост срещу сложни атаки (Alberts, Dorofee, 2003; Humphreys, 2016), а човешкият фактор остава едновременно основен източник на риск и решаващо условие за неговото ограничаване (Siponen, 2000; SANS Institute, 2023). В перспектива развитието на изкуствения интелект, автоматизацията и квантовите технологии ще променя характера на заплахите, но само балансираното съчетаване на технологии, процеси, нормативни механизми и човешки ресурси може да гарантира устойчивост и дългосрочно развитие на организациите в дигиталната епоха.

REFERENCES

- Alberts, C., Dorofee, A. (2003). *Managing Information Security Risks: The OCTAVE Approach*. Addison-Wesley.
- Andress, J. (2020). *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice*. 3rd ed. Elsevier.

- Bishop, M. (2018). *Computer Security: Art and Science*. 2nd ed. Addison-Wesley.
- Cherdantseva, Y., Hilton, J. (2013). A Reference Model of Information Assurance and Security. *International Journal of Information Management*, 33(1), 71–77.
- ENISA. (2024). *ENISA Threat Landscape Report 2024*. European Union Agency for Cybersecurity.
- Gibson, D. (2022). *Managing Risk in Information Systems*. Jones & Bartlett Learning.
- Gollmann, D. (2011). *Computer Security*. 3rd ed. John Wiley & Sons.
- Humphreys, E. (2016). *Implementing the ISO/IEC 27001 Information Security Management System Standard*. Artech House.
- ISO/IEC 27001:2022 *Information Security, Cybersecurity and Privacy Protection – Requirements*. <https://www.iso.org/standard/27001>
- Kim, D., Solomon, M. (2021). *Fundamentals of Information Systems Security*. 4th ed. Jones & Bartlett Learning.
- Kizza, J. (2024). *Guide to Computer Network Security*. 7th ed. Springer.
- NIST. (2024). *NIST Cybersecurity Framework (CSF) 2.0*. National Institute of Standards and Technology.
- Peltier, T. (2016). *Information Security Policies, Procedures and Standards*. CRC Press.
- Pfleeger, C., Pfleeger, S. (2015). *Security in Computing*. 5th ed. Prentice Hall.
- Regulation (EU) 2016/679. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- SANS Institute. (2023). *Security Awareness Report*. SANS Institute.
- Schneier, B. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. W.W. Norton.
- Shostack, A. (2014). *Threat Modeling: Designing for Security*. Wiley.
- Siponen, M. (2000). A Conceptual Foundation for Organizational Information Security Awareness. *Information Management & Computer Security*, 8(1), 31–41.
- Stallings, W., Brown, L. (2018). *Computer Security: Principles and Practice*. 4th ed. Pearson.
- Tipton, H., Krause, M. (2016). *Information Security Management Handbook*. 7th ed. CRC Press.
- Von Solms, R., Van Niekerk, J. (2013). From Information Security to Cyber Security. *Computers & Security*, 38, 97–102.
- Whitman, M., Mattord, H. (2022). *Principles of Information Security*. 7th ed. Cengage Learning.
- World Economic Forum. (2024). *Global Cybersecurity Outlook 2024*. World Economic Forum.
- Yadav, T., Rao, A. (2015). Technical Aspects of Cyber Kill Chain. In: J. H. Abawajy, S. Mukherjea, S. M. Thampi, A. Ruiz-Martínez (Eds). *International Symposium on Security in Computing and Communication*, Third International Symposium, SSCC 2015, Kochi, India, August 10-13, 2015 (pp. 438–452). Springer.

INFORMATION SECURITY IN MODERN ORGANIZATIONS: THREATS, VULNERABILITIES AND PROTECTION MECHANISMS

Abstract: *In the context of accelerated digital transformation, information security has become a strategic factor for the sustainable functioning of modern organizations. The intensive use of information and communication technologies creates new opportunities for development, while simultaneously generating significant risks associated with cyberattacks, data breaches, disruption of business processes, and compromise of organizational resources. The study aims to analyze the conceptual foundations of information security, to systematize the most common threats and vulnerabilities in the contemporary digital environment, and to present effective organizational, technical, and regulatory mechanisms for protecting information assets, applying a methodology based on comparative analysis, a systems approach, and document analysis of academic literature, international standards, and current institutional reports. The main findings show that effective information security cannot be achieved through isolated technical solutions alone, but requires an integrated, multi-layered approach in which the human factor plays a central role in the success of protection. Particular attention is paid to the role of the human factor, risk management, and the need for an integrated approach combining technological, organizational, and regulatory means of protection. The results of the study are applicable for managers, information security professionals, and policy makers, as they provide a systematized framework for risk assessment and the selection of suitable protection mechanisms in an organizational context. The study highlights the importance of information security as a key element of strategic management and sustainable organizational development in the digital age.*

Keywords: *information security; cybersecurity; risk management; information systems; digital transformation*

Assoc. Prof. Sergey Modev, PhD

ORCID 0000-0002-0095-6358

University of Library Studies and Information Technologies
Sofia, Bulgaria

E-mail: s.modev@unibit.bg

Nikolay Atanasov, PhD Student

Scientific Advisor: Assoc. Prof. Sergey Modev, PhD

University of Library Studies and Information Technologies
Sofia, Bulgaria

E-mail: nikdatt@yahoo.com

Miroslav Shalev, PhD Student

Scientific Advisor: Assoc. Prof. Sergey Modev, PhD

University of Library Studies and Information Technologies
Sofia, Bulgaria

E-mail: schalev@ab.investments

Boyko Velkov, PhD Student
Scientific Advisor: Assoc. Prof. Sergey Modev, PhD
University of Library Studies and Information Technologies
Sofia, Bulgaria
E-mail: BoykoVelkov@gmail.com