Міжнародна науково-практична конференція

“Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку”

15 березня 2023 року, м. Харків

Міжнародна науково-практична конференція “Застосування інформаційних технологій у підготовці та діяльності сил охорони правопорядку” / Збірник тез доповідей (м. Харків, 15 березня 2023 р.). – Харків. – 2023. – 248 с.

Організатори конференції: Національна академія Національної гвардії України (м. Харків); Харківський національний університет радіоелектроніки (м. Харків).

Організаційний комітет конференції:

Голова – Іохов О. Ю., доктор технічних наук, с.н.с., професор, начальник кафедри військового зв’язку та інформатизації Національної академії Національної гвардії України (+38097-69-81-250).

Заступник голови – Малюк В. Г., кандидат технічних наук, доцент, доцент кафедри військового зв’язку та інформатизації Національної академії Національної гвардії України.

Відповідальний секретар – Новикова О. О., кандидат технічних наук, доцент, доцент кафедри військового зв’язку та інформатизації Національної академії Національної гвардії України.

Члени організаційного комітету:

Соколовський С. А. – кандидат технічних наук, доцент, начальник Національної академії Національної гвардії України;

Кайдалов Р. О. – доктор технічних наук, професор, заступник начальника з наукової роботи Національної академії Національної гвардії України;

Семенець В. В. – доктор технічних наук, професор, професор Харківського національного університету радіоелектроніки;

Петришин Л. Б. – доктор технічних наук, професор, професор Науково-технологічного університету AGH, м. Краків, Польща; професор кафедри комп’ютерних наук та інформаційних систем Прикарпатського національного університету ім. В. Стефаника;

Собчук Г. (Sobczuk H.) – доктор наук, професор, професор університету “Люблінська політехніка”, м. Люблін, Польща;

Безкоровайний В. В. – доктор технічних наук, професор, професор кафедри системотехніки Харківського національного університету радіоелектроніки;

Дудар З. В. - кандидат технічних наук, професор, завідувачка кафедри програмної інженерії Харківського національного університету радіоелектроніки;

Кобзєв В. Г. – кандидат технічних наук, с.н.с., доцент кафедри програмної інженерії Харківського національного університету радіоелектроніки;

Козлов В. Є. – кандидат технічних наук, доцент, доцент кафедри військового зв’язку та інформатизації Національної академії Національної гвардії України.

Адреса організаційного комітету: 61001, м. Харків, майдан Захисників України, 3, Національна академія Національної гвардії України, науково-організаційний відділ.
Телефон: +38097-69-81-250. **Електронна адреса**: nanguki@ukr.net.

Тези доповідей опубліковано в авторській редакції, мовою оригіналу: **http://kinf.nangu.edu.ua**

Відповідальність за фактичні помилки, зміст і достовірність інформації та точність викладених фактів несуть автори.

Ministry of Internal Affairs of Ukraine
National Academy of the National Guard of Ukraine

Ministry of Education and Science of Ukraine
Kharkiv National University radio electronics

International scientific and practical conference

"Application of information technologies in the preparation and operation of law enforcement forces"

March 15, 2023

Kharkiv

International scientific and practical conference "Application of information technologies in the preparation and operation of law enforcement forces" / Collection of theses of reports (Kharkiv, March 15, 2023). – Kharkiv. – 2023. – 248 p.

Conference organizers: National Academy of the National Guard of Ukraine (Kharkiv), Kharkiv National University of Radio Electronics (Kharkiv).

Organizing committee of the conference:

Chairman - Iokhov O. Yu., Doctor of Technical Sciences, Senior Researcher, Professor, Head of the Department of Military Communications and Informatization of the National Academy of the National Guard of Ukraine (+38097-69-81-250).

Deputy Chairman - Malyuk V.G., Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of Military Communications and Informatization of the National Academy of the National Guard of Ukraine.

Executive secretary - Novykova O.O., Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of Military Communications and Informatization of the National Academy of the National Guard of Ukraine.

Organizing Committee Members:

Sokolovsky S. A. – Candidate of Technical Sciences, Associate Professor, Head of the National Academy of the National Guard of Ukraine;

Kaidalov R.O. - Doctor of Technical Sciences, Professor, Deputy Head for Research of the National Academy of the National Guard of Ukraine;

Semenets V. V. – Doctor of Technical Sciences, Professor, Professor of Kharkiv National University of Radio Electronics;

Petryshyn L. B. - Doctor of Technical Sciences, Professor, Professor of the AGH University of Science and Technology, Krakow, Poland; Professor of the Department of Computer Science and Information Systems, Prykarpattia National University named of V. Stefanik;

Sobczuk G. (Sobczuk H.) – Doctor of Science, Professor, Professor of the University of Lublin Polytechnic, Lublin, Poland;

Bezkorovainy V. V. – Doctor of Technical Sciences, Professor, Professor of the System Engineering Department of the Kharkiv National University of Radio Electronics;

Dudar Z. V. - Candidate of Technical Sciences, Professor, Head of the Department of Software Engineering, Kharkiv National University of Radio Electronics;

Kobzev V. G. – Candidate of Technical Sciences, Senior Researcher, Associate Professor, Department of Software Engineering, Kharkiv National University of Radio Electronics;

Kozlov V. E. – Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department of Military Communications and Informatization of the National Academy of the National Guard of Ukraine.

Organizing committee address: 61001, Kharkiv, Maidan Defenders of Ukraine, 3, National Academy of the National Guard of Ukraine, scientific and organizational department.
Phone: +38097-69-81-250 (Iokhov O. Yu.). **Email:** nanguki@ukr.net.

Theses of reports are published in the author's edition, in the original language: **http://kinf.nangu.edu.ua**

The responsibility for factual errors, the content and reliability of information and the accuracy of the facts presented are carried by the authors.

підпорядкованої військової частини (підрозділу) та своїх функціональних обов'язків; укомплектуванням штабів особовим складом і забезпеченням їх засобами управління; навченістю особового складу, злагодженістю структурних підрозділів органу управління; підтриманням постійної бойової готовності підрозділів охорони і забезпечення; підтриманням пунктів управління і засобів управління у готовності до функціонування, забезпечення їх безперебійної роботи; якісною організацією чергової служби на пунктах управління; підтриманням стійкого зв'язку з підпорядкованими підрозділами, вищим і взаємодіючими штабами

Оперативність управління – здатність командирів (штабів) виконувати управлінські завдання у стислі терміни, що забезпечують випередження ДРС (НЗФ) противника в діях, швидке реагування на зміни обстановки та своєчасний вплив на дії підрозділів в інтересах успішного виконання поставлених завдань і досягнення мети спеціальних (бойових) дій.

Оперативність управління досягається: високим рівнем підготовки командирів (начальників штабів) та службових осіб органів управління, їх організаторськими здібностями; постійним знанням обстановки, прогнозуванням її розвитку та швидким реагуванням на зміни; своєчасним уточненням планів і завдань підрозділам; застосуванням оптимального алгоритму роботи органу управління; ефективним застосуванням засобів автоматизації управління.

Основним органом управління–повсякденною діяльністю військових частин територіальної оборони у мирний час та управління ними в ході ведення територіальної оборони є координаційний штаб. Свою роботу він організовує на підставі вказівок командира та розпоряджень вищого штабу. Штаб об'єднує, координує і направляє зусилля всіх службових осіб інших органів управління на забезпечення своєчасного і повного виконання підрозділами визначених завдань. Крім того, штаб визначає завдання і порядок роботи підлеглих штабів, інформує інші органи управління про обстановку, доводить до них накази (вказівки) командира в частині, що їх стосується, надає їм необхідну допомогу.

Таким чином основними напрямками для підвищення оперативності управління необхідно створення інформаційних тенологій підтримки прийняття рішень при виконанні спеціальних (бойових) завдань за призначенням. Підвищення організаторських здібностей особового складу координаційного штабу.

УДК 005.94+004.056

Данилов А.Д.

АКТУАЛЬНІСТЬ ВИКЛАДАННЯ КУРСІВ, ПОВ'ЯЗАНИХ З БЛОКЧЕЙН-ТЕХНОЛОГІЄЮ ТА КРИПТОВАЛЮТАМИ, У ЗВО

В роботі розглянуто питання актуальності викладання основ електронної комерції, зокрема блокчейн технології та основ використання криптовалюти у ЗВО. За результатами проведеного аналізу предметної галузі наведено особливості використання криптовалюти, загрози її використання для користувачів, переваги користування криптовалютою. Також було розглянуто законодавчу базу використання криптовалюти, зокрема BTC в різних країнах та перспективи подальшого розвитку ринку криптовалюти в Україні та світі.

Використання інформаційних технологій в повсякденному житті та на роботі вже давно стало звичайною практикою. І якщо використання Інтернету є нормою та звичною справою, використання криптовалюти ще не зазнало такого широкого

розповсюдження та несе для пересічного користувача досить багато ризиків та потенційних проблем.

З кожним днем пересічний користувач Інтернету все частіше стикається з використанням різноманітної криптовалюти (біткойни, альткойни, токени). Придбання та використання криптовалют пропонує користувачу швидкий прибуток та значні дивіденди від покупки криптовалюти. Але чи справді все так просто та легко? Можливо більшість подібних повідомлень мають мету ввести людину у оману та шахрайським шляхом виманити у неї гроші.

Для того щоб уникнути подібного доцільно підвищувати рівень інформованості та обізнаності населення в галузі електронної комерції та зокрема використання криптовалюти. Особливо важливим така обізнаність є для майбутніх захисників правопорядку. Таким чином вивчення основ електронної комерції та особливостей використання криптовалюти є актуальним та безумовно корисним надбанням для фахівців будь-якої галузі.

Необхідно розуміти переваги, недоліки та загрози використання криптовалюти.

Наразі дуже багато людей цікавляться даною тематикою та розглядають можливість капіталовкладень у криптовалюту. Розглянемо основні аспекти використання криптовалют, загрози та переваги їх використання.

Основні аспекти використання криптовалют:

– можливість швидкого заробітку;

– популярний та престижний вид капіталовкладень;

– відсутність прив’язки криптовалюти до конкретного ресурсу, тобто зміна курсу криптовалюти не прив’язана до якогось матеріального чинника. Таким чином курс криптовалюти може суттєво коливатись, що може бути суттєвою перевагою та суттєвим недоліком.

Загрози використання криптовалюти:

– залежність криптовалюти від валідаторів;

– незахищеність власників куриптовалюти, особливо з точки зору законодавства. Більшість власників криптовалюти несуть власну відповідальність за свої капіталовкладення;

– відсутність законодавчої бази, що забезпечую умовну безпеку капіталовкладень;

– небезпека втрати валюти у разі втрати «електронного ключа»;

– обмежена дохідність майнінгу, що з кожним роком стає меншою, тобто витрати на обладнання та поточні витрати збільшуються, а вигода від створення нових блоків щороку зменшується.

Переваги криптовалют:

– умовна доступність майнінгу та криптовалюти, фактично кожен користувач при наявності певної кількості ресурсів може займатися майнінгом, або стати власником криптовалюти;

– конфіденційність, фактично криптовалюта майже не відслідковується, це є важливим недоліком з точки зору законодавства, але для пересічного користувача є доволі привабливим;

– відсутність державного управління, фактично будь-яка криптовалюта є незалежною грошовою одиницею, тому відсутнє пряме регулювання курсу криптовалюти;

– надійність – фактично криптовалюта захищається самими власникам монет , що зацікавлені в її стійкості. Тобто всі власники криптовалюти зацікавлені в її стабільності та будуть перешкоджати маніпуляціям криптовалютою. Також варто зазначити, що більшість криптовалют побудовані таким чином, що можливість махінацій з криптовалютою зводяться до мінімуму.

Перспективи розвитку криптовалют. Загалом, ринок криптовалют має перспективи

для подальшого росту. Все частіше ми стикаємося з оплатою товарів та послуг з допомогою електронної валюти.

У багатьох країнах вже зараз BTC є офіційною платіжною одиницею, зокрема в Японії. З 2015 року відповідно до рішення Європейського суду транзакції в біткоїнах були віднесені до платіжних операцій з валютами, монетами і банкнотами. Низка країн узаконили біктоїн, як платіжну одиницю: Канада, Німеччина, Франція, Велика Британія, Іспанія, Данія, Ісландія, Мексика та Японія[1]. Але варто зазначити, що використання біткойна заборонено в низці країн, таких як Китай, В'єтнам, Бангладеж та інші.

За власною ініціативою вже зараз біткоїни, як валюту приймають у багатьох магазинах в США та Європі, зокрема біткоїнами можливо оплатити покупку в Amazon, якщо сума покупки не перевищує 30 доларів[1].

За оцінками платіжної платформи Triple A, у 2021 році кількість усіх криптокористувачів у світі перевищила 300 млн[1].

Розглянемо відношення до біткойн в Україні.

У 2022 році Верховна Рада України ухвалила закон №3637 «Про віртуальні активи», який легалізує ринок віртуальних активів в Україні та виводить криптосектор із тіні[1].

Ось що зміниться в законодавчій базі після підписання зазначеного закону[1]:

- легально працюватимуть іноземні та українські криптобіржі;
- банки відкриватимуть рахунки для криптокомпаній;
- українці зможуть захистити свої вкладення у віртуальних активах;
- уряд гарантуватиме судовий захист прав на віртуальні активи.

Таким чином, розглядаючи перспективи розвитку криптовалюти в світі та Україні можна сказати, що при належному рівні захисту, грамотності населення в галузі електронної комерції та реально працюючій законодавчій базі, що регулює ринок криптовалюти в країні, біткойни та інші види криптовалюти є перспективним капіталовкладенням та потребують подальшого дослідження. Вивчення криптовалюти у ЗВО є доцільним для різних галузей, але особливо актуальним воно залишається саме для технічних галузей та при підготовці фахівців пов'язаних з забезпечення правопорядку та безпеки.

Список використаних джерел

1 Що таке біткоїн і чому він такий популярний. https://mc.today/uk/bitkoyin/: веб сайт URL https://mc.today/uk/bitkoyin/ (дата звернення: 1.03.2023).

УДК 004.056

Іващенко Д.О., Данилов А.Д.

АНАЛІЗ МЕТОДІВ НЕЗАКОННОГО ВИЛУЧЕННЯ ТА ЗАХИСТУ ІНФОРМАЦІЇ

Робота присвячена захисту інформації та інформаційних активів. В тезах доповіді наведено результати аналізу методів незаконного вилучення та захисту інформації, надані загальні рекомендації щодо використання методів захисту від втрати або пошкодження інформаційних активів.

В сучасному світі, де інформаційні технології є невід'ємною частиною нашого життя, захист інформації стає все більш важливим завданням. Незаконне вилучення інформації може призвести до серйозних наслідків, таких як порушення конфіденційності, цілісності та доступності даних.

З кожним роком збільшується кількість злочинів, пов'язаних з кібербезпекою.

Зокрема, зловмисники застосовують різноманітні методи незаконного вилучення інформації, такі як фішинг, кібератаки, розповсюдження шкідливих програм тощо. Ці злочинні дії можуть призвести до значних фінансових втрат, порушення конфіденційності та приватності даних, а також вплинути на репутацію компаній та організацій.

Незаконне вилучення інформації є серйозною загрозою для конфіденційності, цілісності та доступності даних. Конфіденційні дані, такі як особисті дані або комерційна інформація, можуть бути вилучені і використані для злочинних цілей, таких як шахрайство, вимагання викупу або крадіжка особистої інформації. Цілісність даних також може бути порушена, якщо зловмисники вносять небажані зміни до даних або використовують методи шифрування для блокування доступу до даних власникам. Крім того, доступність даних може бути обмежена, якщо зловмисники використовують методи Denial of Service або інші методи атак на мережу, щоб перевантажити систему і заблокувати доступ до даних.

Основні методи незаконного вилучення інформації включають:

1. Фішинг – це метод, при якому злочинці використовують підроблені електронні листи або веб-сайти, щоб отримати доступ до конфіденційної інформації, такої як паролі, номери кредитних карток, паспортні дані і т.д.

2. Віруси та троянські програми – це програми, які можуть використовуватись для вилучення конфіденційної інформації з комп'ютерів без дозволу власника. Віруси можуть поширюватись через електронну пошту, соціальні мережі або програми, які завантажуються з Інтернету.

3. Перехоплення трафіку – це метод, при якому злочинці перехоплюють трафік мережі, щоб отримати доступ до конфіденційної інформації, яку пересилають користувачі. Цей метод може бути використаний для отримання доступу до паролів, номерів кредитних карток та іншої конфіденційної інформації.

4. Фізичний доступ до даних – це метод, при якому злочинці отримують доступ до комп'ютерів або інших пристроїв, щоб викрасти конфіденційну інформацію. Цей метод може використовуватись в офісах або інших місцях, де зберігається конфіденційна інформація.

5. Соціальна інженерія – це метод, при якому злочинці використовують соціальні навички, щоб отримати доступ до конфіденційної інформації. Наприклад, злочинець може намагатись переконати працівника компанії надати йому доступ до системи, надавши підробку ідентифікації або зламавши пароль. Також соціальна інженерія може включати в себе фішинг-атаки, коли злочинці надсилають електронні листи, які здаються легітимними, але насправді містять шкідливі посилання або додатки для вилучення інформації.

Існує кілька методів захисту від незаконного вилучення інформації, які допомагають зменшити ризики втрати даних і зберегти конфіденційність, цілісність і доступність інформації. Основні методи захисту включають:

1. Фізичні методи захисту, такі як захист приміщення з обладнанням, забезпечення фізичної безпеки пристроїв зберігання даних, контроль доступу до приміщення з серверами і іншим обладнанням.

2. Організаційні методи захисту, які включають політику безпеки, культуру безпеки, процедури, правила і інструкції, що встановлюються в компанії для забезпечення безпеки інформації. Такі методи також включають регулярні навчання працівників з питань безпеки даних та аудит безпеки даних.

3. Технічні методи захисту, які включають захист мереж, захист даних, використання сильних паролів, шифрування даних, контроль доступу і ідентифікацію користувачів.

4. Юридичні методи захисту, такі як договірні зобов'язання, які є обов'язковою умовою взаємодії між компаніями, правові засоби, що захищають права на

інтелектуальну власність та конфіденційність даних.

Існує декілька методів протидії незаконному вилученню інформації, серед яких можна виділити такі:

1. Використання комплексної системи захисту: використання технічних, організаційних та юридичних методів захисту даних.
2. Регулярні оновлення програмного забезпечення: оновлення програмного забезпечення, що дозволяють закрити вразливості та запобігти злому.
3. Використання шифрування даних: шифрування даних дозволяє зберігати інформацію в зашифрованому вигляді, що ускладнює доступ до неї для зловмисників.
4. Політика безпеки та культура безпеки: розробка та впровадження політики безпеки, яка містить вимоги щодо захисту даних, а також створення культури безпеки серед співробітників.
5. Навчання персоналу: навчання співробітників технікам безпеки та правилам користування комп'ютерною технікою та інформаційними системами.
6. Контроль доступу та ідентифікація: використання засобів контролю доступу до інформації та ідентифікації користувачів.
7. Резервне копіювання даних: регулярне створення резервних копій даних дозволяє відновити інформацію у разі її втрати або пошкодження.
8. Моніторинг та аудит безпеки: проведення моніторингу та аудиту безпеки даних для виявлення можливих загроз та вразливостей системи.

Методи незаконного вилучення інформації можуть бути дуже різноманітними і складними, тому потрібно розробляти ефективні методи протидії несанкціонованого та незаконного вилучення інформації. Для цього необхідно розуміти потенційні загрози та використовувати відповідні методи захисту даних та інформаційних активів, щоб забезпечити їхню конфіденційність, цілісність та доступність. Також важливо постійно оновлювати методи протидії відповідно до нових загроз та викликів, які постійно змінюються.

УДК 355.424::623.418.2

Стернат Д.О.

ЗАСТОСУВАННЯ ТРОФЕЙНОГО ОЗБРОЄННЯ ЗЕНІТНИХ РАКЕТНИХ ВІЙСЬК, ДОБУТОГО ПІД ЧАС РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

Під час повномасштабного вторгнення Російської Федерації на територію України оборонцями країни було здобуто багато трофейної техніки зенітних ракетних військ в справному стані або такої що потребує незначного ремонту. Світова практика передбачає три варіанти застосування трофеїв, а саме: дослідження на полігоні, безпосереднє застосування на полі бою та реінжиніринг.

Полігонні випробування трофейної техніки дозволяють проводити дослідження озброєння, вивчення його дійсних характеристик, слабких місць та переваг. Цей шлях в умовах дефіциту зенітного ракетного озброєння в країні не є пріоритетним. Більш раціональним в сучасних умовах є бойове застосування даної техніки для прикриття об’єктів та військ від ударів противника з повітря з паралельним дослідженням його характеристик. Головною умовою в цьому випадку є наявність боєкомплекту та висококваліфікованих фахівців, здатних експлуатувати дане озброєння.

Проведення по відношенню до трофейного озброєння реінжинірингу здійснюється з метою його дослідження та конструювання подібного озброєння та військової техніки, або дослідження технологій, що використовувалися в даному виді озброєння з метою удосконалення власного озброєння. Для цього необхідні значні наукові та технічні

Руда І.М., Данилов А.Д.

ДО ПИТАНЬ ЕФЕКТИВНОСТІ ТА БЕЗПЕКИ ВИКОРИСТАННЯ БОТІВ У МЕСЕНДЖЕРАХ В РОБОТІ ПРАВООХОРОННИХ ОРГАНІВ

Робота присвячена аналізу особливостей використання чат ботів у роботі правоохоронних органів. В тезах проаналізовані переваги та загрози використання чат ботів у роботі правоохоронних органів.

Ми живемо під час активного розвитку нових технологій, автоматизації та комп'ютеризації багатьох процесів. Для того аби не відставати від технологічного розвитку у 2016 році Національна поліція України створила власний, офіційний портал, для інформування громадян. Згодом у 2018 році почав функціонувати телеграм-бот @drughunters_ukraine_bot. З того моменту було створено багато інших ботів у таких соціальних мережах як Viber та Telegram. В цій роботі було розглянуто позитивні та негативні аспекти використання телеграм ботів поліцією та іншими органами.

Позитивною стороною використання сучасних технології в роботі правоохоронних органів, зокрема телеграм бота, є швидкість та відносна легкість створення боту, використання двох найпопулярніших месенджерів в Україні, онлайн співпраця з правоохоронними органами, економія часу співробітників та користувачів, зручність у використанні.

Найочевиднішим недоліком є можливий спам та дезінформація, оскільки відправити запит до бота зазвичай може будь-який користувач месенджера. Деякі системи створенні з урахуванням цієї проблеми, тому бот запрошує доступ до номера телефону. Враховуючи що в Україні до мобільних номерів не прив'язані документи власника, будь-хто може використовувати будь-яку кількість номерів.

Використання ботів у месенджерах надає вірогідність викрадення чи видалення боту, внаслідок проникнення до облікового запису, через який було створено бота. Також часто створюють аналог бота, щоб збирати персональні дані людей чи поширювати дезінформацію.

Варто було б зазначити, що Telegram позиціонує себе як безпечний інструмент зв'язку, і є безумовним лідером порівняно з тим же Viber, але на жаль, у своїх ботах використовує протокол HTTP(S). Це означає, що коли Ви надсилаєте текстове повідомлення, воно не надсилається одразу до отримувача. Спочатку воно потрапить на сервер Telegram, потім там збережеться, а потім потрапить до одержувача. Тобто ваше повідомлення може бути прочитане сторонніми особами [1].

За результатами проведеного аналізу можна прийти до висновку, що чат-боти звичайно корисні та полегшують роботу правоохоронним органам, але зі сторони безпеки вони мають очевидні недоліки, які ставлять під питання безпеку даних надісланих ботом, наприклад якщо система обробляє інформацію з закритих баз даних чи отримує повідомлення від громадян.

Список використаних джерел

1. Be Careful Using Bots on Telegram. https://www.wired.com/story/telegram-bots-tls-encryption/ : веб сайт URL https://www.wired.com/story/telegram-bots-tls-encryption/ (дата звернення: 27.02.2023).

Для нотаток

For notes

Для нотаток

Наукове видання

Міжнародна науково-практична конференція

“ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ПІДГОТОВЦІ ТА ДІЯЛЬНОСТІ СИЛ ОХОРОНИ ПРАВОПОРЯДКУ”

Збірник тез доповідей

Відповідальний за випуск *О. Ю. Іохов*

В авторській редакції.
Упорядники: *В. Є. Козлов, О. О. Новикова*
Комп’ютерна верстка: *О. О. Новикова*

Формат 60х84/16. Ум. друк. арк. 9,62. Тираж 30 пр. Зам. № 39.

Видавець і виготовлювач Національна академія Національної гвардії України
Майдан Захисників України, 3, м. Харків, 61001.
Свідоцтво суб’єкта видавничої справи ДК № 4794 від. 24.11.2014 р.

Наукове видання

Міжнародна науково-практична конференція

“ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ПІДГОТОВЦІ ТА ДІЯЛЬНОСТІ СИЛ ОХОРОНИ ПРАВОПОРЯДКУ”

Збірник тез доповідей

Відповідальний за випуск *О. Ю. Іохов*

В авторській редакції.
Упорядники: *В. Є. Козлов, О. О. Новикова*
Комп’ютерна верстка: *О. О. Новикова*

Формат 60х84/16. Ум. друк. арк. 9,62. Тираж 30 пр. Зам. № 39.

Видавець і виготовлювач Національна академія Національної гвардії України
Майдан Захисників України, 3, м. Харків, 61001.
Свідоцтво суб’єкта видавничої справи ДК № 4794 від. 24.11.2014 р.