Міністерство освіти і науки України

Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут»

МЕТОДИ ТА ТЕХНОЛОГІЇ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ІНДУСТРІАЛЬНИХ І ВЕБ-ОРІЄНТОВАНИХ СИСТЕМ І МЕРЕЖ

Автори:

1. **МОРОЗОВА Ольга Ігорівна** – доктор технічних наук, доцент, професор Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут».
2. **НІЧЕПОРУК Андрій Олександрович** – кандидат технічних наук, доцент, доцент Хмельницького національного університету.
3. **ТЕЦЬКИЙ Артем Григорович** – кандидат технічних наук, старший викладач Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут».
4. **ТКАЧОВ Віталій Миколайович** – кандидат технічних наук, доцент Харківського національного університету радіоелектроніки.

реферат
Харків – 2021

Актуальність теми дослідження. Одним з перспективних напрямів сталого розвитку сучасних інформаційних та комунікаційних технологій є забезпечення кібербезпеки індустріальних і веб-орієнтованих систем і мереж. Це пов'язано з тим, що четверта промислова революція поступово трансформує всі сфери суспільного життя, виробництва й економіки, інтегруючи їх процеси у кіберпростір.

Разом із очевидними перевагами та зручностями, що несе із собою імплементація індустріальних систем, для зловмисників залишається ряд потенційних «вузьких» місць у кібербезпеці таких систем. Усі дані, які створюються, передаються та оброблюються, мають цінність для кіберзлочинців. Отримання третьою стороною доступу до даних може призвести до різноманітних збитків.

Будь-який пристрій, підключений до мережі, може бути потенційно вразливим. Зловмисник може здійснити атаку на будь-яку ланку індустріальної системи, зокрема на фізичні пристрої, керовані стаціонарними або мобільними операційними системами, мережні сервіси, веб-орієнтовані системи, хмарні сервіси.

Більшість технологічних процесів в індустрії безпосередньо пов'язані зі застосуванням технології віртуалізації. Дійсно, наявність великої кількості різноманітного обладнання створює додаткові складності системним адміністраторам, що обслуговують цю інфраструктуру. Для поліпшення кібербезпеки в індустрії все частіше використовують в якості робочих місць тонкі клієнти, для яких комунікації відбуваються за певним протоколом (безпосередньо протокол залежить від вибору конкретного термінального рішення). При цьому важливим питанням є забезпечення кібербезпеки віртуальних мереж, які є середовищем передачі даних.

Разом з тим, створення та функціонування будь-якої системи кіберзахисту неможливе без висококваліфікованого фахівця в галузі забезпечення кібербезпеки. Сьогодні професійна освіта України постійно перебуває в стані реорганізації та модернізації, постійно адаптуючись до вимог роботодавців.

Зокрема, це стосується механізмів підготовки фахівців, які мають володіти новітніми знаннями й компетентностями.

З огляду підготовки фахівців з кібербезпеки, основними стратегіями розвитку професійної освіти на найближчі роки є створення життєздатної системи безперервного навчання для досягнення актуальних знань і компетентностей. Крім того, компетентності формуються завдяки вивченню багатьох різних дисциплін, використанню в освітньому процесі математичного апарату й різних методів подання знань, які не завжди є близькими до тих, що необхідні при вирішенні завдань роботодавців. Як наслідок, одним зі шляхів підготовки фахівців з кібербезпеки є запровадження дуальної системи професійної освіти.

Таким чином, актуальним напрямом досліджень є розроблення та впровадження моделей, методів і технологій забезпечення кібербезпеки індустріальних і веб-орієнтованих систем і мереж.

Аналіз відомих праць і проєктів, а також досвід експлуатації індустріальних і веб-орієнтованих систем, надають змогу сформулювати мету та завдання досліджень, які проводилися авторами з 2011 року.

Мета роботи: забезпечення кібербезпеки індустріальних і веб-орієнтованих систем і мереж шляхом розроблення та впровадження відповідної методології (концепції, принципів, комплексу моделей, методів) і технологій в індустрії, а також при підготовці фахівців з кібербезпеки під час здобуття професійних знань.

Науково-прикладне завдання, яке вирішується в роботі: розроблення моделей, методів і технологій забезпечення кібербезпеки мобільних систем, веб-орієнтованих систем на основі систем керування вмістом, віртуальних мереж, що забезпечують їх взаємодію, та методології підготовки фахівців з кібербезпеки.

Зв'язок роботи з науковими програмами, планами, темами. Дана комплексна наукова робота містить дослідження авторів, які було проведено з 2011 по 2020 рік:

а) *у рамках реалізації наукових проектів Міністерства освіти і науки України, що фінансувалися за рахунок загального фонду державного бюджету*:

– «Наукові засади, методи та засоби зеленого комп'ютингу та комунікацій» (Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ», Д503–9/2015-ф, ДР №0115U000996, 2015-2017 рр.);

– «Методологія сталого розвитку та інформаційні технологій зеленого комп'ютингу та комунікацій» (Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ», Д503–1/2018-ф, ДР №0118U003822, 2018-2020 рр.);

– «Методологічні засади та технології оцінювання та забезпечення безпеки (захисту) критичних інформаційних інфраструктур» (Національний аерокосмічний університет ім. М. Є. Жуковського «ХАІ», Д503–2/2019-ф, ДР № 0119U100979, 2019 р. – по т.ч.);

– «Методологія інтелектуального автоматизованого оцінювання відповідності програмного забезпечення систем критичного застосування вимогам» (Хмельницький національний університет, ДР № 0111U002294, 2011 р.);

– «Розроблення високоефективних методів відбору енергії від фотоелектричних модулів» (Хмельницький національний університет, ДР № 0116U001548, 2018 р.);

– «Агентно-орієнтована система підвищення безпеки та якості програмного забезпечення комп'ютерних систем» (Хмельницький національний університет, № ДР 0119U100662, 2019 р.);

б) *виконувалися в рамках міжнародних наукових та освітніх проектів*:

– проєкт Європейського Союзу TEMPUS SEREIN (543968-TEMPUS-1-2013-1-EE-TEMPUS-JPCR) Модернізація курсів з інформаційної безпеки та стійкості для гуманітарних та індустріальних доменів, «Modernization of Postgraduate Studies on Security and Resilience for Human and Industry Related Domains» (2013 – 2016 рр.);

– проєкт Європейського Союзу TEMPUS CABRIOLET (544497-TEMPUS-1-2013-1-UK-TEMPUS-JPHES) Модельно-орієнтований підхід та інтелектуальна система для еволюційного співробітництва академії та промисловості в сфері електронної та обчислювальної техніки, «Model-Oriented Approach and Intelligent Knowledge-Based System for Evolvable Academia-Industry Cooperation in Electronic and Computer Engineering» (2014 – 2016 pp.);

– проєкт Європейського Союзу ERASMUS+ ALIOT (573818-EPP-1-2016-1-UK-EPPKA2-CBHE-JP) Інтернет речей: нова навчальна програма для потреб промисловості та суспільства, «Internet of Things: Emerging Curriculum for Industry and Human Applications» (2016 – 2020 pp.);

– проєкт Європейського Союзу Horizon2020 ECHO «European network of Cybersecurity centres and competence Hub for innovation and Operations», Європейська мережа центрів кібербезпеки та Центр компетенцій для інновацій та управління (2019 – по т.ч.);

в) *виконувалися в рамках «Державної цільової науково-технічної програми впровадження і застосування грід-технологій на 2009-2013 роки»:*

– проєкт «Адаптація ПЗ для радіоастрономічних досліджень для роботи в грід-середовищі та модернізація грід-інфраструктури РІ НАНУ» (Радіоастрономічний інститут НАН України, – № ДР 0111U004497 (2011 р.);

– проєкт «Адаптація грід інфраструктури РІНАНУ до передачі та обробки великих масивів радіоастрономічних даних», – № ДР 0112U004104 (2012 р.);

г) *виконувалися як госпдоговірні науково-дослідні роботи, що фінансувалися за рахунок Державного фонду фундаментальних досліджень*: «Створення науково-методичних основ забезпечення живучості мережевих систем обміну інформацією в умовах зовнішнього впливу потужного НВЧ випромінювання» (Харківський національний університет радіоелектроніки, – № ДР 0117U003916 (2017 р.); № ДР 0118U000832 (2018 р.)).

У відповідності до мети вирішено комплекс наступних завдань:

1. Запропоновано концепцію та принципи забезпечення кібербезпеки індустріальних і веб-орієнтованих систем і мереж.

2. Розроблено модель згорткової нейронної мережі на основі використання змішаних даних та метод виявлення шкідливого програмного забезпечення в операційній системі Android на основі опрацювання викликів прикладного програмного інтерфейсу (API) та набору дозволів.

3. Розроблено методи інформаційної технології забезпечення кібербезпеки веб-орієнтованих систем на основі систем керування вмістом, засновані на оцінюванні схильності до поширених сценаріїв атак та виборі найбільш ефективних засобів захисту.

4. Розроблено моделі та методи забезпечення кібербезпеки віртуальних мереж, засновані на використанні концепції віртуального тунелювання в мережі Інтернет.

5. Розроблено методологічні основи створення інформаційної технології та модель цифрової платформи знань для використання в дуальній системі підготовки фахівців під час здобуття професійних знань.

6. Впроваджено методи технологій забезпечення кібербезпеки індустріальних і веб-орієнтованих систем і мереж.

Наукова новизна одержаних результатів полягає у тому, що:

1. Розроблено концепцію, принципи забезпечення кібербезпеки індустріальних і веб-орієнтованих систем і мереж.

2. Розроблено модель згорткової нейронної мережі на основі використання змішаних даних та метод виявлення шкідливого програмного забезпечення в операційній системі Android на основі опрацювання викликів прикладного програмного інтерфейсу (API) та набору дозволів:

– вперше розроблено модель згорткової нейронної мережі на основі використання змішаних даних, архітектура якої, відрізняється від відомих відсутністю чергування шарів згортки та агрегувальних шарів, що дозволило виділити прості ознаки в згорткових шарах першого рівня для представлення шаблонів поведінки згортковими шарами другого рівня без втрати даних;

– вперше розроблено метод виявлення шкідливого програмного забезпечення в операційній системі Android на основі опрацювання викликів

прикладного програмного інтерфейсу (API) та набору дозволів, який на відміну від відомих залучає модель згорткової нейронної мережі на основі використання змішаних даних, що дозволило підвищити достовірність виявлення шкідливого програмного забезпечення в операційній системі Android у порівнянні із відомими методами.

3. Розроблено методи інформаційної технології забезпечення кібербезпеки веб-орієнтованих систем на основі систем керування вмістом, засновані на оцінюванні схильності до поширених сценаріїв атак та виборі найбільш ефективних засобів захисту:

– вперше одержано метод забезпечення кібербезпеки систем керування вмістом, який базується на виборі контрзаходів з урахуванням їх характеристик і сумісності;

– удосконалено метод оцінювання кібербезпеки систем керування вмістом шляхом використання дерев атак і визначення параметрів базових подій з урахуванням складності їх проведення і виявлення.

4. Розроблено моделі та методи забезпечення кібербезпеки віртуальних мереж, засновані на використанні концепції віртуального тунелювання в мережі Інтернет:

– удосконалено модель віртуальної мережі з темпоральним критерієм диспетчеризації запитів на обслуговування на вузлах, яка базується на використанні зваженої суми часткових середніх взаємних інформацій між конкретним запитом і простором можливих відкликів вузлів віртуальної мережі, що дозволяє здійснювати оперативну обробку найбільш актуальних запитів при створенні віртуальних тунелів;

– вперше запропоновано метод автоматизованої побудови VPN-ланцюгів між кінцевими користувачами віртуальної мережі, який відрізняється від відомих відмовою від використання регіональних ознак вузлів, які є опорними при побудові ланцюга в віртуальній або багатошаровій віртуальній мережі, та перебудовую структури у разі досягнення граничних значень затримки, що дає

виграш у часі на побудову та перебудову структури VPN-ланцюга всередньому на 50%;

– отримала подальший розвиток методика застосування задачі комівояжера з декількома активними агентами, що діють за принципом квест-сценаріїв, для аналізу мережних структур при пошуку уразливих вузлів.

5. Розроблено методологічні основи створення інформаційної технології й модель цифрової платформи знань для використання в дуальній системі підготовки фахівців під час здобуття професійних знань:

– вперше розроблено методологічні основи інформаційної технології для дуальної системи підготовки фахівців, які базуються на комплексі методів і моделей топологічних різноманіть, що забезпечує комплексну інформатизацію процесів здобуття професійних знань;

– вперше розроблено модель цифрової платформи підтримки процесів здобуття професійних знань, у якій на відміну від наявних використовуються моделі професійних знань з основної й суміжних спеціальностей, що дає змогу інтегрувати методичні й змістовні взаємозв'язки в дуальній системі для комплексної підготовки фахівців.

Результати дослідження надали змогу розробити та впровадити моделі, методи та технології забезпечення кібербезпеки мобільних систем, веб-орієнтованих систем на основі систем керування вмістом, віртуальних мереж, що забезпечують їх взаємодію, та методологію підготовки фахівців з кібербезпеки в сфері інформаційних технологій, машинобудуванні, авіаційній промисловості, вищій освіті тощо. Використання результатів досліджень підтверджується актами впровадження розроблених моделей і методів технологій в навчальний процес, сферу інформаційних технологій та науково-дослідну діяльність підприємств індустрії.

Практичне значення одержаних результатів полягає в доведенні теоретичних основ моделей, методів і технологій забезпечення кібербезпеки індустріальних і веб-орієнтованих систем і мереж до їх безпосереднього використання в діяльності підприємств у сфері інформаційних технологій,

машинобудуванні, авіаційній промисловості, а також у закладах вищої освіти під час розробки навчальних курсів і модулів для підготовки фахівців з кібрбезпеки.

На основі одержаних результатів безпосередньо розроблено моделі, методи, технології забезпечення кібербезпеки:

– мобільних систем,

– веб-орієнтованих систем на основі систем керування вмістом,

– віртуальних мереж,

а також методологію підготовки фахівців з кібербезпеки.

Основні результати та рекомендації комплексної наукової роботи реалізовано у наступних підприємствах і установах за галузями:

– у компанії «LineUp», яка спеціалізується на інформаційних технологіях (м. Харків);

– у підприємстві «GMhost» при наданні послуг хостингу з віртуалізації веб-орієнтованих систем (м. Хмельницький);

– у ТОВ «Blackthorn Vision» при розробленні мобільних систем (м. Хмельницький);

– у ТОВ «ІТТ» при тестуванні програмного забезпечення в індустріальних системах передачі даних (м. Хмельницький);

– у ТОВ «ХАКЕН» при наданні рішень із забезпечення кібербезпеки веб-орієнтованих систем (м. Київ);

– у ТОВ «Компанія «Електронний Світ» при провадженні електронної комерції (м. Харків);

– у державному підприємстві «Південний державний проектно-конструкторський та науково-дослідний інститут авіаційної промисловості» при комплексному проектуванні авіаційних підприємств (м. Харків);

– на підприємстві машинобудування АТ «ФЕД» (м. Харків);

– у навчальному процесі в закладах вищої освіти України (Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут», Хмельницького національного університету, Харківського національного університету радіоелектроніки);

– при виконанні міжнародних проєктів за європейськими програмами TEMPUS, ERASMUS+, Horizon2020;

– при виконанні національних проєктів за замовленням Міністерства освіти та науки України у 2011–2020 рр.

Впровадження запропонованих моделей, методів і технологій забезпечення кібербезпеки індустріальних і веб-орієнтованих систем і мереж надало можливість:

– розробити та впровадити рішення, одержані в роботі, у сфері інформаційних технологій, машинобудуванні, авіаційній промисловості, вищій освіті тощо;

– створити та впровадити в навчальний процес для здобувачів першого (бакалаврського), другого (магістерського) та третього (освітньо-наукового – докторів філософії) рівнів вищої освіти низку курсів: «Операційні системи», «Алгоритми та методи обчислень», «ПЗ мікропроцесорних систем (Програмування штучного інтелекту на Python)», «Теорія і методи Інтернет-обчислень», «Адміністрування та налагодження мереж», «Сервісні платформи інформаційних мереж», «Програмні засоби оверлейних комп’ютерних мереж», «Cloud-технології», «Корпоративні комп’ютерні мережі», «Комп’ютерні системи», «Безпека та захист комп’ютерних систем», «Технічна діагностика і надійність комп'ютерних пристроїв та систем», «Штучні імунні системи», а також тренінг-модулі для фахівців з кібербезпеки;

– досягнути значення достовірності виявлення шкідливого програмного забезпечення в операційній системі Android на рівні 0,933% та зменшити показник хибних спрацювань до 3,3%, у порівнянні із відомими методами виявлення шкідливого програмного забезпечення в операційній системі Android;

– забезпечити допустиме значення показника успішності атак при мінімальній вартості й вибрати заходи захисту, враховуючи їх вплив на показник успішності атак та вартість, а саме використання методів на прикладі однієї

інсталяції системи керування вмістом дозволило зменшити значення показника успішності атаки на 42,3%;

– зменшити часові затрати на побудову та перебудову структури віртуальної мережі у разі досягнення граничних значень мережної затримки або компроментації вузлів кіберзлочинцями всередньому на 50%;

– підвищити ефективність підготовки фахівців з кібербезпеки, зокрема експериментальна перевірка свідчить, що абсолютна успішність унаслідок впровадження запропонованої інформаційної технології в навчальний процес, збільшилися на 4%, а якісна успішність – на 14% відповідно.

Апробація результатів дослідження. Основні положення, ідеї, висновки комплексної наукової роботи доповідалися і обговорювалися на 69 міжнародних наукових конференціях і симпозіумах: міжнародній науково-практичній конференції «The Strategies of Modern Science Development» (м. Йєлм, США, 2013 р.), XIV Міжнародній науково-технічній конференції «Современные информационные и электронные технологии» (м. Одеса, 2013 р.), міжнародній науково-технічній конференції «Інформаційні технології в освіті, науці і виробництві» (м. Луцьк, 2013, 2019 рр.), XXI Міжнародній конференції «Computer Networks» (м. Брунув, Польща, 2014 р.), міжнародному молодіжному форумі «Радіоелектроніка та молодь у XXI столітті» (м. Харків, 2014–2018 рр.), міжнародній конференції «Контроль і управління в складних системах» (м. Вінниця, 2014, 2016, 2018, 2020 рр.), IEEE міжнародній науково-практичній конференції «Problems of Infocommunications. Science and Technology» (м. Харків, 2014, 2018 рр.; м. Київ, 2019 р.), III Міжнародній науково-технічній конференції «Обчислювальний інтелект (результати, проблеми, перспективи)» (м. Київ – м. Черкаси, 2015 р.), міжнародній науково-практичній конференції «Проблеми інформатики та комп’ютерної техніки» (м. Чернівці, 2015 р.), всеукраїнській науково-технічній конференції «Інтегровані комп’ютерні технології в машинобудуванні» (м. Харків, 2015-2018 рр.), міжнародній науково-технічній конференції «Проблеми інформатизації» (м. Харків, 2015, 2018 рр.),

X ювілейній міжнародній конференції «Antenna Theory and Techniques» (м. Харків, 2015 р.), IEEE міжнародному молодіжному науковому форумі «Applied Physics» (м. Харків, 2015 р.), міжнародній науково-практичній конференції «Інформаційні технології і мехатроніка: освіта, наука та працевлаштування» (Харків, 2016 р.), міжнародній науково-практичній конференції, присвяченій 50-річчю кафедри земельного адміністрування та геоінформаційних систем Харківського національного університету міського господарства імені О.М. Бекетова (Харків, 2016 р.), І міжнародній науково-практичній конференції «Проблеми науково-технічного та правового забезпечення кібербезпеки у сучасному світі» (м. Харків, 2016 р.), міжнародній науково-технічній конференції «Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління» (м. Полтава – м. Баку – м. Харків – м. Кіровоград, 2016-2019 рр.), міжнародній науково-технічній конференції «International Conference on ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer» (м. Київ, 2016-2018 р., м. Херсон, 2019 р., м. Харків, 2020 р.), студентській науковій конференції «Konferencja Studenckich Kół Naukowych» (м. Краків, Республіка Польща, 2016 р.), міжнародному науково-практичному семінарі молодих вчених та студентів «Програмовані логічні інтегральні схеми та мікропроцесорна техніка в освіті і виробництві» (м. Луцьк, 2016 р.), міжнародній науково-технічній конференції «Электротехнические и компьютерные системы: теория и практика» (м. Одеса, 2016 р.), всеукраїнській науково-практичній конференції «Інтелектуальні системи та прикладна лінгвістика» (м. Харків, 2016 р.), XI міжнародній науково-практичній конференції «Сучасні інформаційні і комунікаційні технології на транспорті, в промисловості та освіті» (м. Дніпро, 2017 р.), міжнародній науково-технічній конференції «Комп'ютерні та інформаційні системи і технології» (м. Харків, 2017-2018 рр.), міжнародній науково-практичній конференції «Інформаційні технології та безпека» (м. Київ, 2017-2019 рр.), IEEE міжнародній конференції «Intelligent Data Acquisition and

Advanced Computing Systems: Technology and Applications (IDAACS)» (м. Бухарест, Румунія, 2017 р.), міжнародній науково-практичній конференції «Modern methods, innovations, and experience of practical application in the field of technical sciences» (м. Радом, Республіка Польща, 2017 р.), IX міжнародній науково-практичній конференції «Dependable Systems, Services and Technologies» (м. Київ, 2018 р.), I Міжнародній науково-практичній конференції IT-професіоналів та аналітиків комп'ютерних систем, присвяченій 50-річчю кафедри інформатики ХАІ «ProfIT Conference» (м. Харків, 2018 р.), міжнародній науково-практичній Internet-конференції «Моделювання та інформаційні технології в науці, техніці та освіті» (м. Харків, 2018 р.), 73-й науково-технічній конференції професорсько-викладацького складу, науковців, аспірантів та студентів ОНАЗ ім. О.С. Попова (м. Одеса, 2018 р.), II IEEE міжнародній конференції «Data Stream Mining & Processing» (м. Львів, 2018 р.), III міжнародній конференції «Computational Linguistics and intelligent systems» (м. Харків, 2019 р.), всеукраїнській конференції студентів та молодих науковців «Інтелектуальний потенціал 2019» (м. Хмельницький, 2019 р.), VIII IEEE міжнародній конференція «Advanced Optoelectronics and Lasers» (Scientific Workshop on Data Science in Modern Optoelectronics and Laser Engineering) (м. Созопол, Болгарія, 2019 р.), I IEEE міжнародній конференції «Advanced Trends in Information Theory» (м. Київ, 2019 р.).

Наукові результати роботи доповідалися також на постійно діючому науково-технічному семінарі «Критичні комп'ютерні технології та системи», що проводиться на кафедрі комп'ютерних систем, мереж і кібербезпеки Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут» (2011–2020 рр.).

Загальна кількість публікацій за науковою працею – **145**. З них **6** монографій, **48** наукових статей у збірниках, що включені до переліку наукових фахових видань України, **4** статті в збірниках, що входять до наукометричних баз даних, **4** статті в міжнародних журналах, **24** публікацій в матеріалах

конференцій, що входять до наукометричних баз даних, **45** публікацій у матеріалах конференцій, тезах доповідей та виданнях, що не включені до переліку наукових фахових видань України, **8** патентів на корисну модель, **2** свідоцтва на авторський твір, **4** навчальних посібників.

_____ /О. І. Морозова/

(підпис)

_____ /А. О. Нічепорук/

(підпис)

_____ /А. Г. Тецький/

(підпис)

_____ /В. М. Ткачов/

(підпис)

Учений секретар університету С. Є. Чмихун

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ * Національний аерокосмічний університет ім. М.Є. Жуковського "Харківський авіаційний інститут" * №02066769

20