Вісник Національного університету “Львівська політехніка”. Серія: “Юридичні науки”
№ 4 (48), 2025 ISSN 2415-3818 (print); ISSN 3041-122X (online)

УДК 349.2

Володимир ОРТИНСЬКИЙ
Національний університет “Львівська політехніка”,
Директор Навчально-наукового інституту
права, психології та інноваційної освіти,
доктор юридичних наук, професор,
Заслужений юрист України
volodymyr.l.ortynskyi@lpnu.ua
ORCID: 0000-0001-9041-6330

ОСОБЛИВОСТІ ВИКЛАДАННЯ ІНФОРМАЦІЙНИХ ДИСЦИПЛІН: ІНТЕГРАЦІЯ ЗНАНЬ ПРО БЕЗПЕКУ ІНФОРМАЦІЙНИХ СИСТЕМ ТА КОМПЛЕКСІВ

http://doi.org/10.23939/law2025.48.001

У статті розглядаються актуальні виклики та концептуальні підходи до викладання інформаційних дисциплін із інтеграцією знань про безпеку інформаційних систем та комплексів у вищій освіті. З огляду на стрімкий розвиток цифрових технологій, хмарних сервісів, автоматизованих систем управління та зростання кіберзагроз, зокрема гібридного впливу, особливої ваги набуває проблема формування у студентів цілісного бачення як принципів побудови інформаційних систем, так і їхнього ефективного захисту. У роботі наголошується на необхідності міждисциплінарного підходу до підготовки майбутніх ІТ-фахівців, де поєднуються технічні, інженерні, математичні й безпекові компоненти навчання.

Аналізуються приклади реалізації сучасних освітніх методик, зокрема eduScrum та STEM-орієнтованих проєктів, що впроваджувалися в межах ініціатив CRDF Global. Розкрито практичну значущість проєктів із автентифікації пристроїв на основі унікальних фізичних параметрів та програм з кібергігієни, які були спрямовані на студентів різних спеціальностей. Продемонстровано, як інтеграція гнучких форм навчання, гейміфікації та командної роботи сприяє формуванню в здобувачів освіти професійних компетентностей у сфері кібербезпеки.

Зроблено висновок про доцільність розробки міждисциплінарних програм, що базуються на поєднанні теорії та практики, а також визначено ключові чинники, які забезпечують ефективність підготовки: участь у реальних проєктах, методологічне оновлення курсів та підтримка академічної автономії студентів.

Ключові слова: Інформаційна безпека, кібербезпека, національна безпека, кіберзагроза, кібертероризм, CRDF Global, STEM-освіта, eduScrum.

Постановка проблеми. Стрімкий розвиток цифрових технологій, активне впровадження автоматизованих систем управління, розширення кіберпростору та хмарних сервісів зумовили зростання ролі інформаційної безпеки як критичного елементу функціонування державних, корпоративних і особистих інформаційних систем [1, с. 6]. Відповідно, потреба у фахівцях, здатних не лише

розробляти та експлуатувати інформаційні системи, а й ефективно захищати їх від внутрішніх і зовнішніх загроз, набуває першочергового значення. Це актуалізує питання змістового оновлення та методичного вдосконалення викладання інформаційних дисциплін у закладах вищої освіти.

Сучасна освітня парадигма потребує міждисциплінарного підходу, в межах якого навчання з інформаційних технологій має поєднуватися з формуванням знань і практичних навичок у сфері інформаційної безпеки. Проте на практиці часто спостерігається фрагментарність подачі цих компонентів, що ускладнює формування у студентів цілісного бачення загроз та захисних механізмів. У зв'язку з цим постає проблема інтеграції знань про безпеку інформаційних систем та комплексів у процес викладання інформаційних дисциплін як необхідної умови підготовки конкурентоспроможних ІТ-фахівців.

Аналіз дослідження проблеми. Оскільки дана проблема виникла порівняно недавно, теоретичних напрацювань в даному напрямку поки мало. Проте певні аспекти цього питання розглядали Т. А. Васильєва, М.Т. Гаврильців, Я.П. Мазур, І.М. Сопілко та ін.

Мета статті. Зважаючи на вище викладене, мета дослідження полягає у виявленні та науковому обґрунтуванні ефективних підходів до викладання інформаційних дисциплін із урахуванням необхідності інтеграції знань про безпеку інформаційних систем і комплексів. Дослідження спрямоване на аналіз сучасного стану методик навчання, виявлення недоліків існуючих програм та розробку рекомендацій щодо формування міждисциплінарної моделі підготовки фахівців, яка б забезпечувала формування в студентів цілісного уявлення про принципи побудови, функціонування та захисту інформаційних систем в умовах зростаючих кіберзагроз.

Виклад основного матеріалу. В умовах становлення інформаційного суспільства, де переважна частина працездатного населення залучена до сфери обігу, обробки та створення інформації, спостерігається інтенсивний розвиток інноваційних механізмів досягнення політичних, економічних та інших цілей саме через інформаційний вплив. У зв'язку з цим провідні країни світу в межах своїх систем національної безпеки приділяють значну увагу формуванню та впровадженню всебічних стратегій, які охоплюють політичну, воєнну, економічну, соціальну та інформаційну компоненти. Водночас пріоритетна роль відводиться інформаційній складовій, що слугує основою для стабільного та ефективного функціонування усіх інших напрямів стратегічного розвитку.

Протягом останніх десятиліть значущість інформаційної безпеки невпинно зростає. Інформаційні ресурси дедалі більше відіграють ключову роль у формуванні державної політики, розробці новітніх видів озброєння, проведенні інформаційно-психологічних кампаній, а також у забезпеченні бойової готовності як національних, так і партнерських військових формувань [2, с. 200-201].

Класичне уявлення про «тотальну війну», яка передбачала масове застосування збройної сили, втрачає свою актуальність в умовах трансформації форм міжнародного протиборства. На зміну жорстким силовим методам приходять більш витончені способи досягнення політичних, економічних і геостратегічних цілей, що ґрунтуються на маніпуляції інформаційними потоками, впливі на масову свідомість, дестабілізації суспільств через інфопростір.

Так звані «цивілізовані» війни, у яких головна ставка робиться не на бойову техніку, а на комунікаційні технології, перетворилися на домінантну модель сучасного конфлікту. В епоху цифровізації «нетрадиційні» загрози – зокрема, інформаційні війни, кампанії дезінформації, кібератаки – стали ключовими інструментами реалізації національних інтересів для глобальних акторів. Для України, яка має вразливе геополітичне положення і межує з агресивними інформаційними впливами, ці виклики набули системного характеру. Постійний інформаційно-психологічний тиск створює умови для її втягнення у багатовимірне інформаційне протистояння, що вимагає відповідної державної стратегії у сфері інформаційної безпеки [3, с. 600-601].

Питання забезпечення інформаційної безпеки в сучасному глобалізованому світі набуває критично важливого значення, особливо для держав, що перебувають у стані зовнішнього тиску чи збройної агресії. Конституція України у статті 17 прямо визначає, що захист інформаційного простору прирівнюється до оборони суверенітету, територіальної цілісності та економічної стабільності країни [4], що свідчить про конституційно закріплений статус інформаційної безпеки як пріоритетного напряму державної політики.

У межах національної безпеки інформаційна складова виступає як самостійний вектор захисту та водночас як елемент, що інтегрується з воєнною, економічною, енергетичною та гуманітарною безпекою. Сучасна державна політика в цій сфері передбачає формування цілісної системи заходів, спрямованих на розвиток вітчизняної інформаційної інфраструктури, захист стратегічно важливих даних, протидію деструктивним впливам та кіберзагрозам. Усе це особливо актуально в умовах гібридної війни, коли інформаційна сфера стає полем першого удару. Інформаційні ресурси, цифрові технології та мережі перетворюються на основу інноваційного поступу держави, її міжнародного авторитету та стійкості до зовнішніх впливів [5, с. 12-16].

Проблематика кібербезпеки на сучасному етапі набуває особливої актуальності. Згідно зі Стратегією кібербезпеки України, затвердженою Указом Президента від 26 серпня 2021 року, кібербезпека офіційно визнана одним із ключових пріоритетів державної політики. У цьому документі кіберпростір розглядається як повноправна сфера воєнного протиборства, де поряд із забезпеченням захисту об’єктів критичної інфраструктури передбачено можливість здійснення превентивних кібероперацій наступального характеру [6].

Такий підхід відображає нову воєнно-стратегічну реальність, у якій інформаційні технології використовуються не лише для оборони, а й для активного впливу на противника. Однією з найсерйозніших і системних загроз у цій сфері залишається деструктивна політика російської федерації, яка широко застосовує кібератаки та інформаційно-психологічні впливи як частину ширшої гібридної війни проти України та інших демократичних держав.

Стрімкий прогрес засобів масової інформації, розвиток цифрових технологій і розширення інформаційної інфраструктури значно підвищили масштаби та ефективність сучасного інформаційного протистояння. Сьогодні значна частина конфліктів переміщується у кіберпростір, де інформація перетворюється на стратегічний інструмент політичного тиску та економічного впливу. В умовах інформаційної епохи впливовість держави дедалі більше визначається не лише рівнем її економічного розвитку чи військової потуги, а й здатністю активно діяти у сфері інформаційних комунікацій.

Геополітична перевага все частіше досягається через формування вигідних світоглядних моделей, вплив на ментальність суспільств інших країн, маніпуляцію масовою свідомістю та системне підривання ідеологічних засад противника. Таким чином, інформаційна перевага стає визначальним чинником міжнародного впливу та безпеки в новітніх умовах глобального протиборства.

Становлення інформаційного суспільства, розширення глобального інформаційного середовища та розвиток кіберпростору стали визначальними чинниками сучасної цивілізаційної динаміки. Водночас ці процеси породили низку новітніх загроз, серед яких особливо небезпечними є кіберзлочинність, кібертероризм та інформаційні війни [7, с. 68-69]. Ефективна протидія цим викликам вимагає наявності фахівців нового покоління – компетентних, технічно обізнаних, здатних забезпечувати надійний захист цифрових інфраструктур і стратегічно важливої інформації, водночас відстоюючи національні інтереси України у цифровому середовищі. У зв’язку з цим питання підготовки професійних кадрів у сфері інформаційної та кібербезпеки набуло статусу одного з пріоритетних напрямів державної політики. Навчальні заклади вищої освіти формують у здобувачів знання, уміння та практичні навички, необхідні для служби в таких державних структурах, як Служба безпеки України, Міністерство оборони, Державна служба спеціального зв’язку тощо.

Навчальні посібники, спрямовані на підготовку фахівців у сфері кібербезпеки, відіграють важливу роль у системі вищої освіти, виступаючи не лише джерелом знань, а й інструментом реалізації державних ініціатив у сфері кіберзахисту. Вони суттєво сприяють формуванню кадрового потенціалу, здатного ефективно реагувати на сучасні інформаційні загрози та забезпечувати належний рівень безпеки в цифровому середовищі.

У процесі підготовки майбутніх фахівців з кібербезпеки доцільно спиратися на концептуальні моделі розвитку інтелектуальних і когнітивних навичок, зокрема Тріархічну теорію інтелекту Р. Стенберга та таксономію освітніх цілей Б. Блума. Застосування тріархічної моделі дозволяє інтегровано розвивати у студентів аналітичні здібності, креативність і практичну компетентність, особливо через роботу в команді. Таксономія Блума, у свою чергу, забезпечує ефективне структурування навчального процесу залежно від рівня когнітивної складності та орієнтації на вирішення реальних проблем [8, 4]. Зазначені підходи до навчання були ефективно впроваджені в межах низки міжнародних освітніх ініціатив, у яких брали участь студенти як технічних, так і гуманітарних спеціальностей.

Важливі результати, були отримані під час реалізації проєктів, що здійснювалися за підтримки організації CRDF Global − незалежної некомерційної інституції, яка сприяє розвитку міжнародного науково-технічного партнерства шляхом надання грантів, освітніх програм, експертної підтримки та спеціалізованих сервісів [9].

Одним із показових науково-дослідних проєктів, що реалізовувався за участю викладачів і студентів, стала розробка методів підвищення захисту пристроїв обробки інформації - зокрема комп'ютерів, планшетів і мобільних телефонів − шляхом застосування автентифікації, заснованої на унікальних фізичних характеристиках пристрою, що формуються ще на етапі виробництва. Йдеться про використання внутрішнього електричного шуму, властивого кожному пристрою, як своєрідного «електронного відбитка», що дозволяє точно ідентифікувати пристрій без залучення додаткових апаратних засобів. Такий підхід істотно підвищує надійність автентифікації, зменшуючи ризики компрометації доступу.

Особливу цінність цей проєкт має з точки зору освітнього процесу, оскільки поєднав усі складові STEM-освіти. Студенти вивчали фізичну природу сигналів (наука), застосовували технічні засоби збору даних через аудіокарти (технології), створювали програмні модулі обробки та передачі інформації (інженерія), а також аналізували сигнали методами математичної статистики (математика) [10]. Такий інтегрований підхід не лише сприяв засвоєнню теоретичних знань, а й формував у майбутніх фахівців практичні навички у сфері кібербезпеки, що відповідає актуальним потребам галузі.

Іншим прикладом успішної ініціативи, став освітній проєкт, спрямований на формування базових навичок кібергігієни. Участь у ньому взяли студенти, які навчаються за спеціальностями, не пов'язаними безпосередньо з інформаційною або кібербезпекою, проте для яких обізнаність у цифровій безпеці є важливою у повсякденному та професійному житті. Навчальний процес було організовано у формі ігрового моделювання реальних ситуацій: учасники мали змогу аналізувати наслідки власних дій у цифровому середовищі − зокрема, на персональних комп'ютерах, смартфонах та ноутбуках − а по завершенні виконували тестові завдання для закріплення знань [9].

Для стимулювання когнітивної залученості студентів і розвитку командної взаємодії в межах цього проєкту було впроваджено методологію Scrum − гнучкий підхід до організації колективної роботи, що дозволив покращити ефективність навчання через поетапне планування, зворотний зв'язок і рефлексію [11].

Інтерес до впровадження гнучких методів управління проєктами в освітній процес зумовив появу адаптованої методики eduScrum, що поєднує педагогічні цілі з принципами Scrum. Цей підхід був розроблений у Нідерландах і з 2015 року активно застосовується в навчальних закладах різного рівня, зокрема у середніх школах та університетах. Практичний досвід використання eduScrum засвідчив його ефективність: за даними спостережень, успішність студентів, які навчаються за цією методикою, підвищується в середньому на 20 % порівняно з традиційними формами навчання [12].

Ключовою ідеєю eduScrum є передача студентам частини відповідальності за власне навчання. Це відповідає принципам гнучкої (agile) організації: метод визначає, що і навіщо необхідно зробити, але надає учасникам свободу в обранні способів реалізації. Структура eduScrum передбачає наявність чітких ролей (наприклад, скрам-майстер), регулярних подій (щоденні стендапи, ретроспективи), а також встановлених правил командної взаємодії [13]. Методика ефективно працює в технічних дисциплінах, таких як інженерія, програмування мікроконтролерів Arduino, створення віртуальних лабораторій, розробка інтерактивних курсів на платформі Moodle, зокрема з JavaScript, тощо.

Таким чином, eduScrum формує середовище, в якому навчання перетворюється на динамічний процес із чіткими цілями, постійною комунікацією та глибоким залученням студентів.

Освітній процес XXI століття повинен динамічно трансформуватися відповідно до викликів сучасної економіки та високотехнологічного виробництва. Саме такі методики, як eduScrum, стимулюють розвиток ініціативності, самостійності та відповідальності у студентів, формуючи в них навички, необхідні для успішної адаптації в умовах реального ринку праці та професійної діяльності.

Участь студентів у проєктах, підтримуваних організацією CRDF Global, стає вагомим кроком до поглиблення розуміння актуальних питань у сфері кібербезпеки, адже під час досліджень вони можуть ознайомлюватися з інноваційними підходами до захисту інформаційних систем, зокрема з використанням індивідуальних фізичних характеристик пристроїв як своєрідної «цифрової біометрії» для створення унікальних, складних ключів автентифікації. Цей підхід значно підвищує стійкість систем до несанкціонованого доступу.

Практичні результати доводять, що навіть зовні ідентичні серійні пристрої мають незначні відмінності на рівні апаратних компонентів, спричинені технологічними допусками під час виробництва, що й дозволяє їх ідентифікувати з високою точністю.

Висновки. Отже, проведений аналіз засвідчує, що інтеграція знань про безпеку інформаційних систем у процес викладання інформаційних дисциплін є не лише доцільною, а й вкрай необхідною умовою підготовки фахівців нового покоління. Досвід міжнародної освітньої практики, зокрема використання таких інноваційних методик, як eduScrum, переконливо доводить: активні, гнучкі форми навчання сприяють не лише покращенню академічних результатів, але й формують у здобувачів освіти важливі професійні якості − самостійність, мобільність, адаптивність до нових умов, готовність до постійного професійного зростання.

Ефективна підготовка спеціалістів у сфері інформаційної безпеки потребує комплексного підходу, що поєднує теоретичну підготовку з практичною реалізацією знань у проєктах, активне використання гейміфікації, розвиток навичок командної роботи, критичного мислення та управління проєктами. Лише через системне оновлення освітніх програм з урахуванням технологічного поступу й новітніх загроз Україна зможе забезпечити належний рівень кіберзахисту та виховати фахівців, здатних ефективно діяти в умовах глобального інформаційного протистояння

Подяки. Немає.

Фінансування. Автор заявляє про відсутність фінансової підтримки для проведення досліджень чи публікації цієї статті.

Внесок автора. Автор підтверджує свою виключну відповідальність за цю роботу.
Автор схвалює цю роботу і бере на себе відповідальність за її цілісність.

Конфлікт інтересів. Автор заявляє про відсутність конфлікту інтересів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Цифрові технології в освіті: сучасний досвід, проблеми та перспективи: монографія /Т. А. Васильєва та ін.; за заг. ред. д-рки екон. наук, проф. Т. А. Васильєвої, д-ра екон. наук, проф. Ю. М. Петрушенка. Суми: Сумський державний університет, 2022. 150 с.

2. Гаврильців М.Т. Інформаційна безпека держави в системі національної безпеки України. *Юридичний науковий електронний журнал*. № 2/2020. С. 200−203.

3. Мазур Я.П. Основні кіберзагрози в умовах ведення інформаційної війни. *Аналітично-порівняльне правознавство*. № 6. 2024. С. 599−604.

4. Конституція України від 28.06.1996 № 254к/96-ВР. *Відомості Верховної Ради України (ВВР)*, 1996, № 30, ст. 141.

5. Кіберкультура та кібербезпека в умовах війни: психологічний практикум: практичний посібник /Юлія Чаплінська; Національна академія педагогічних наук України, Інститут соціальної та політичної психології. Київ, 2023. 80 с.

6. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України від 26.08.2021 № 447/2021. *База даних "Законодавство України" / ВР України*. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (Дата звернення: 30.04.2025).

7. Сопілко І.М. Становлення інформаційного суспільства та інформаційні загрози в мережі інтернет. *Юридичний вісник*. № 3 (44) 2017. С. 61−69.

8. Hamman S.T., Hopkinson K.M. Teaching Adversarial Thinking for Cybersecurity. *J. Colloq. Inf. Syst. Secur. Educ*. (CISSE) 4, 2016. pp. 1–19.

9. CRDF Global. URL: https://www.crdfglobal.org/ (Дата звернення: 10.05.2025).

10. STEM-освіта. URL: https://imzo.gov.ua/stem-osvita/ (Дата звернення: 10.05.2025).

11. Що таке методологія Scrum і коли варто її використовувати. URL: https://career.softserveinc.com/uk-ua/stories/what-is-scrum-methodology (Дата звернення: 12.05.2025).

12. eduScrum. URL: https://eduscrum.org/ (Дата звернення: 12.05.2025).

13. Методика EDU-SCRUM в освіті. URL: https://osvitanova.com.ua/posts/989-metodyka-edu-scrum-v-osviti (Дата звернення: 12.05.2025).

REFERENCES

1. Digital technologies in education: modern experience, problems and prospects: monograph T. A. Vasylieva ta in.; za zah. red. d-rky ekon. nauk, prof. T. A. Vasylievoi, d-ra ekon. nauk, prof. Yu. M. Petrushenka. Sumy: Sumskyi derzhavnyi universytet, 2022, 150 p. [In Ukrainian].

2. Havryltsiv M.T. Information security of the state in the system of national security of Ukraine. *Yurydychnyi naukovyi elektronnyi zhurnal.* No 2/2020, p. 200–203. [In Ukrainian].

3. Mazur Ya.P. Main cyber threats in the conditions of information warfare. *Analitychno-porivnialne pravoznavstvo.* No 6, 2024, pp. 599–604. [In Ukrainian].

4. Constitution of Ukraine from June 28, 1996 No 254k/96-VR. *Vidomosti Verkhovnoi Rady Ukrainy (VVR)*, 1996, No 30, p. 141. [In Ukrainian].

5. Cyberculture and cybersecurity in wartime: psychological workshop: practical guide Yuliia Chaplinska; Natsionalna akademiia pedahohichnykh nauk Ukrainy, Instytut sotsialnoi ta politychnoi psykholohii. Kyiv, 2023, 80 p. [In Ukrainian].

6. On the Decision of the National Security and Defense Council of Ukraine of May 14, 2021 "On the Cybersecurity Strategy of Ukraine": Decree of the President of Ukraine of August 26, 2021, No. 447/2021. Retrieved from: https://zakon.rada.gov.ua/laws/show/447/2021#Text (Accessed: 30.04.2025) [In Ukrainian].

7. Sopilko I.M. Formation of the information society and information threats on the Internet. *Yurydychnyi visnyk.* No 3 (44), 2017, pp. 61–69. [In Ukrainian].

8. Hamman S.T., Hopkinson K.M. Teaching Adversarial Thinking for Cybersecurity. *J. Colloq. Inf. Syst. Secur. Educ. (CISSE),* No 4, 2016, pp. 1–19. [In English].

9. CRDF Global. Retrieved from: https://www.crdfglobal.org/ (Accessed: 10.05.2025) [In English].

10. STEM-osvita [STEM-education]. Retrieved from: https://imzo.gov.ua/stem-osvita/ (Accessed: 10.05.2025) [In Ukrainian].

11. What is Scrum methodology and when it should be used. Retrieved from: https://career.softserveinc.com/uk-ua/stories/what-is-scrum-methodology(Accessed: 12.05.2025) [In Ukrainian].

12. eduScrum. Retrieved from: https://eduscrum.org/ (Accessed: 12.05.2025) [In English].
13. EDU-SCRUM methodology in education. Retrieved from: https://osvitanova.com.ua/posts/989-metodyka-edu-scrum-v-osviti (Accessed: 12.05.2025) [In Ukrainian].

Отримано: 24.07.2025
Прорецензовано: 02.09.2025
Схвалено до друку: 29.09.2025
Опубліковано (онлайн): 12.12.2025
Надруковано: 26.12.2025

Volodymyr ORTYNSKYI
Lviv Polytechnic National University,
Director of the Educatioal and Rasearch Institute of Law,
Psychology and Innovative Education,
Dr. habil. (Law), Professor,
Honoured Lawyer of Ukraine
volodymyr.l.ortynskyi@lpnu.ua
ORCID: 0000-0001-9041-6330

FEATURES OF TEACHING INFORMATION DISCIPLINES: INTEGRATION OF KNOWLEDGE ABOUT THE SECURITY OF INFORMATION SYSTEMS AND COMPLEXES

The article discusses current challenges and conceptual approaches to teaching information disciplines with the integration of knowledge about the security of information systems and complexes in higher education. Given the rapid development of digital technologies, cloud services, automated control systems, and the growth of cyber threats, in particular hybrid influence, the problem of forming a holistic vision among students of both the principles of building information systems and their effective protection is becoming particularly important. The paper emphasizes the need for an interdisciplinary approach to training future IT specialists, combining technical, engineering, mathematical, and security components of education.

Examples of the implementation of modern educational methods, in particular eduScrum and STEM-oriented projects, which were implemented within the framework of CRDF Global initiatives, are analyzed. The practical significance of projects for device authentication based on unique physical parameters and cyber hygiene programs aimed at students of various specialties is revealed. It demonstrates how the integration of flexible forms of learning, gamification, and teamwork contributes to the development of professional competencies in the field of cybersecurity among students.

The conclusion was made about the feasibility of developing interdisciplinary programs based on a combination of theory and practice, and the key factors that ensure the effectiveness of training were identified: participation in real projects, methodological updating of courses, and support for academic autonomy of students.

Keywords: Information security, cybersecurity, national security, cyber threat, cyberterrorism, CRDF Global, STEM education, eduScrum.