УДК 372.851

к.т.н., доц. **Гайша О.О.** (НУК)
Ряба Л.О. (ВІ КНУ)

ОСОБЛИВОСТІ МЕТОДИКИ ВИКЛАДАННЯ ДИСЦИПЛІНИ «МАТЕМАТИЧНІ МЕТОДИ МОДЕЛЮВАННЯ ТА ОПТИМІЗАЦІЇ ПРОЦЕСІВ КІБЕРБЕЗПЕКИ» З ВИКОРИСТАННЯМ СУЧАСНИХ КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ

У статті розглядається проблема інтенсифікації зусиль студентів, направлених на вивчення матеріалу з дисципліни «Математичні методи моделювання та оптимізації процесів кібербезпеки». В статті основна увага приділена «комп'ютеризації» предмету: як в частині моделювання саме комп'ютерних систем (захисту інформації), так і шляхом ширшого їх використання для моделювання та оптимізації. Значна увага приділена моделюванню систем масового обслуговування; пропонується аналогічним способом вести моделювання довільних процесів галузі кібербезпеки, а не обов'язково масового обслуговування (як приклад, розглядається процес авторизації користувача у комп'ютерній системі). Підкреслюється, що важливу роль у моделюванні грають статистичні методи, як, наприклад, регресійний аналіз (одно- та багатовимірний). Чимала увага приділена порівнянню результатів вирішення однієї і тієї ж самої задачі, отриманих різними способами (аналітично, чисельно, обробкою експериментальних даних). Стаття може бути корисною для здобувачів вищої освіти відповідних спеціальностей та викладачів.

Ключові слова: кібербезпека, математичне моделювання, оптимізація, комп'ютерні інформаційні технології.

Постановка проблеми. Спеціальність «Кібербезпека» вперше з'явилася у переліку спеціальностей України у 2015 році [1] і позиціонується як заміна (об'єднання) групи спеціальностей «Системи захисту інформації», «Інформаційна безпека держави», «Забезпечення державної безпеки України», тощо [2].

У порівнянні з багатьма іншими технічними спеціальностями, що розвиваються уже протягом тривалих проміжків часу, «Кібербезпека» (та споріднені напрями) з'явилася зовсім недавно. Фактично її розвиток можна прив'язати до процесу виникнення та еволюції комп'ютерної техніки та мережевих технологій. Звичайно, не слід відкидати тривалий розвиток цієї галузі в частині використання технічних засобів захисту інформації, зокрема від витоку по аудіо та відео каналу (наприклад, безперечно заслуговує уваги дослідження численних рішень, спрямованих на боротьбу із закладними пристроями). Накопичено величезний досвід створення систем саме інженерного захисту (як, наприклад, обмежувальних стін, решіток, сигналізацій, систем контролю доступу, і т.і.) ще задовго до масового поширення комп'ютерної техніки та, тим більше, комп'ютерних мереж. Але, не зважаючи на ці очевидні факти, все ж слід визнати, що перехід до нової назви спеціальності вплинув на розстановку акцентів, що завжди існують при вивченні таких обширних галузей знань, якою є і кібербезпека. Тепер питання інженерного захисту поступово відходять на другий план, звільняючи місце для ширшого вивчення питань комп'ютерного захисту.

Відповідно, виникає задача перерозподілу навчального матеріалу у наявних дисциплінах загальної спрямованості, якою є, зокрема, «Математичні методи моделювання та оптимізації процесів кібербезпеки»: необхідно приділити більшу увагу методам та засобам, пов'язаним із комп'ютерною технікою та мережами. Окрім ширшого моделювання та прикладів оптимізації систем саме комп'ютерного захисту, є доцільним також якомога повніше впровадження наявної в учбовому закладі комп'ютерної техніки. В першу чергу, це необхідно для створення у студентів комп'ютерного «духу», спрямованості на останні досягнення технологій, підтримання статусу сучасного навчального закладу із відповідно організованим процесом навчання.

Аналіз попередніх досліджень. У вільному доступі наявні численні науково-методичні матеріали для дисципліни «Математичні методи моделювання та оптимізації» без урахування специфіки галузі кібербезпеки, (наприклад, [3-5]. Безперечно, ці відомості можуть бути адаптовані до курсу, що розглядається, але в той же час аргументовано мають бути враховані і його особливості. Саме на вирішення цього питання направлена дана стаття. Що ж стосується готових рішень саме з дисципліни «Математичні методи моделювання та оптимізації процесів кібербезпеки», то вони у вільному доступі відсутні: ймовірно, у великій мірі ця обставина має місце через вказану вище новизну всієї концепції даної спеціальності, а також і через її специфіку, що враховує захист інформації, збереження її у певній таємниці, що, очевидно, переноситься і на науково-методичні матеріали з окремих предметів.

Відповідно до вищенаведених тез, можна сформулювати наступну мету даної роботи.

Мета статті: проаналізувати особливості курсу «Математичні методи моделювання та оптимізації процесів кібербезпеки» на предмет якомога інтенсивнішого впровадження комп'ютерних інформаційних технологій і надати рекомендації по їх моделюванню та оптимізації.

Основний матеріал дослідження. Зважаючи на специфіку сучасних систем захисту інформації серед існуючих засобів для їх математичного моделювання можна виділити два основні класи: методи символьного моделювання та графічного. Символьні (знакові) моделі об'єктів та процесів кібербезпеки можуть будуватися на основі використання:

- диференціальних рівнянь;
- алгебраїчних рівнянь;
- логічних рівнянь та умов;
- спеціальних мов (наприклад, GPSS – мови моделювання систем загального призначення);
- досягнень теорії ймовірностей та математичної статистики.

Серед засобів та методів графічного моделювання можна назвати наступні:

- теорія графів;
- блок-схеми алгоритмів;
- процес-суб'єкт-об'єктні схеми;
- діаграми потоків даних DFD;
- діаграми сутність-зв'язок ERD;
- інші діаграми з галузі CASE-технологій;
- уніфікована мова моделювання UML;
- тощо.

Часто зустрічаються комбінації символьного та графічного підходів, як, наприклад, при моделюванні систем масового обслуговування (далі – СМО): граф станів та система рівнянь Колмогорова. Особливо корисним тут також є моделювання мовою GPSS, що являє студентам ще один корисний, сучасний (і, навіть, «модний») інструмент по дослідженню СМО.

Слід відмітити, що математичний та графічний опис СМО при деякому узагальненні застосовний не лише до систем масового обслуговування, а й до опису практично будь-якого процесу, що розбивається на сукупність окремих станів, переходи між якими можна оцінити певними ймовірностями (таких процесів можна будувати у галузі кібербезпеки дуже багато). Зобразивши такі стани на графі і показавши усі можливі варіанти переходів між станами (необов'язково лише між двома сусідніми, як у СМО), можна записати систему диференціальних рівнянь Колмогорова, а, отже, за умови можливості її розв'язку, і знайти ймовірності станів та усі супутні відомості.

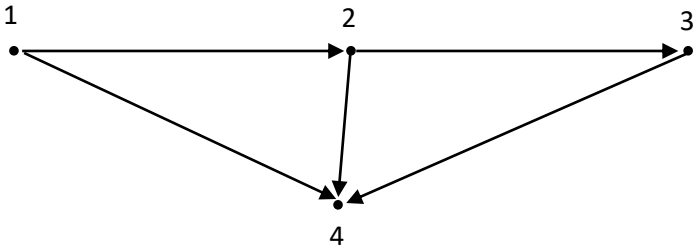
Прикладом процесу, що може моделюватися як робота СМО, є авторизація користувача (див. рис.). Окремими станами будуть наступні ситуації:

1 – користувач бачить екран-запрошення до введення свого імені;

2 – користувач бачить екран-запрошення до введення паролю;

3 – користувач потрапив до системи;

4 – користувачеві видано екран-попередження про необхідність повторної авторизації.



Переходи є наступними:

1-2 – користувач вводить ім’я, що наявне у базі даних;

2-3 – користувач вводить пароль, що відповідає раніше введеному імені;

1-4 – користувач вводить ім’я, якого немає у базі даних;

2-4 – користувач вводить пароль, що не відповідає раніше введеному імені;

3-4 – закінчився час сесії (за умови, що вона є обмеженою у часі), і слід заново ввести ім’я та пароль.

Особливістю комп’ютерних систем, їх суттєвою відмінністю від систем інженерного захисту є дискретність, що проявляється у переважній більшості усіх прикладних задач. Так, потоки інформації зазвичай мають розглядатися як дискретні сутності, тому для їх описання можуть застосовуватися не диференціальні, а рівняння у скінченних різницях. За наявності такої можливості дискретний потік (в першу чергу при його високій інтенсивності) може моделюватися як неперервний, що вносить певну похибку, але дозволяє працювати із більш звичними диференціальними рівняннями, які оперують неперервними змінними.

Алгебраїчні рівняння, якщо не використовуються як самостійний елемент, то можуть бути отримані із систем диференціальних рівнянь (далі - СДР) при розгляді стаціонарного режиму роботи об’єкта, який описує СДР. При цьому усі похідні перетворюються на нуль і система рівнянь значно спрощується – перетворюється на алгебраїчні. Корисно проілюструвати студентам як трудомісткий повний розв’язок однієї і тієї ж СДР аналітичним способом (в результаті чого отримують функціональні залежності для шуканих величин), так і «швидкий» розв’язок системи для стаціонарного режиму. Обов’язково слід порівняти асимптотичні значення, до яких наближаються знайдені функціональні залежності при необмеженому зростанні часу, та стаціонарні ймовірності станів, отримані із алгебраїчної системи. Також дуже корисним є чисельний розв’язок тієї ж СДР (навіть і найпростішим методом Ейлера) з подальшим обов’язковим порівнянням результатів аналітичного та чисельного розв’язків. Отже повне дослідження СДР має виглядати наступним чином:

- розв’язок аналітичним способом, в результаті чого слід отримати функціональні залежності для шуканих величин $x_i(t)$;
- розв’язок системи чисельним методом і порівняння розв’язків, наприклад, графічно;
- розв’язок алгебраїчної системи, що відповідає СДР, та порівняння отриманих розв’язків з асимптотичними значеннями;
- якщо існує така можливість, слід порівняти результати моделювання (вищеозначеними способами) з експериментальними даними, що описують реальний процес.

Для встановлення певних залежностей (однієї важливої з точки зору захисту інформації величини від іншої) можна застосовувати методи такої частини математичної статистики, як регресійний аналіз. Наприклад, величини побічного електромагнітного випромінювання та наводок на границі контрольованої зони прямим чином залежать від ступеня екранування (товщини фольги – за умови екранування суцільним її шаром, або від характерних розмірів комірки – при екранування решіткою) і встановлення такого зв'язку є цікавою задачею, що може бути вирішена як експериментально (з подальшою обробкою і отриманням регресійної моделі), так і теоретично (шляхом розгляду затухання електромагнітних хвиль у заданому екрануючому середовищі). Як і у попередніх випадках, особливо корисним з педагогічної точки зору є порівняння результатів, отриманих студентом кількома різними способами, між собою (чим ближчими виявляються результати, тим вище рівень задоволення своєю роботою, що його отримують студенти).

Якщо одна контрольована величина залежить від кількох інших (також поширена ситуація у галузі кібербезпеки), то можна застосовувати методи багатовимірного регресійного аналізу для побудови відповідної функціонально залежності.

Суттєву роль для моделювання мають і графічні засоби, такі як, наприклад, блок-схеми (застосовні для наочного представлення алгоритмів з не дуже великою кількістю стадій). Уніфікована мова моделювання (UML) є зручною для об'єктно-орієнтованої розробки (зокрема, програмного забезпечення, чи технічних систем) і являє собою набір діаграм із певними жорсткими правилами їх створення. Відповідно, за наявними діаграмами можна автоматично генерувати програмний код, що є суттєвою допомогою, не доступною більшій частині CASE-засобів. Широкого поширення, зокрема при розробці програмних систем захисту інформації набули і інші графічні методи моделювання та оптимізації.

Висновки. Таким чином, у статті проаналізовано методику викладання знань про методи та засоби моделювання та, відповідно, оптимізації процесів та систем у галузі кібербезпеки. На конкретних прикладах показано підходи до моделювання та оптимізації процесів кібербезпеки. Стаття може бути корисною здобувачам вищої освіти із відповідної спеціальності та викладачам вузів відповідного напрямку.

ЛІТЕРАТУРА:

1. Постанова Кабінету Міністрів України «Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти» від 29 квітня 2015 р. №266.

2. Наказ Міністерства освіти і науки України «Про особливості запровадження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти, затвердженого постановою Кабінету Міністрів України від 29 квітня 2015 року № 266» від 06.11.2015 року №1151.

3. Васильєв В.В. Математичні методи моделювання та оптимізації систем і процесів: Навчальний посібник / В.В. Васильєв, Ю.М. Квач, К.В. Киркач. – К.: НАУ, 2012. – 270 с.

4. Коба О.В., Вавіленкова А.І. Математичні методи моделювання та оптимізації систем і процесів: Навчальна програма навчальної дисципліни – К.: НАУ, 2015. – 9 с.

5. Лізунов С.І. Сучасні методи математичного моделювання та оптимізації: Навчальна програма / Лізунов С.І. – Запоріжжя: ЗНТУ, 2011. – 12 с.

REFERENCES:

1. Postanova Kabinetu Ministriv Ukrayiny «Pro zatverdzhennya pereliku haluzey znan' i spetsial'nostey, za yakymy zdiysnyuyet'sya pidhotovka zdobuvachiv vyshchoyi osvity» vid 29 kvitnya 2015 r. N266.

2. Nakaz Ministerstva osvity i nauky Ukrayiny «Pro osoblyvosti zaprovadzhennya pereliku haluzey znan' i spetsial'nostey, za yakymy zdiysnyuyet'sya pidhotovka zdobuvachiv vyshchoyi osvity,

zatverdzhenoho postanovoyu Kabinetu Ministriv Ukrayiny vid 29 kvitnya 2015 roku N 266» vid 06.11.2015 roku N1151.

3. Vasyl'yev V.V., Kvach Yu.M., Kyrkach K.V. Matematychni metody modelyuvannya ta optymizatsiyi system i protsesiv: Navchal'nyy posibnyk. – K.: NAU, 2012. – 270 s.

4. Koba O.V., Vavilenkova A.I. Matematychni metody modelyuvannya ta optymizatsiyi system i protsesiv: Navchal'na prohrama navchal'noyi dystsypliny – K.: NAU, 2015. – 9 s.

5. Lizunov S.I. Suchasni metody matematychnoho modelyuvannya ta optymizatsiyi: Navchal'na prohrama. – Zaporizhzhya: ZNTU, 2011. – 12 s.

Рецензент: д.т.н., проф. Кошкін К.В., директор Інституту комп'ютерних та інженерно-технологічних наук Національного університету кораблебудування імені адмірала Макарова

к.т.н., доц. Гайша А.А., Рябая Л.А.

ОСОБЕННОСТИ МЕТОДИКИ ИЗЛОЖЕНИЯ ДИСЦИПЛИНЫ «МАТЕМАТИЧЕСКИЕ МЕТОДЫ МОДЕЛИРОВАНИЯ И ОПТИМИЗАЦИИ ПРОЦЕССОВ КИБЕРБЕЗОПАСНОСТИ» С ИСПОЛЬЗОВАНИЕМ СОВРЕМЕННЫХ КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ

В статье рассматривается проблема интенсификации усилий студентов, направленных на изучение материала по предмету «Математические методы моделирования и оптимизации процессов кибербезопасности». В статье основное внимание уделено «компьютеризации» предмета: как в части моделирования именно компьютерных систем (защиты информации), так и путем их более широкого использования для моделирования и оптимизации. Значительное внимание уделено моделированию систем массового обслуживания; предлагается аналогичным способом вести моделирование произвольных процессов отрасли кибербезопасности, а не обязательно массового обслуживания (в качестве примера рассматривается процесс авторизации пользователя в компьютерной системе). Подчеркивается, что важную роль в моделировании играют статистические методы, как, например, регрессионный анализ (одно- и многомерный). Значительное внимание уделено сравнению результатов решения одной и той же задачи, полученных разными способами (аналитически, численно, обработкой экспериментальных данных). Статья может быть полезной для студентов соответствующих специальностей и преподавателей.

Ключевые слова: кибербезопасность, математическое моделирование, оптимизация, компьютерные информационные технологии.

Ph.D. Gaisha A.A., Ryaba L.A.

PECULIARITIES OF THE TEACHING TECHNIQUE OF "MATHEMATICAL METHODS OF SIMULATION AND OPTIMIZATION OF CYBER-SECURITY PROCESSES" COURSE WITH THE USE OF MODERN COMPUTER TECHNOLOGIES

It is considered the problem of intensifying the efforts of students aimed at studying the material on the subject "Mathematical methods for modeling and optimizing the processes of cybersecurity." The article focuses on the "computerization" of the subject: both in the modeling of computer systems (protection of information) and in their wider use for modeling and optimization. Considerable attention is paid to the modeling of queuing systems; It is proposed to simulate the arbitrary processes of the cybersecurity industry in a similar way, and not necessarily queuing systems (as an example, the process of authorizing a user in a computer system is considered). It is emphasized that statistical methods play an important role in modeling, such as regression analysis (one- and multidimensional). Considerable attention is paid to comparing the results of solving the same problem obtained by different methods (analytically, numerically, by processing experimental data). The article can be useful for students of relevant specialties and teachers.

Keywords: Cyber security, mathematical modeling, optimization, computer information technologies.