УДК 378.147

Н.Ю. Ротаньова

ПРИКЛАДНА СПРЯМОВАНІСТЬ КУРСУ «ТЕОРІЯ ЙМОВІРНОСТЕЙ ТА МАТЕМАТИЧНА СТАТИСТИКА» ДЛЯ СТУДЕНТІВ СПЕЦІАЛЬНОСТІ «КІБЕРБЕЗПЕКА»

Маріупольський державний університет

Анотація

У роботі доведена необхідність прикладної спрямованості навчання курсу «Теорія ймовірностей та математична статистика», шляхом наповнення змісту дисципліни прикладними задачами. Обґрунтована роль прикладних задач в процесі вивчення дисципліни для студентів спеціальності «Кібербезпека».

Ключові слова: теорія ймовірностей та математична статистика, прикладна спрямованість, прикладні задачі.

Abstract

The work proves the necessity of applied orientation of the course «Probability Theory and Mathematical Statistics» by filling the content of the discipline with applied tasks. The role of applied problems in the process of studying the discipline is substantiated for students of the specialty "Cybersecurity».

Keywords: Probability Theory and Mathematical Statistics, applied orientation, applied tasks.

Вступ

У процесі підготовки висококваліфікованих кадрів для сфери інформаційних технологій, зокрема кібербезпеки, особливу роль відіграє оволодіння ними ймовірнісно-статистичними методами, оскільки їх діяльність пов'язана з невизначеністю досягнення кінцевого результату через вплив великого числа випадкових і неконтрольованих чинників. Тому зміст курсу і його спрямованість на професійну діяльність є запорукою успішної та якісної підготовки студента, що в свою чергу є важливим фактором орієнтації на майбутню спеціальність.

Результати дослідження

Дисципліна «Теорія ймовірностей та математична статистика» викладається на основі освітньо-професійної програми 125 «Кібербезпека» Маріупольського державного університету для здобувачів першого (бакалаврського) рівня вищої освіти та входить до складу обов'язкових компонентів освітньо-професійної програми як дисципліна циклу професійної підготовки [1,2].

Прикладна спрямованість курсу «Теорія ймовірностей та математична статистика» необхідна. Для студентів важливо бачити взаємозв'язок дисципліни з майбутньою професійною діяльністю. Не випадково, що серед перших питань, що задають студенти на заняттях, звучать такі: «А навіщо мені потрібно це вивчати, якщо я буду фахівцем із захисту інформації?», «А де це може стати в нагоді в моїй професії?». Відповіддю на ці запитання може бути систематичне використання в навчанні математичних дисциплін криптографічних понять, законів, ідей, моделей і завдань, пов'язаних з комп'ютерною безпекою, постійна ілюстрація математичного матеріалу додатками з «теоретичних основ комп'ютерної безпеки», «захисту інформації в комп'ютерних системах» і т. д.

Сутність прикладної спрямованості дисципліни полягає в орієнтації цілей, змісту і засобів навчання у напрямку: здійснення цілеспрямованих змістових і методологічних зв'язків математики, а саме теорії ймовірностей та математичної статистики з практикою; набуття студентами в процесі математичного моделювання знань, умінь і навичок, які будуть використовуватись ними в повсякденному житті, в майбутній професійній діяльності. Остання теза передбачає включення в навчання таких специфічних моментів, які характерні для дослідження прикладних проблем, зокрема для розв'язання прикладних задач, під якими ми розуміємо задачі, що виникають за межами математики, але розв'язуються з використанням математичного апарату [3].

Прикладні задачі мають задовольняти такі методичні вимоги: 1) задачі повинні мати реальний практичний зміст, який забезпечує ілюстрацію практичної цінності і значущості набутих математичних знань; 2) зміст задачі повинен викликати у студентів пізнавальний інтерес, давати можливість демонструвати ефективне використання математичних знань на практиці; 3) поняття і терміни задач мають бути відомі або інтуїтивно зрозумілі; 4)числові дані в прикладних задачах повинні відповідати існуючим на практиці, тобто бути реальними [3].

Проблема прикладної спрямованості навчання вже давно є об'єктом дослідження педагогів, методистів, математиків. Цій проблемі приділяли увагу Г.П. Бевз, Б.В. Гнеденко, М.Я. Ігнатенко, Ю.М. Колягін, А.В. Прус, З.І. Слєпкань, В.В. Фірсов, В.О. Швець та інші. Збірники завдань з теорії ймовірностей та математичної статистики налічують багато прикладних задач, що відображають різноманітні життєві ситуації, але з галузі інформаційних технологій їх недостатньо.

Тому мета статті – розкрити шляхи прикладної спрямованості навчання дисципліни «Теорія ймовірностей та математична статистика» для студентів спеціальності «Кібербезпека».

Отже, велике значення в процесі навчання дисципліни «Теорія ймовірностей та математична статистика» має розуміння студентами практичної значимості навчального матеріалу, перспективи його використання. Тому при вивченні будь-якого теоретичного матеріалу слід намагатися відразу ж приводити приклади з життя, завдання, в яких цей матеріал знаходить фактичне застосування, а особливо корисно, якщо умова задачі наближена до майбутньої професійної діяльності.

Під час вивчення теми «Класичне означення ймовірності» буде доцільно запропонувати студентам розв'язати наступні задачі, зі змісту яких, вони отримають ще і корисну інформацію з кібербезбеки.

Ймовірність злому мережі зовнішнім хакером або внутрішнім зловмисником залежить від трьох параметрів:

1. Перший параметр – надійність засобів, що захищають мережу (наприклад, міжмережевий екран або фільтруючий маршрутизатор, системи запобігання вторгнень, антивіруси, системи захисту електронної пошти і контролю веб-доступу і т. Д.). Даний параметр (надійність) ніколи не буде дорівнює максимальному значенню – одиниці. Пов'язано це з тим, що, на жаль, не існує абсолютно надійних систем, які позбавлені помилок і вразливостей. Адже людям, котрі створюють такі системи, властиво помилятися, і помилки можуть коштувати дуже дорого, що вже не раз демонструвала історія. Слід відзначити, що і нулю цей параметр дорівнює не може, оскільки хоч якийсь, але рівень захисту ці засоби забезпечують. За статистичними даними інституту Карнегі-Меллона, який вже багато років займається дослідженнями надійності програмного забезпечення, середньостатистична програма містить до 15 помилок/вразливостей на 1000 рядків коду. Знайти ймовірність злому мережі від пошкодження засобів, що захищають мережу через вміст помилки.

2. Другий параметр, що впливає на захищеність мережі, це вже якість не реалізації, а настройки і конфігурації системи захисту. Даний параметр також залежить від людського фактору, але число можливих налаштувань незрівнянно менше числа рядків програмного коду в системі, то його максимальне значення, одиниця, теоретично може бути досягнуто. Вказаний параметр нулю не дорівнює, адже зазвичай система захисту як-не-як, а налаштована. На практиці значення параметра змінюються хвилеподібно, тому що якість налаштувань поступово погіршується і потребує їх регулярного аудиту. На практиці майже завжди конфігурація неідеальна. Наприклад, в звіті компанії Positive Technologies наводяться факти про те, що в рамках зовнішнього тестування на проникнення експертам вдалося подолати мережевий периметр 92 організацій зі 100. Знайти ймовірність того, що від внутрішнього порушника було отримано повний контроль над інфраструктурою в усіх досліджуваних системах, то тобто було виявлено проникнення у внутрішню мережу.

3. Третій параметр – швидкість реагування на атаки зловмисників з боку не тільки автоматизованих засобів захисту, а й фахівців, що відповідають в компанії за безпеку. Навіть пропущена периметровими захисними засобами атака може бути вчасно помічена в наявному центрі моніторингу безпеки (Security Operations Center, SOC), який дозволить запобігти її руйнівні дії. Сьогодні взагалі парадигма безпеки зсувається від спроб запобігти 100% загроз до збалансованої ідеї розділити порівну захисні механізми між запобіганням, виявленням і реагуванням. Цей імовірнісний параметр, як і попередній, може бути дорівнює одиниці, і на практиці саме в такому випадку можна постаратися досягти ідеалу. Але ймовірність захисту від злому або обходу захисної системи ніколи не буде дорівнює одиниці, тобто створити абсолютно захищену систему неможливо в принципі. Наприклад, генеральної директор однієї великої корпорації, яка має 1000 комп'ютерів, приніс на роботу заражений домашній ноутбук, і саме з нього почалося зараження внутрішньої мережі, досить

непогано захищеної від зовнішньої загрози. А ось перед необачністю гендиректора і небажанням дотримуватися політики безпеки компанія здалася і ще 590 співробітників, що підключали до своїх комп'ютерів 4G-модеми, через які вірус проникав всередину систем, виявили цей вірус. Знайти відносну частоту заражених комп'ютерів.

Безумовно, неприємно усвідомлювати, що всі наші дії приречені на невдачу і зловмисники здатні зовні або зсередини, безпосередньо або обхідним шляхом, все одно проникнути в захищену систему або зламати її. Тому завдання фахівців з безпеки сьогодні в 99% випадків полягає в тому, щоб істотно ускладнити життя зловмисників, роблячи їх спроби проникнення/злому занадто дорогими, а якщо вони все-таки і увінчаються успіхом, то служба інформаційної безпеки підприємства повинна оперативно нівелювати всі наслідки, збудувавши відповідний процес реагування на інциденти інформаційної безпеки.

З висновку про неможливість побудови абсолютного захисту є кілька цікавих наслідків. По-перше, абсолютно захищену мережу створити неможливо до тих пір, поки ймовірність злому системи захисту не досягне нульового значення (і навпаки, поки надійність захисту не досягне одиниці). А це можливо тільки в тому випадку, якщо усунути з процесу створення захисного засобу або механізму людський фактор, який є головною причиною всіх помилок (і програмування, і конфігурації, і реагування). Очевидно, що на сучасному етапі розвитку науки та інформаційних технологій повністю це неможливо, але останнім часом багато гравців ринку кібербезпеки приділяють підвищену увагу питанню автоматизації багатьох захисних процесів – від розпізнавання загроз за допомогою машинного навчання до реагування на них, від інтеграції засобів захисту між собою до написання автоматичних правил захисту [4].

Тобто будь-яка система вимагає кваліфікованого персоналу, що не тільки знає, а й вміє налаштовувати засоби захисту, але і який знає та вміє оцінити всі ризики та обчислити ймовірність збою системи за допомогою знань, умінь і навичок, отриманих в результаті вивчення курсу «Теорія ймовірностей та математична статистика».

Під час вивчення теми «Геометричне означення ймовірності» можна запропонувати розв'язати таке завдання: в контрольний блок системи охорони сигналізації надходять сигнали від двох датчиків, причому надходження кожного з сигналів рівно можливий в будь-який момент проміжку часу тривалістю *T*. Моменти надходження сигналів незалежні один від одного. Контрольний блок спрацьовує, якщо різниця між моментами надходження сигналів менше t ($t < T$). Знайти ймовірність того, що контрольний блок спрацює за час *T*, якщо кожен з датчиків буде надсилати по одному сигналу.

Серед практичних завдань з теми «Теореми додавання і множення ймовірностей. Формула повної ймовірності. Формула Байєса» провідне місце повинні займати завдання прикладного характеру, наприклад, такі як «На Web-сайт впроваджуються три незалежних атаки. Імовірність вдалою першої атаки дорівнює 0,4, другої – 0,5, третьої – 0,6. Для виведення Web-сайту з ладу досить трьох вдалих атак. При двох вдалих атаках сайт виходить з ладу з ймовірністю 0,6; при вдалій одній атаці сайт виходить з ладу з ймовірністю 0,2. Знайти ймовірність того, що в результаті трьох атак Web-сайт буде виведений з ладу?».

Отже, з метою мотивації до вивчення курсу важливо, щоб умова завдання була наближена до реального життя. Корисно проводити бесіди про важливість знань, що необхідні студентам у повсякденному житті та у майбутній професії. Саме це переконує їх у тому, що теорія ймовірностей необхідна у всіх видах людської діяльності, зокрема у галузі інформаційної безпеки.

Висновки

Завдяки використанню прикладних завдань студент має можливість побачити прямий взаємозв'язок матеріалу, що вивчається, з його практичним застосуванням. Саме при такому підході створюються передумови активного застосування математичних знань, здатність працювати самостійно й творчо, уміння працювати з навчальною й довідковою літературою, студенти залучаються до сфери професійної культури, тому впровадження прикладної спрямованості курсу «Теорія ймовірностей та математична статистика» є важливим кроком на шляху до підвищення якості підготовки фахівців з кібербезпеки.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Освітньо-професійна програма 125 Кібербезпека [Електронний ресурс]. - Режим доступу: http://mdu.in.ua/Ucheb/OPP/bak-2019/kiberbezpeka.pdf

2. Стандарт вищої освіти України: перший (бакалаврський) рівень, галузь знань 12 – Інформаційні технології, спеціальність 125 – Кібербезпека [Електронний ресурс]. - Режим доступу: https://mon.gov.ua/storage/app/media/vishcha-osvita/zatverdzeni%20standarty/12/21/125-kierbezpeka-bakalavr.pdf

3. Соколенко Л.О., Філон Л.Г., Швець В.О. Прикладні задачі природничого характеру в курсі алгебри і початків аналізу: практикум. Навчальний посібник. – Київ: НПУ імені М.П. Драгоманова, 2010. – 128 с.

4. Десять аксиом кибербезопасности. Аксиома первая. Взломать можно абсолютно все! [Електронний ресурс]. - Режим доступу: https://www.it-world.ru/cionews/danger/143892.html

Ротаньова Наталія Юріївна **—** кандидат педагогічних наук, доцент кафедри математичних методів та системного аналізу, Маріупольський державний університет, Маріуполь, e-mail:rotanevan@gmail.com

Rotaneva Natalia – Candidate of Pedagogical Sciences, Associate Professor of the Department of Mathematical Methods and System Analysis, Mariupol State University, Mariupol, e-mail:rotanevan@gmail.com