програмних систем чи онлайн ресурсів, як наприклад, системи дистанційного навчання (перевірка самостійності виконаного завдання користувачем).

Список використаних джерел

1. Gaines R. Authentication by keystroke timing: some prelimary results / Gaines R., Lisowski W., Press S. // Technical Report R-2526-NSF. – Santa Monica:RAND Corporation, 1980. – 51 p.
2. Leggett J. Verifying identity via keystroke characteristics / Leggett J., Williams G.// International Journal of Man-Machine Studies. –London: Acadenmic Press Ltd, 1988. –pp.67-76.
3. Hawkins D. Identification of Outliers / Hawkins D. – Springer Netherlands, 1980. –188 p.
4. Haider S. A multi-technique approach for user identification through keystroke dynamics / Haider S., Abbas A., Zaidi A.K. // IEEE International Conference on Systems, Man and Cybenetics, 2000. –pp. 1336–1341.
5. Manevitz L. Document Classification on Neural Networks Using Only Positive Examples / Manevitz L., Malik Y. // ACM SIGIR conference, 2000.
6. Большев А.К. Применение нейронных сетей для обнаружения вторжений в компьютерные сети / Большев А.К., Яновский В.В. // Вестник Санкт-Петербургского университета, Вып. 4. СПб., 2009. – С. 38-44.
7. Kevin S. Comparing Anomaly-Detection Algorithms for Keystroke Dynamics / Kevin S. // IEEE, 2009. – pp.125-134.

Биометрическая идентификація пользователей систем дистанционного образования на основании методов обнаружения аномалий средствами искуственных нейронных сетей

Иваськив И.С.

Аннотация. В статье рассмотрен вопрос биометрической идентификации пользователей систем дистанционного образования на основании анализа их клавиатурного ритма с использованием средств искусственной нейронной сети. Описываются основные алгоритмы и модели данных, применяемые в задачах моделирования клавиатурной динамики пользователей. Описываются структура и параметры сети – детектора аномалий, применяемой для биометрической идентификации пользователей системы дистанционного обучения.

Ключевые слова: системы дистанционного образования, обнаружение аномалий, биометрическая идентификация, анализ клавиатурного ритма.

Biometric users identification in online education systems based on anomaly detection methods by means of artificial neural networks

I.S. Ivaskiv

Resume. The article deals with the issue of biometric identification of users of distance education systems based on the analysis of their keyboard rhythm by means of an artificial neural network. The main algorithms and data models used in modeling problems of user's keyboard dynamics are described. The structure and parameters of the artificial network – an anomaly detector used for biometric identification of users, are described.

Keywords: online learning, anomaly detection, biometric identification, neural networks.

УДК 37 004(07)

Ящик О. Б.

Тернопільський національний педагогічний університет імені Володимира Гнатюка

Зміцнення глобальної культури кібербезпеки в мережі Інтернет

Анотація. У статті досліджуються проблеми кібербезпеки в мережі Інтернет; вивчено історію її виникнення та розвитку; з'ясовані основні принципи вдосконалення глобальної культури безпечної мережевої взаємодії. Розглянуті питання, пов'язані із забезпеченням інформаційної безпеки особистості учнів в контексті професійної підготовки компетентних педагогів, здатних сприяти створенню інфобезпечного середовища в школі, а також навчити школярів захищатись від небезпечного і шкідливого інформаційного контенту.

Ключові слова: кібербезпека, мережева взаємодія, захист персональних інформаційних ресурсів, шкідливий інформаційний контент, інфо-безпечне навчальне середовище.

Актуальність проблеми. XXI століття характеризується інтенсивним використанням інформаційних технологій у житті суспільства. Широке проникнення соціальних мереж в повсякденне життя, використання Інтернету як основного джерела різноманітних відомостей внесли серйозні зміни в соціальні стосунки у світі. Сьогодні використання інформаційних технологій дає можливість людям з різних країн і континентів обговорювати актуальні проблеми в режимі реального часу, отримувати відомості безпосередньо з місця подій.

Усі великі світові ЗМІ мають представництва в мережі Інтернет, даючи нам унікальну можливість отримувати відомості з розмаїтих джерел, формувати загальне уявлення про те, що відбувається в освіті, бачити через таке спілкування відмінність у культурах (Рис. 1). Помітною особливістю Інтернету до останнього часу була можливість залишитися анонімним, приховати своє

соціальне положення, місце проживання, ґендерну належність, що сприяло формуванню нового середовища спілкування, позбавленого психологічних барєрів та внутрішніх компромісів співрозмовників.

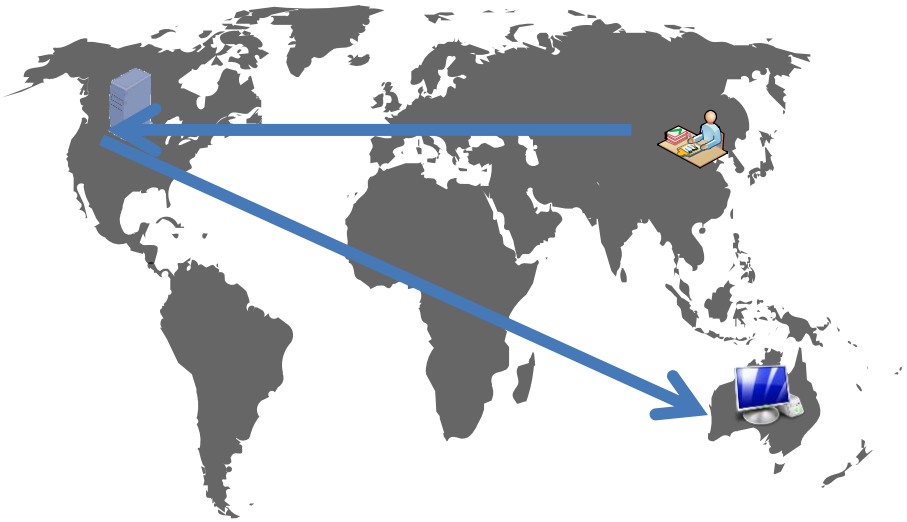

Рис. 1. Світова взаємодія

Проте завдяки таким особливостям інформаційні технології стали унікальним середовищем для розвитку негативних явищ, таких як: поширення нелегального контенту, використання недосконалості інформаційних систем для здійснення протиправних дій, включаючи розсилання SPAM повідомлень тощо.

На сьогодні ситуація з безпекою в Інтернеті є надзвичайно складною та потребує ґрунтовного вивчення.

Подання основного матеріалу. Проблема кібербезпеки порівняно нова: її фундаментом став винахід у другій половині XX століття засобів обчислювальної техніки, комп'ютерних мереж і новітніх засобів зв'язку. Перший відомий інцидент у цій сфері стався в 1981 р. і був пов'язаний з поширенням комп'ютерних вірусів для персонального комп'ютера (ПК) Apple II [4]. Основними цілями зловмисників тоді були самоствердження і пошук нових можливостей самореалізації. Протидія вірусним епідеміям і захист інформаційних ресурсів від несанкціонованого доступу у світовому масштабі стали головними завданнями в галузі інформаційної безпеки.

У кінці 1980-х рр. уперше з'являються повідомлення про можливість шахрайства з використанням банківських карт. Саме цей момент став поворотним – кримінальний світ дізнався, що за допомогою інформаційних технологій можна отримувати реальні гроші. Таким чином, правоохоронні органи були поставлені перед необхідністю розбиратися в нових технологіях і будувати доказову базу на основі віртуальних даних.

У цей час проблема забезпечення інформаційної безпеки трактувалася як забезпечення конфіденційності. Основними замовниками в цій галузі були представники різного роду державних структур і розвідувальних управлінь.

Нові можливості кіберзлочинність отримала з винаходом технологій *HTTP, HTML і URL* в 1990 році і запуском першого «www» сайту. Вплив цього винаходу на сучасні засоби комунікації важко оцінити, але деякі експерти в галузі інформаційних технологій вважають, що Інтернет став світовою мережею тільки завдяки технологіям Web. Фактично до цього моменту Інтернет був просто середовищем обміну статичними даними через електронну пошту, електронні дошки оголошень і спеціалізовані сервери. Використання технології гіпертексту дозволило користувачам з мінімальними технічними можливостями створювати документи з посиланнями на ресурси, розташовані на інших серверах.

З розвитком технологій подання важливих повідомлень у всесвітній павутині, еволюцією мережевих технологій (і, як наслідок, збільшенням швидкості під'єднання комп'ютерів до Інтернету), впровадженням технологій on-line платежів значно розширилися можливості кіберзлочинців для протиправної діяльності. Істотну роль тут зіграв розвиток технологій Web 2.0 у вересні 2005 року. Особливістю Web 2.0 є принцип залучення користувачів до наповнення і багатократного вивіряння контенту. Однак, як правило, йдеться лише про наповнення повідомленнями, а питання їх надійності, вірогідності, об'єктивності не розглядаються. З точки зору кібербезпеки, Web 2.0 зручний тим, що дає змогу зловмисникові розмістити нелегальний контент на сайті, на якому підтримується можливість наповнення користувачем.

Світ також зіткнувся з проблемою визначення юрисдикції в кіберпросторі. У випадку, якщо в злочині брали участь, наприклад, хакер з Китаю, сервери знаходилися на території США, а потерпілий був з Австралії, то за законами якої країни вести судовий розгляд?

Ще одним цікавим явищем, що вплинуло на кібербезпеку, став прихід Інтернет реклами. Сьогодні існують сайти з величезною кількістю відвідувань. Особливістю інформаційних технологій в цій галузі є значний обсяг відомостей про людину, яка переглядає рекламне повідомлення. Можна

відслідкувати адресу користувача Інтернету, включаючи номер будинку, сайти, які він переглядав перед цим, які запити вводив в пошукових системах, який у нього комп'ютер, яка операційна система. На основі усіх таких відомостей можна зробити рекламне повідомлення націленим на цілком конкретну аудиторію. Сьогодні існує безліч сайтів, єдиним доходом яких є реклама.

З приходом в Інтернет комерції помінялися і цілі кіберзлочинців. Провідним завданням стало отримання грошових коштів. Якщо розглянути зміст сайту, де публікується нелегальний контент, то можна виявити наступні функції:

– показ рекламних банерів, у тому числі провокація користувача для переходу на відповідні сайти-рекламодавців;

– Malware. Зараження комп'ютера різного роду шкідливим програмним забезпеченням. Цілі можуть бути наступні:

а) крадіжка ідентифікаційних даних – логін/пароль на відомих серверах; номери, паролі адреси інтернет-банків, реквізити платіжних карт тощо;

б) встановлення botnet клієнтів для подальшого використання комп'ютера без відома жертви.

– публікація матеріалів, що порушують міжнародне і місцеве законодавство.

Таким чином, безпека користувача в сучасних системах інформаційного обміну останнім часом стала однією з найбільш важливих проблем. Поява в 1995 році американського порталу Classmates.com призвела до створення нового покоління інформаційних сервісів, які об'єднують людей не лише за інтересами в інформаційній сфері, але й за соціальними зв'язками. Сьогодні вони називаються Соціальними мережами. Зараз багато таких мереж використовуються не лише для спілкування з людьми, що поділяють однакові погляди та переконання або просто знайомими, а й для пошуку контрагентів і партнерів у бізнесі. Проте соціальні мережі стали ще і площадкою, з якої можна зібрати величезну кількість персональних даних про людину для використання їх в протиправних цілях. Так, наприклад, в дослідженні Panda Security [6] наводяться наступні дані досліджень: 20% дітей, які регулярно використовували Інтернет, піддавалися сексуальним домаганням за віртуального спілкування один раз, 11% піддавалися цьому кілька разів. В інших випадках дія може набувати форми образ з боку інших Інтернет-користувачів або поштових повідомлень з образливим змістом. Тривожні дані: 14,5% дітей, що взяли участь в опитуванні, призначали зустрічі з незнайомцями через Інтернет, 10% з них ходили на зустрічі самостійно, а 7% нікого не повідомляли про такі зустрічі [5].

Як наслідок, вже зафіксовані злочини, що здійснювалися після збирання відомостей про жертву, її звички, розпорядок дня, імена знайомих, аналізу фотографій для визначення фінансового стану жертви тощо.

Варто також відмітити використання Інтернет-ресурсів різноманітними екстремістськими угрупуваннями та терористичними організаціями. Не ігнорують сучасні технології і секти різного типу. Кіберзлочинці цього виду використовують ресурси і сервіси соціальних мереж для вербування нових послідовників і виконавців.

Проте використання сучасних комунікаційних технологій для організації безладів і революцій сьогодні ще недооцінена. Як показали недавні події в Єгипті, від'єднання цілої країни від міжнародного мережевого простору не здійснило істотного впливу на розвиток подій.

Таким чином, необхідно зазначити, що стрімкий розвиток інформаційних технологій кардинально змінив підхід до кібербезпеки державних органів, підприємств, інших організацій та індивідуальних користувачів, які розробляють ці інформаційні системи і мережі, здійснюють управління ними, обслуговують і використовують їх. Глобальна культура кібербезпеки вимагає від усіх учасників мережевої взаємодії дотримання таких головних принципів:

– *обізнаність* (про необхідність безпеки інформаційних систем і мереж і про те, що можна зробити для підвищення безпеки);

– *відповідальність* (регулярний огляд та оцінювання інформаційних систем і мереж з точки зору відповідності середовищу їх застосування);

– *реагування* (реалізація своєчасних заходів з попередження небезпечних інцидентів, їх виявлення і реагування на них; обмін відомостями про загрози і чинники вразливості; здійснення процедур, що передбачають оперативну і ефективну співпрацю у справі попередження таких інцидентів; трансграничний інформаційний обмін і співпраця);

– *етика* (врахування законних інтересів інших; розуміння можливості шкідливих наслідків власних дій або бездіяльності);

– *демократія* (відповідність демократичним цінностям, включаючи свободу обміну думками та ідеями, вільний потік повідомлень, конфіденційність повідомлень і комунікації, належний захист відомостей особистого характеру, відкритість і гласність тощо);

– *оцінювання ризику* (здійснення періодичного оцінювання ризику, що дозволяє виявляти загрози і чинники уразливості; ґрунтується на досить широкій базі, щоб охопити такі ключові внутрішні і зовнішні чинники, як технологія, фізичні і людські чинники, використовувана методика і послуги третіх осіб, що позначаються на безпеці; дає можливість визначити допустиму міру ризику; допомагає вибрати належні інструменти контролю, що дозволяє регулювати ризик потенційного збитку інформаційним системам і мережам з урахуванням характеру і значущості інформаційних ресурсів);

– *впровадження та управління засобами забезпечення кібербезпеки* (внесення міркувань безпеки в якості найважливішого елементу планування, експлуатації і використання інформаційних систем і мереж; комплексний підхід до управління забезпеченням кібербезпеки).

На сьогоднішній день можна виокремити такі основні проблеми в галузі кібербезпеки:

1) захист дітей в on-line комунікаціях;
2) протидія проявам екстремізму, розпалюванню міжнаціональної ворожнечі тощо;
3) захист авторських прав;
4) забезпечення безпеки електронних платежів і торгівельних угод;
5) протидія розсиланню спаму;
6) забезпечення збереження таємниці особистого життя в мережі Інтернет.

Одним із ключових підходів до розв'язування проблем кібербезпеки на сучасному етапі розвитку інформаційних технологій має стати введення теми з безпеки Інтернету в загальноосвітніх, професійних та вищих навчальних закладах. У учнів на уроках інформатики необхідно формувати інформаційний світогляд, що є невідємною складовою інформаційної культури. У своїх працях Ю.С. Рамський та М.А. Умрик [2, с. 16-25] детально розглядають найважливіші компоненти інформаційного світогляду (образ самого суб'єкта, картина світу, життєва стратегія індивіда), зокрема в структурі інформаційного світогляду виокремлюють пізнавальну складову, до якої включається необхідність усвідомлювати проблеми інформаційної безпеки особистості, її інформаційної екології та проблеми інформаційної злочинності. Швидкість, з якою діти та молодь залучаються до взаємодії в Інтернет-мережах, є надзвичайною. Відсоток дітей, які активні в on-line, такий високий, що діти починають виступати найчисленнішою категорією користувачів онлайн-технологій. Хоча через Інтернет забезпечуються величезні можливості для того, щоб діти та молодь розгорнули свої горизонти світобачення через вивчення і пошук в мережі, та ризики, які супроводжують ненадійне використання Інтернету, можуть перекреслити ці on-line-вигоди.

Варто відмітити, що у багатьох країнах світу відбулося включення уроку on-line-безпеки в програми навчання в школі. В більшості країн Європи вже з 2008 р. проводиться навчання дітей основних аспектів кібербезпеки. Зокрема, в Іспанії включено захисну Онлайн-тему в курс «Інформація і технологія зв'язків»; в Швеції дозволяється місцевим органам влади школи вибирати, де саме вони хочуть включати цю тему; у Великобританії включено цю проблему до курсу «Здоров'я, Технологія і Досліди»; в Данії зосереджують увагу на навчанні дітей та молоді питань захисту комунікацій у всесвітній павутині [7, с. 9].

Таким чином, виникає необхідність переглянути спільні навчальні цілі у площині безпеки використання Інтернету та зосередитись на розгляді аспектів захисту дій в кіберпросторі, особливо стосовно формування навичок безпечного спілкування дітей у соціальних мережах. Розділи, які можуть включатися до теми з безпеки використання Інтернету, є наступними: кібербулінг, сексуальні домагання в Інтернеті, відеоігри, соціальні media, безпечне дослідження, онлайн-зустрічі тощо. Відсутність підручників та матеріалів з даної проблеми також виступає вагомою перешкодою додавання теми безпеки Інтернету до шкільної програми.

Таким чином, постає нагальна потреба не тільки в теоретичних та методичних напрацюваннях у цій сфері, а й у кваліфікованій підготовці майбутніх педагогів, які володітимуть професійними компетентностями, необхідними для здійснення навчальної та розвиваючої діяльності з питань інформаційної безпеки.

Особливістю формування компетентностей майбутніх учителів у галузі забезпечення інформаційної безпеки школярів є і те, що разом з навчанням організаційних і технічних засобів захисту інформаційних ресурсів, необхідно прищеплювати учням моральну складову і відповідальність за використання інформаційних ресурсів, що потенційно може заподіяти збитки від невмілого з ними поводження не тільки учневі, але й іншим суб'єктам навчального процесу [1, с. 79].

Для формування спеціальних компетентностей у сфері безпеки використання Інтернету і вивчення проблематики інформаційної безпеки для майбутніх педагогів необхідно розробити навчальний курс, основною метою якого буде навчання студентів принципів і засобів забезпечення інформаційної безпеки учнів, конкретних освітніх об'єктів і установ, суспільства і держави. Також необхідно показати важливість засвоєння системних комплексних методів захисту персональних інформаційних ресурсів від різноманітних видів об'єктивних і суб'єктивних загроз для організації інфо-безпечного середовища в освітній організації з метою недопущення шкоди від небезпечних інформаційних дій здоров'ю, психіці і свідомості школярів.

Завданнями навчання такого курсу будуть:

– оволодіння теоретичними знаннями в сфері інформаційної безпеки;
– формування умінь добору методів для захисту персональних даних;
– отримання практичного досвіду діяльності з питань забезпечення інформаційної безпеки школярів, сім'ї, освітньої установи.

Студенти повинні ознайомитися з сучасною концепцією інформаційної безпеки, організаційно-правовими аспектами безпеки Інтернету, завданнями захисту персональних даних і інформаційних ресурсів, а також основними тенденціями і напрямами формування та функціонування систем захисту інформаційних ресурсів.

Результатом цього буде отримання майбутніми педагогами теоретичних знань про основні існуючі нормативно-правові акти в галузі інформаційної безпеки і захисту інформаційних ресурсів, методи фільтрації інформаційного контенту і батьківського контролю в глобальній мережі Інтернет, принципи організаційного захисту інформаційних потоків, а також заходи протидії несанкціонованим інформаційним діям на користувача. Практичні навички включатимуть володіння методами і засобами виявлення інформаційних загроз, навички виявлення і знищення комп'ютерних вірусів, безпечне використання технічних засобів в професійній педагогічної діяльності і, як кінцевий результат, – проектування політики інформаційної безпеки навчального закладу.

Висновок. Підводячи підсумок, можна стверджувати, що для зміцнення культури кібербезпеки в мережі Інтернет необхідно враховувати вимоги і реалії сучасного інформаційного суспільства масової комунікації. Як свідчить досвід, не можна не зважати на всі істотні загрози і можливі негативні наслідки тотальної інформатизації. Разом з традиційними аспектами навчання інформаційної безпеки і захисту інформаційних ресурсів обов'язково мають використовуватися методологічні, соціально-філософські, культурологічні, правові, організаційно-управлінські аспекти.

Ключовим чинником забезпечення інформаційної безпеки дітей та молоді є наявність контингенту компетентних педагогів, здатних на основі професійної підготовки забезпечити як створення інфо-безпечного середовища в навчальному закладі, так і підготувати учнів до самостійного прийняття рішень із захисту своєї особистості від потенційно шкідливого інформаційного контенту. Підготовка таких фахівців повинна вестися на основі єдиного задуму та розуміння цілей і завдань професійної підготовки педагогів у системі вищої педагогічної освіти.

Список використаних джерел

1. Бочаров М. И. Преемственность содержания обучения информационной безопасности в новых государственных образовательных стандартах общего образования / М. И. Бочаров // Информатика и образование. – 2011. – № 6. – С. 78 – 83.
2. Рамський Ю. С. Складові інформаційної культури майбутнього вчителя математики / Ю. С. Рамський, М. А. Умрик // Науковий часопис НПУ імені М. П. Драгоманова. Серія 2. Комп'ютерно-орієнтовані системи навчання. – 2011. – Вип. 11. – С. 16 – 25.
3. Рамський Ю. С. Активізація пізнавальної діяльності школярів засобами «ІнфоНІС» / С. О. Лещук, Ю. С. Рамський / Науковий часопис НПУ імені М. П. Драгоманова. Серія 2. Комп'ютерно-орієнтовані системи навчання. – 2007. – Вип. 5 (12). – С. 120 – 125.
4. Інформаційна безпека [Електронний ресурс] / Режим доступу : https://uk.wikipedia.org/wiki/Інформаційна_безпека.
5. Глобальна програма кібербезпеки МСЕ. Основа для міжнародної співпраці в галузі кібербезпеки [Електронний ресурс] / Режим доступу : http://www.ifap.ru/pr/ 2008/080908aa.pdf.
6. Як уберегти дітей від небезпек інтернету: правила поведінки в мережі [Електронний ресурс] / Режим доступу : http://reggin.ru/publ/kak uberech detej ot opasnostej interneta pravila povedenija v seti/ 20-1-0-55.
7. Statovci G. Adding Internet Safety and Financial Education for Children as New Courses in Elementary School Curriculum / Gresa Statovci. – Rochester Institute of Technology, 2015. – 35 p.

Укрепление глобальной культуры кибербезопасности в сети Интернет

Ящик А.Б.

Аннотация. В статье исследуются проблемы кибербезопасности в сети Интернет; изучена история ее возникновения и развития; выяснены основные принципы укрепления глобальной культуры безопасного сетевого взаимодействия. Рассмотрены вопросы, связанные с обеспечением информационной безопасности личности учащихся в контексте профессиональной подготовки компетентных педагогов, способных обеспечить создание инфобезопасной среды в школе, а также научить школьников защищаться от опасного и вредного информационного контента.

Ключевые слова: кибербезопасность, сетевое взаимодействие, защита персональных информационных ресурсов, вредный информационный контент, инфобезопасная учебная среда.

Strengthening the global culture of cyber security on the Internet

Yashchyk O.B.

Resume. The article deals with the problem of cyber security on the Internet; it delves into the history of its appearance and development. The main principles of global culture of secure network interaction are defined in the paper. The author analyzes issues connected with providing information security of student`s personality in the context of in-service training of competent pedagogues who are capable of providing the creation of infosecure environment at school as well as teach students to protect themselves from dangerous and harmful information content.

Key words: cyber security, network interaction, personal information resources protection, harmful information content, infosecure educational environment.